УТВЕРЖДЕНО

приказом
НО «Фонд капитального ремонта
МКД в ЯНАО»
от «31» июля 2015 года № 69-ОД

КОНЦЕПЦИЯ
безопасности персональных данных, обрабатываемых в информационных системах персональных данных некоммерческой организации «Фонд капитального ремонта многоквартирных домов в Ямало-Ненецком автономном округе»

г. Салехард
2015 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Концепция безопасности персональных данных, обрабатываемых в информационных системах персональных данных некоммерческой организации «Фонд капитального ремонта многоквартирных домов в Ямало-Ненецком автономном округе» (далее по тексту – Фонд, Концепция), является локальным нормативным актом, в котором определена система взглядов на обеспечение безопасности персональных данных Фонда.

1.2. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных Фонда, в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности персональных данных (ПДн).

1.3. Концепция разработана в соответствии с системным подходом к обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных Фонда. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз безопасности ПДн и разработку системы защиты ПДн с позиции комплексного применения технических и организационных мер и средств защиты.

1.4. Система защиты персональных данных (СЗПДн) представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

1.5. 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.

1.6. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) локальных нормативных актов в области обработки и защиты персональных данных в ИСПДн Фонда.

1.7. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

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

1.9. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению безопасности ПДн Фонда, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации,

отвечающих за обеспечение безопасности информационных технологий и защиту информации.

1.10. Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Фонда;
- принятия управленческих решений, разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности структурных подразделений Фонда при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Фонде.

1.11. Область применения Концепции распространяется на все структурные подразделения Фонда, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на структурные подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

1.12. Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных.

1.13. В настоящей Концепции используются следующие термины и их определения:

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

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

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.

Доступ к информации – возможность получения информации и ее использования.

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

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

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

Информационная технология – 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 распространять их 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.

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 – 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.

Объект вычислительной техники (ОВТ) – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы (АС), автоматизированные рабочие места (АРМ), информационно-вычислительные центры (ИВЦ) и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор (персональных данных) – юридическое 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.

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

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов,

организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

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.

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.

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

2. ЦЕЛЬ И ЗАДАЧИ СЗПДн

2.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

2.1.1. Для достижения основной цели система защиты ПДн в ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ОВТ и доступ к его ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;

- аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;
- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

3. ОБЪЕКТЫ ЗАЩИТЫ

3.1. Основными объектами защиты при обеспечении безопасности информации ПДн являются:

- информационные ресурсы, представленные в виде носителей информации на различной физической основе и информационных массивов;
- средства обработки информации;
- информационно-телекоммуникационные сети Фонда;
- помещения Фонда, в которых размещаются носители или средства обработки информации;
- все технические средства и системы, размещенные в помещениях Фонда, где обрабатывается (циркулирует) информация ограниченного доступа;
- система защиты информации.

4. КАТЕГОРИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ФОНДА, ПОДЛЕЖАЩИХ ЗАЩИТЕ

4.1. Обработка персональных данных в Фонде производится в информационных системах персональных данных.

4.2. В подсистемах Фонда циркулирует информация различных уровней конфиденциальности, содержащих сведения ограниченного распространения (служебная информация, персональные данные и т.п.) и открытые сведения.

В документообороте Фонда присутствуют:

- платежные поручения и другие расчетно-денежные документы;
- различного рода отчеты (финансовые, аналитические и другие);
- сведения о лицевых счетах;
- обобщенная информация, документы ограниченного распространения;
- служебная переписка.

4.3. Защите подлежит вся информация, циркулирующая в Фонде и содержащая:

- общие открытые сведения;
- сведения ограниченного распространения;
- сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен собственником информации (Фондом) в соответствии с Федеральным законодательством;
- сведения о гражданах (персональные данные), доступ к которым ограничен в соответствии с Федеральным законодательством.

4.4. Перечень персональных данных, подлежащих защите, определен в Положении об организации работы с персональными данными в некоммерческой организации «Фонд капитального ремонта многоквартирных домов в Ямало-Ненецком автономном округе».

4.5. Кроме того, в ИСПДн защите подлежат:

- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

5. КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДн

5.1. Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является работник Фонда, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком доступа и служебными обязанностями.

5.2. Пользователи ИСПДн делятся на следующие категории:

5.2.1. Администратор ИСПДн – работник Фонда, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечным пользователям (Операторам ИСПДн) к элементам системы, хранящим персональные данные.

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 к техническим средствам обработки информации и средствам защиты;

- обладает возможностями внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

5.2.2. Оператор ИСПДн – работник Фонда, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор 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. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Построение системы обеспечения безопасности ПДн в ИСПДн Фонда ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

6.1.1. Законность

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

Пользователи ИСПДн Фонда должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение требований данного порядка.

6.1.2. Системность

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

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

6.1.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств для построения целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

6.1.4. Непрерывность защиты ПДн

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

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

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты.

6.1.5. Своевременность

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

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

6.1.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требованиях по защите, достигнутом отечественном и зарубежном опыте в этой области.

6.1.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко определен или сведен к минимуму.

6.1.8. Принцип минимизации полномочий

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

Доступ к ПДн должен предоставляться только в тех целях и объемах, которые необходимы работнику для выполнения его должностных обязанностей.

6.1.9. Взаимодействие и сотрудничество

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

В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие сотрудникам, ответственным за защиту информации.

6.1.10. Гибкость системы защиты ПДн

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

осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

6.1.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже разработчикам системы). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

6.1.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий операторов и администраторов ИСПДн.

6.1.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности ПДн и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

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

6.1.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Администрации.

6.1.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ

7.1. Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

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

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

7.1.1. Законодательные (правовые) меры защиты.

К правовым мерам защиты относятся правила обращения с персональными данными, установленные действующими в стране нормативно-правовыми актами, которые, закрепляют права и обязанности участников информационных отношений, а также устанавливают ответственность за нарушения этих правил. Правовая база создает препятствия неправомерному использованию ПДн и является сдерживающим фактором для потенциальных нарушителей.

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

7.1.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения вычислительной техники в стране. 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.

7.1.3. Организационные(административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, 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.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику безопасности ПДн, отражающую подходы к защите ПДн, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики безопасности ПДн в ИСПДн состоит из мер административного уровня и организационных (процедурных) мер защиты ПДн.

К административному уровню относятся решения руководства, затрагивающие функционирование ИСПДн в целом. Эти решения закрепляются в Политике безопасности ПДн. Примером таких решений могут быть:

- назначение Администратора информационной безопасности;
- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, назначение сотрудников, ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Фонда в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

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

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

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности ПДн, а также их ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать порядок 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 другими защитными механизмами;
- организовать меры противодействия НСД пользователей на этапах аутентификации, авторизации, идентификации, обеспечивающие гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

- регламентации доступа в помещения ИСПДн;
- порядка допуска работников к использованию ресурсов ИСПДн Фонда;
- регламентации процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламентации процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
- принятия инструкции Администратора информационной безопасности.
- принятия инструкций пользователей ИСПДн (Администратора ИСПДн, Оператора ИСПДн).

7.1.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств, 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 системы охраны, включающую посты охраны, технические средства охраны, которая всеми способами, предотвращает или существенно затрудняет проникновение в здания, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, а также исключает нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

7.1.5. 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;

- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов, изложенных в разделе 5, предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый работник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн Фонда разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся в строго установленном порядке (регистрируются и контролируются);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- специалистами Фонда осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

8. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИСПДн

8.1. Контроль эффективности СЗПДн Фонда должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

8.2. Контроль может проводиться как Администратором информационной безопасности, Администраторами ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

8.3. Контроль может осуществляться Администратором информационной безопасности, Администраторами ИСПДн как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

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

9. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПДн

9.1. Сотрудники, ответственные за обработку персональных данных с использованием средств автоматизации или без использования таких средств в структурных подразделениях Фонда назначаются приказом директора Фонда (или лицом его замещающим).

9.2. Сфера ответственности руководителей структурных подразделений Фонда включает следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, положений, регламентов, инструкций и других организационных документов по обеспечению безопасности ПДн;
- обучение и информирование пользователей ИСПДн о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

10. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ

10.1. Под нарушителем в Фонде понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб элементам ИСПДн, подлежащим защите (раздел 4).

10.2. Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

11. ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Угрозы информационной безопасности и их источники

11.1.1. Наиболее опасными (значимыми) угрозами ИСПДн Фонда (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную информацию ограниченного распространения, а также персональных данных;
- нарушение работоспособности (дезорганизация работы) ИСПДн Фонда, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов ИСПДн Фонда, а также фальсификация (подделка) документов.

11.1.2. Основными источниками угроз информационной безопасности в ИСПДн Фонда являются:

- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований ИБ и другие действия сотрудников (в том числе администраторов средств защиты) структурных подразделений Фонда при эксплуатации ИСПДн, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих мест, подсистем или ИСПДн Фонда в целом;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом) действия сотрудников структурных подразделений Фонда, допущенных к работе с ИСПДн, а также сотрудников структурных подразделений, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения ИБ;
- воздействия из других логических и физических сегментов ИСПДн Фонда со стороны сотрудников других структурных подразделений Фонда, а также удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего Internet) через легальные и несанкционированные каналы подключения сети Фонда к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам ИСПДн Фонда;
- деятельность международных и отечественных преступных групп, и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и ее отдельных компонент;
- деятельность иностранных разведывательных и специальных служб, направленная против интересов Фонда и Российской Федерации в целом;
- ошибки, допущенные при проектировании ИСПДн Фонда и ее системы защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств ЗИ и контроля эффективности защиты) ИСПДн Фонда;
- пожары, аварии, стихийные бедствия и другие случаи форс-мажорных обстоятельств.

11.2. Пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности в ИСПДн Фонда

11.2.1. Пользователи, операторы, системные администраторы и сотрудники Фонда, обслуживающие систему, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

11.2.2. Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИСПДн Фонда (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) и

меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 11.2.2.

Таблица 11.2.2.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИСПДн	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Действия сотрудников Фонда, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств; отключению оборудования или изменению режимов работы устройств и программ; разрушению ИР системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и подобное)	1. Организационные меры (регламентация действий, введение запретов). 2. Применение физических средств, препятствующих неумышленному совершению нарушения. 3. Применение технических (аппаратно-программных) средств разграничения доступа к ресурсам. 4. Резервирование критичных ресурсов.
Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и подобное)	1. Организационные меры (удаление всех потенциально опасных программ с дисков АРМ). 2. Применение технических (аппаратно-программных) средств разграничения доступа к технологическим и инструментальным программам на дисках АРМ.
Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и подобное)	1. Организационные меры (введение запретов). 2. Применение технических (аппаратно-программных) средств, препятствующих несанкционированному внедрению и использованию неучтенных программ.
Непреднамеренное заражение компьютера вирусами	1. Организационные меры (регламентация действий, введение запретов).

	2. Технологические меры (применение специальных программ обнаружения и уничтожения вирусов). 3. Применение аппаратно-программных средств, препятствующих заражению компьютеров компьютерными вирусами.
Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ключей ЭЦ, идентификационных карточек, пропусков)	1. Организационные меры (регламентация действий, введение запретов, усиление ответственности). 2. Применение физических средств обеспечения сохранности указанных реквизитов.
Игнорирование организационных ограничений (установленных правил) при работе в системе	1. Организационные меры (усиление ответственности и контроля). 2. Использование дополнительных физических и технических средств защиты.
Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом, ответственным за ИБ	Организационные меры (обучение персонала, усиление ответственности и контроля).
Ввод ошибочных данных	1. Организационные меры (усиление ответственности и контроля). 2. Технологические меры контроля за ошибками операторов ввода данных.

11.3. Умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала.

11.3.1. Основные возможные пути умышленной дезорганизации работы, вывода ИСПДн Фонда из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.) и меры по нейтрализации соответствующих угроз и снижению возможного наносимого ими ущерба приведены в Таблице 11.3.1.

Таблица 11.3.1

Основные возможные пути умышленной дезорганизации работы, вывода ИСПДн из строя, проникновения в систему к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.)	Меры по нейтрализации угроз и снижению возможного наносимого ущерба
Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы	1. Организационные меры (регламентация действий, введение запретов). 2. Применение физических средств,

(устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)	препятствующих неумышленному совершению нарушения. 3. Резервирование критичных ресурсов. 4. Обеспечение личной безопасности сотрудников.
Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность), вербовка (путем подкупа, шантажа, угроз и т.п.) пользователей, имеющих определенные полномочия по доступу к защищаемым ресурсам	Организационные меры (подбор, расстановка и работа с кадрами, усиление контроля и ответственности). Автоматическая регистрация действий персонала.
Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)	Организационные меры (организация хранения и использования носителей с защищаемой информацией).
Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств	1. Организационные меры (организация хранения и использования носителей с защищаемой информацией). 2. Применение технических средств разграничения доступа к защищаемым ресурсам и автоматической регистрации получения твердых копий документов.
Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.) с последующей маскировкой под зарегистрированного пользователя	1. Организационные меры (регламентация действий, введение запретов, работа с кадрами). 2. Применение технических средств препятствующих внедрению программ перехвата паролей, ключей и других реквизитов.
Несанкционированное использование АРМ пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.	1. Организационные меры (строгая регламентация доступа в помещения и допуска к работам на данных АРМ). 2. Применение физических и технических средств разграничения доступа.
Несанкционированная модификация	1. Организационные меры

программного обеспечения - внедрение программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования системы	(строгая регламентация допуска к работам). 2. Применение физических и технических средств разграничения доступа и препятствующих несанкционированной модификации аппаратно-программной конфигурации АРМ. 3. Применение средств контроля
Перехват данных, передаваемых по каналам связи, и их анализ с целью получения конфиденциальной информации и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему	1. Физическая защита каналов связи. 2. Применение средств криптографической защиты передаваемой информации. 3. Применение средств электронной подписи (ЭП)
Вмешательство в процесс функционирования ИСПДн из сетей общего пользования с целью несанкционированной модификации данных, доступа к конфиденциальной информации, дезорганизации работы подсистем и т.п.	1. Организационные меры (регламентация подключения и работы в сетях общего пользования). 2. Применение специальных технических средств защиты (межсетевых экранов, средств контроля защищенности и обнаружения атак на ресурсы системы и т.п.).

11.4. Утечка информации по техническим каналам

11.4.1. При проведении мероприятий и эксплуатации технических средств Фонда возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств ИСПДн Фонда и линий передачи информации;
- наводки информативного сигнала, обрабатываемого ИСПДн Фонда, на провода и линии, выходящие за пределы контролируемой зоны, в том числе на цепи заземления и электропитания;
- изменения тока потребления, обусловленные обрабатываемыми ИСПДн Фонда информативными сигналами;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав ИСПДн Фонда, или при наличии паразитной генерации в узлах (элементах) ИСПДн;
- электрические сигналы или радиоизлучения, обусловленные воздействием на ИСПДн Фонда высокочастотных сигналов, создаваемых с помощью разведывательной

аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом (облучение, "навязывание");

- радиоизлучения или электрические сигналы от внедренных в ИСПДн Фонда и выделенные помещения специальных электронных устройств перехвата информации ("закладок"), модулированные информативным сигналом;

- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации (телеграф, телетайп, принтер, пишущая машинка и т.п.);

- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

- просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств ЗИ, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства ("закладки").

11.4.2. Перехват информации ограниченного распространения или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов ИСПДн Фонда, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими структурных подразделений Фонда, а также с помощью скрытно устанавливаемой в районах важнейших объектов и на их территориях автономной автоматической аппаратуры.

11.4.3. В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

- космические средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации ("закладок");

- стационарные средства, размещаемые в зданиях;

- портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, ведущими разведку;

- автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

11.4.4. Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям,

коммуникациям и сооружениям. Портативные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы контролируемой территории.

11.4.5. Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна вследствие:

- непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;
- случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов дисплеев и других средств ее отображения.

11.5. Неформальная модель возможных нарушителей:

Нарушитель - лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и подобное).

Система защиты ИСПДн Фонда должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

"Неопытный (невнимательный) пользователь" - сотрудник Фонда, зарегистрированный как пользователь системы, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам ИСПДн Фонда с превышением своих полномочий, ввода некорректных данных и подобные действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

"Любитель" - сотрудник Фонда, зарегистрированный как пользователь системы), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из "спортивного интереса". Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей, средств доступа других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные

средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

"Мошенник" - сотрудник ИСПДн Фонда, зарегистрированный как пользователь системы, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого сотрудника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

"Внешний нарушитель (злоумышленник)" - постороннее лицо или сотрудник Фонда, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения ИБ, методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети ИСПДн Фонда.

"Внутренний злоумышленник" - сотрудник Фонда, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками Фонда. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне - из сетей общего пользования.

11.6. Внутренним нарушителем может быть лицо из следующих категорий персонала Фонда:

- зарегистрированные конечные пользователи ИСПДн Фонда (сотрудники структурных подразделений);
- сотрудники структурных подразделений, не допущенные к работе с ИСПДн Фонда (обслуживающий персонал, в том числе водители и т.п.);
- персонал, обслуживающий технические средства ИСПДн Фонда;
- технический персонал, обслуживающий офисное здание (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИСПДн Фонда);
- руководители и специалисты различных уровней.

11.7. Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники Фонда;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности Фонда (энерго-, водо-, теплоснабжения и т.п.);
- посетители;

- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

- лица, случайно или умышленно проникшие в сети ИСПДн Фонда из внешних (по отношению к Фонда) сетей телекоммуникации (хакеры).

11.8. Пользователи и обслуживающий персонал из числа сотрудников Фонда имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

11.9. Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в Фонде знания и опыт выделяют их среди других источников внешних угроз.

11.10. Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников Фонда всеми доступными им силами и средствами.

11.11. Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в Фонде. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками Фонда и криминальными структурами.

11.12. Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к ИР. Криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к защищаемой информации в Фонда.

11.13. Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей - сотрудников Фонда по преодолению системы защиты;

- нарушитель скрывает свои несанкционированные действия от других сотрудников;

- несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

12. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

12.1. Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

13. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

13.1. Реализация Концепции безопасности ПДн, обрабатываемых в ИСПДн Фонда позволит:

- оценить состояние безопасности ПДн, выявить источники внутренних и внешних угроз безопасности ПДн, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести классификацию ИСПДн;
- провести определения уровня защищенности персональных данных при их обработке в ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности элементов ИСПДн, подлежащих защите.

13.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы защиты персональных данных и создаст условия для ее дальнейшего совершенствования.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Концепция вступает в силу с момента ее утверждения приказом директора Фонда.

14.2. Настоящая Концепция подлежит изменению и дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

14.3. При приеме на работу новых сотрудников отделом правовой и кадровой работы осуществляется обязательное ознакомление с настоящей Концепцией.

14.4. Настоящая Концепция является общедоступным внутренним документом Фонда, и подлежит размещению на официальном сайте Фонда.

14.5. Контроль исполнения требований настоящей Концепции осуществляется ответственным лицом за обеспечение безопасности персональных данных Фонда.

14.6. Ответственность должностных лиц Фонда, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и

защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Фонда.

Согласовано:

Начальник отдела правовой
и кадровой работы _____ Ускачева Е.М.

Начальник отдела информационно-
технического обеспечения _____ Охлупин В.В.

Лист ознакомления
с Концепцией безопасности персональных данных,
обрабатываемых в информационных системах персональных данных
НО «Фонд капитального ремонта МКД в ЯНАО»,
утвержденной приказом от ___ _____ 2015 г. № _____

№ п/п	ФИО	Личная подпись	Дата ознакомления