УТВЕРЖДАЮ:
Директор Благотворительного фонда
“Солнечный город”
_____ Аксенова М.А.
“ 16 ” ноября 2021 г.

Политика информационной безопасности информационных ресурсов автоматизированной системы Благотворительного фонда “Солнечный город” (БФ «Солнечный Город»)

г. Новосибирск, 2021

Список используемых сокращений:

АРМ	Автоматизированное рабочее место обработки информации
АС	Автоматизированная система
ГОСТ	Государственный стандарт
НСД	Несанкционированный доступ
ИБ	Информационная безопасность
ИР	Информационные ресурсы
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПС	Программные средства
ПЭВМ	Персональная ЭВМ
ФСБ РФ	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Определения

Администрация сайта – сотрудники Фонда уполномоченные на управление сайтом Фонда, которые организуют и/или осуществляют обработку ПДн пользователей, а также определяют цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

АС обработки информации (АС) - организационно- техническая система, представляющая собой совокупность: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего ПО, массивов данных на различных носителях, сотрудников и пользователей, выполняющих автоматизированную обработку персональных данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных потребителей информации.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. АРМ объединяет программно-аппаратные средства, обеспечивающие взаимодействие человека с компьютером.

Авторизация- предоставление прав доступа.

Авторизованный субъект доступа - субъект, которому предоставлены соответствующие права доступа к объектам системы.

Аутентификация (подтверждение подлинности)- процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введённого им пароля с паролем, сохраненным в базе.

Безопасность субъектов информационных отношений - защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

Безопасность АС (компьютерной системы) - защищенность АС от несанкционированного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

Безопасность информационного ресурса (в частности АС) - складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность заключается в том, что ресурс доступен только тем субъектам доступа, которым предоставлены на то соответствующие полномочия.

Целостность, что ресурс может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией неизменности и работоспособности ресурса в любой момент времени.

Доступность информационного ресурса означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к нему.

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.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Вредоносная программа - программа, предназначенная для несанкционированного доступа и/или воздействия на ПДн или ресурсы ИСПДн

Документ - зафиксированная на материальном носителе (бумага, магнитный диск и т.п.) информация с реквизитами, позволяющими ее идентифицировать, при этом, документирование информации является обязательным условием включения информации в информационные ресурсы.

Доступ к информации - возможность получения информации и ее обработки, модификация или уничтожение.

Доступность информации - способность системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Доступ к ресурсу - получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

Защита информации от несанкционированного доступа (НСД) - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации, прав или правил доступа к защищаемой информации.

Идентификация (опознавание) - установление тождественности неизвестного объекта известному на основании совпадения признаков.

Информация в АС - сведения о лицах, фактах, событиях, процессах и явлениях в предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

Информационная безопасность (ИБ) - защищенность информации, в том числе ПДн от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Информационная система -совокупность содержащейся в базах данных информации, информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн)- информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также

информационные технологии и технические средства, позволяющие осуществлять обработку таких ПДн.

Информационные ресурсы - отдельные документы и отдельные массивы документов в информационных системах.

Конфиденциальность ПДн - обязательное для соблюдения Фондом или иным получившим доступ к ПДн лицом требование не допускать распространения ПДн без согласия субъекта ПДн или наличия иного законного основания.

Лицензия в области защиты информации - разрешение на право проведения тех или иных работ в области защиты информации (в соответствии с Постановлением Правительства РФ от 15.08.2006 № 504 “О лицензировании деятельности по технической защите конфиденциальной информации” и Постановлением правительства РФ от 31.08.2006 г. № 532 “О лицензировании деятельности по разработке и (или)производству средств защиты конфиденциальной информации").

Межсетевой экран - программный элемент, реализующий контроль за информацией, поступающей в ИСПДн и/или выходящей из информационной системы

Морально-этические меры защиты информации - традиционно сложившиеся в обществе нормы поведения и правила обращения с информацией. Эти нормы не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, репутации человека, группы лиц или организации. Морально-этические нормы бывают как неформальные (например, общепризнанные нормы честности и т.п.), так и оформленные в некоторый свод правил или предписаний.

Нарушитель безопасности ПДн и ИР - это лицо, 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.

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ (НСД) - доступ субъекта к информации или действия с информацией в нарушение установленных в системе правил разграничения доступа.

Обработка информации в АС - совокупность операций (сбор, запись, систематизация, накопление, хранение, уточнение, преобразование, использование, отображение, передача, обезличивание, удаление, уничтожение и т.п.), осуществляемых над информацией с использованием средств АС.

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 ПДн.

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.

Объект - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

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

Организационные меры защиты- меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность сотрудников, а также порядок взаимодействия пользователей с системой таким образом, чтобы затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Пароль - набор символов (цифры, буквы, прочие символы) который известен узкому кругу лиц или одному лицу необходимый для ограничения доступа к информации.

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

Политика информационной безопасности (Политика ИБ) - документация, определяющая цели, содержание и основные направления деятельности по ИБ, предназначенная для Фонда.

Пользователь АС и ИСПДн - субъект информационных отношений, пользующейся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Пользователь сайта Фонда - лицо, имеющее доступ к сайту Фонда через IP-адрес (уникальный сетевой адрес узла в компьютерной сети), посредством информационно-телекоммуникационной сети Интернет и использующее информацию, и материалы сайта Фонда в личных, профессиональных, ознакомительных и иных целях.

Правовые меры защиты информации- действующие в РФ законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Рабочая станция- комплекс аппаратных и программных средств, предназначенных для решения определённого круга задач.

Разграничение доступа к ресурсам АС - это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Сайт Фонда- совокупность связанных между собой веб-страниц, размещенных в информационно-телекоммуникационной сети Интернет с доменным именем https://sgdeti.ru , включая его поддомены. На сайте используется протокол https для защиты данных.

Система защиты АС - совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности АС (циркулирующей в АС информации).

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

Субъект - пользователь или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект информационных отношений - государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

Технические средства ИСПДн - средства вычислительной техники, специальные программы, средства и системы передачи, приема и обработки ПДн, программные средства и входящие в состав АС, которые выполняют функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, и т.д.).

Угроза безопасности ПДн - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного (неумышленного) доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн.

Естественные угрозы - это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

Искусственные угрозы - это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить: непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АС и ее элементов, ошибками в ПО, ошибками в действиях персонала и т.п.; преднамеренные (умышленные) угрозы, связанные с корыстными целями нарушителей.

Угроза автоматизированной системе - потенциально возможное событие, действие или процесс, которое может привести к нанесению ущерба ресурсам АС.

Угроза информационной безопасности - случайное (неумышленное) или преднамеренное (умышленное) воздействие, приводящее к нарушению целостности, доступности и конфиденциальности информации, которое наносит ущерб собственнику или пользователю информации.

Информационные способы нарушения ИБ включают: противозаконный сбор, распространение и использование информации; манипулирование информацией (дезинформация, сокрытие или искажение информации); незаконное копирование информации (данных и программ); незаконное уничтожение информации; хищение информации из баз данных; нарушение адресности и оперативности информационного обмена; нарушение технологии обработки данных и информационного обмена.

Программно-математические способы нарушения ИБ включают: внедрение программ-вирусов; внедрение программных “закладок” как на стадии проектирования системы, так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия

по отношению к информации и системам ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.)

Физические способы нарушения ИБ включают: уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи; хищение средств защиты информации от несанкционированного доступа; воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз ИБ.

Организационно-правовые способы нарушения ИБ включают: закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий; невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области информационной безопасности.

Физические меры защиты - это разного рода механические, электро- или электронно-механические устройства и сооружения, предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к АС и защищаемой информации, а также технические средства наблюдения, связи и охранной сигнализации.

1. Введение

Развитие и распространение информационных технологий требуют создания целостной системы информационной безопасности, взаимоувязывающей правовые, оперативные, технологические, организационные, технические и физические меры защиты информации.

Настоящая Политика информационной безопасности (далее- Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности информационных ресурсов (далее- ИР) в частности персональных данных (далее-ПДн), обрабатываемых в информационной системе персональных данных (далее- ИСПДн) Детского благотворительного фонда “Солнечный город” (далее- Фонд).

2. Общие положения

2.1 Назначение документа

В Политике определены порядок и цели получения, учета, накопления, обработки, хранения и защиты ПДн, требования к пользователям ИСПДн, перечень субъектов и обрабатываемых персональных данных, степень ответственности пользователей, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников Фонда, ответственных за обеспечение безопасности ИР в автоматизированной системе (далее-АС) и ПДн в ИСПДн Фонда.

Целью настоящей Политики является обеспечение безопасности (конфиденциальности, целостности и доступности) ИР в АС и ИСПДн от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Безопасность ИСПДн достигается путем исключения несанкционированного и/или случайного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн.

Конфиденциальность информации - обработка, хранение и передача информации осуществляется только авторизованными пользователями, которые обязаны не передавать информацию, полученную в результате осуществления должностных обязанностей, третьим лицам без согласия ее обладателя.

Целостность информации- состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только по необходимости.

Доступность информации -доступ в установленном порядке авторизованных пользователей.

Настоящая Политика утверждается приказом директора Фонда и подлежит пересмотру по мере необходимости.

Положения настоящей Политики распространяются на весь объем ПДн и иной конфиденциальной информации, обрабатываемых в Фонде, полученных как до, так и после вступления Политики в силу.

2.2 Правовая основа документа

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Также правовой основой настоящей Политики являются:

- Конституция Российской Федерации;
- Гражданский и Уголовный кодексы;
- Кодекс об административных правонарушениях;

- законы, указы, постановления и другие нормативные документы в области обработки информации и информационной безопасности действующего законодательства Российской Федерации;

- нормативные и регламентирующие документы государственных органов Российской Федерации (ФСТЭК, ФСБ, Роскомнадзор и др.);

- внутренние нормативно-методические и организационно-распорядительные документы Фонда.

Основные положения и требования Политики распространяются на всех сотрудников Фонда (штатных, временных, работающих по контракту) и все структурные подразделения Фонда, в которых осуществляется автоматизированная и смешанная обработка информации, содержащей сведения, составляющие персональные данные, а также на лиц или организации, осуществляющие сопровождение, обслуживание и обеспечение работы АС.

3. Информация об операторе

Полное название: Благотворительный фонд “Солнечный город”

Фактический адрес: г. Новосибирск, ул. Гоголя 15, этаж 7

Телефон: +7 (383) 208 1117

E-mail: office@suncitylife.ru

ИНН 5401292310

ОГРН 1075400004195

Сайт: https://sgdeti.ru

Обработка персональных данных осуществляется с передачей по информационно-телекоммуникационной сети Интернет.

Фонд не осуществляет трансграничную передачу ПДн субъектов ПДн.

4. Цели обработки информации и ПДн

Обработка информации и ПДн осуществляется в следующих целях:

- исполнения положений нормативных правовых актов, регулирующих сбор, хранение и обработку персональных данных (пункт 2.2 Политики)

- подбора и найма сотрудников; организации кадровой работы Фонда и его структурных подразделений; исполнения положений трудового и налогового законодательства РФ;

- защиты жизни, здоровья и иных жизненно важных интересов субъектов ПДн;

- заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическими и иными лицами; проверка добросовестности контрагента до заключения договора;

- ведение работы (анализ, диагностика, тестирование, анкетирование, консультации и т.п.) с письменными и устными обращениями физических, юридических и иных лиц по вопросам, связанным с уставной деятельностью Фонда;

- идентификация пользователя, зарегистрированного на сайте Фонда для его дальнейшей авторизации;

- установления с пользователем обратной связи, включая направление уведомлений, запросов, ответов, результатов работы Фонда;

- формирования базы кандидатов в замещающие родители и детей для дальнейшего содействия устройству детей сирот и детей, оставшихся без попечения родителей;

- предоставление пользователю с его согласия новостной рассылки или специальных предложений от имени Фонда;

-подтверждения достоверности (полноты, точности, адекватности, целостности) предоставленной информации физическими, юридическими и иными лицами;

- создания учетной записи Пользователя для целевого использования частей сайта Фонда в рамках проводимых мероприятий, акций или программ Фонда;

- предоставление Пользователю эффективной технической поддержки.

5. Объекты защиты

Основными объектами системы ИБ в Фонде являются:

- ИР с ограниченным доступом, составляющие ПДн физических лиц, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и ПС ее обработки, передачи и отображения, в том числе каналы информационного обмена, системы и средства защиты информации;
- процессы обработки информации в АС, которые включают информационные технологии, процедуры сбора, обработки, хранения, накопления и передачи информации, объекты и помещения в которых размещены компоненты АС.

5.1 Цель создания и эксплуатации АС

АС предназначена для автоматизации деятельности сотрудников Фонда и иных лиц, взаимодействующих с Фондом в рамках деятельности Фонда.

Создание и применение АС преследует следующие цели:

- повышение качества управления процессами, связанными с деятельностью Фонда;
- повышение качества контроля движения ИР Фонда;
- повышение оперативности, полноты и достоверности сбора и обработки информационных данных;
- сокращение временных затрат на поддержку внутреннего и внешнего документооборота;
- обеспечение интегрированной обработки информации, формирования и ведения баз данных;
- обеспечение взаимодействия с клиентами Фонда и пользователями сайта, и другими сторонними организациями.

5.2 Структура, состав АС, информационные связи с другими объектами

АС представляет собой системы, связанные между собой посредством информационно-телекоммуникационной сети Интернет.

В АС циркулирует информация разных категорий. Конфиденциальная информация и ПДн могут совместно использоваться различными пользователями АС.

В АС предусмотрено взаимодействие с внешними (государственными, коммерческими, некоммерческими) организациями, физическими лицами посредством информационно-телекоммуникационной сети Интернет.

Комплекс технических средств АС Фонда включает средства обработки данных (персональный компьютер, сервера баз данных, файловые сервера и т.п.), средства обмена данными с возможностью выхода в глобальные сети (кабельная система, шлюзы, модемы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

Особенности функционирования АС:

- объединение в единую систему разнообразных технических средств обработки и передачи информации;
- объединение в базах данных информации различного назначения, принадлежности и уровней конфиденциальности;

- доступ к вычислительным и информационным ресурсам различных категорий пользователей (источников и потребителей информации);
- наличие каналов взаимодействия с внешними источниками и потребителями информации.

Общая структурная и функциональная организация АС определяется правилами Фонда и задачами, решаемыми субъектами информационных отношений в зависимости от их роли в Фонде с применением средств автоматизации.

Объекты информатизации АС включают:

- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
- информационные ресурсы, в том числе содержащие ПДн и представленные в виде документов или записей в массивах и базах данных;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное ПО);
- автоматизированные системы связи и передачи данных (средства телекоммуникации);
- служебные помещения, в которых обрабатывается информация, в том числе ПДн.

5.3 Категории информационных ресурсов, подлежащих защите

В АС Фонда хранится и обрабатывается информация различных уровней конфиденциальности, а также общедоступные ПДн и сведения.

Фонд осуществляет сбор, хранение и обработку общих (ФИО, телефон, дата рождения, и т.д.), специальных (наличие детей, супружеский статус, жилищные условия, состояние здоровья и т.д.) и биометрических (фотографий) ПДн сотрудников, пользователей и иных лиц, взаимодействующих с Фондом в рамках его уставной деятельности.

Сбор, хранение и обработка ПДн осуществляется с письменного согласия субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие данное в электронном виде, путем заполнения чек-бокса под политикой конфиденциальности, договором оферты или формой для сбора ПДн, размещенных на сайте Фонда.

Согласие в письменной форме субъекта ПДн на обработку его ПДн включает в себя:

- ФИО, адрес электронной почты или почтовый адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

-ФИО, адрес электронной почты или почтовый адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;

- наименование или ФИО; адрес оператора (место регистрации, место жительства или место пребывания), ИНН, ОГРН, сайт оператора, получающего согласие субъекта (представителя субъекта);

- цель обработки ПДн;

- перечень ПДн, на обработку которых субъект (представитель субъекта) дает согласие;

- наименование или ФИО, место регистрации, место жительства или место пребывания, ИНН, ОГРН, сайт лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;

- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва;

- подпись субъекта ПДн.

Фонд обязуется не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством РФ и договором с субъектом (представителем субъекта).

6. Система защиты ИР в АС и ПДн

Система защиты ПДн, построена на основании: результатов проведения внутренней проверки; перечня информации и ПДн, подлежащих защите; акта классификации ИСПДн; модели угроз безопасности информации и ПДн; руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности информации и ИСПДн Фонда. На основании анализа актуальных угроз безопасности делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности информации и ИСПДн. Выбранные необходимые мероприятия отражаются в плане мероприятий по обеспечению защиты информации и ИСПДн.

Система защиты информации и ИСПДн включает следующие средства:

-HTTPS протокол сайта

-систему управления доступом, регистрации и учета;

-систему обеспечения целостности и доступности;

- антивирусные средства защиты;

- средства межсетевого экранирования;

- средства обнаружения вторжений;

-средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

7. Цели и задачи обеспечения информационной безопасности

7.1 Интересы субъектов информационных отношений

Субъектами правоотношений при использовании АС и обеспечении информационной безопасности являются:

- Фонд, как собственник информационных ресурсов;
- сотрудники Фонда, как пользователи и поставщики информации в АС;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в АС;
- другие юридические и физические лица, привлекаемые для создания и обеспечения работы АС (разработчики компонентов АС, обслуживающий персонал, IT-специалисты и организации, привлекаемые для оказания услуг в области информационной безопасности, информационных технологий и др.)

Субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации;
- своевременного доступа к необходимой им информации;
- возможности осуществления контроля и управления процессами обработки и передачи информации.

7.2 Цели защиты АС и ИСПДн

Основной целью обеспечения ИБ в Фонде является защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании АС) от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного воздействия на информацию, ее носители, процессы обработки и передачи, разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования, а также минимизации других рисков (риск нанесения урона репутации Фонда, правовой риск и т.д.)

7.3 Задачи защиты АС и ИСПДн

Для достижения основной цели защиты система безопасности АС обеспечивает решение следующих задач:

- защиту от НСД в процесс функционирования АС посторонних лиц (доступ к ресурсам АС должны иметь только авторизованные, зарегистрированные сотрудники Фонда и пользователи);
- разграничение доступа зарегистрированных и авторизованных пользователей к аппаратным, программным и информационным ресурсам АС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС);
- регистрацию действий авторизованных пользователей при использовании ИР АС Фонда;
- защиту от несанкционированной модификации АС и от внедрения несанкционированных и/или вредоносных программ в АС;
- защиту ПДн от утечки, несанкционированного разглашения или искажения при их обработке, хранении и передачи;
- обеспечение аутентификации авторизованных пользователей, участвующих в информационном обмене;
- своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации ущерба, наносимого неправомерными действиями нарушителей.

7.4 Основные пути достижения целей защиты и решения задач ИБ

Основные цели защиты и решение задач ИБ достигаются посредством:

- учета всех подлежащих защите ресурсов АС (информации, систем управления базами данных и другого системного и прикладного ПО, каналов связи, серверов, АРМ);
- доступности информации и операций с ней только для зарегистрированных пользователей;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой АС и передаваемой по каналам связи;
- обеспечения целостности и достоверности информации, хранимой и обрабатываемой в АС и передаваемой по каналам связи;
- наделения сотрудников Фонда минимально необходимыми для выполнения ими своих функциональных обязанностей полномочиями в соответствии с уровнем доступа к информационным ресурсам Фонда;
- соблюдения сотрудниками, использующими АС и лицами, обслуживающими АС требований и правил Фонда, регулирующих вопросы обеспечения информационной безопасности;
- персональной ответственности субъектов информационных отношений за нарушения требований и правил, регулирующих вопросы обеспечения информационной

безопасности, повлекшие за собой ущерб для субъекта или нескольких субъектов информационных отношений;

- регламентации процессов обработки подлежащей защите информации и действий сотрудников Фонда, использующих АС, а также действий лиц, осуществляющих обслуживание и модификацию АС;
- принятия мер обеспечения физической целостности и защищенности АС;
- применения физических и программных средств защиты ресурсов ИСПДн;
- юридической защиты интересов субъектов информационных отношений при взаимодействии с внешними организациями (связанном с обменом информацией) от противоправных действий как со стороны этих организаций, так и от несанкционированных действий третьих лиц;
- проведения постоянного анализа эффективности и достаточности применяемых мер и средств защиты информации, разработки и реализации предложений по совершенствованию мер системы защиты информации.

8. Основные угрозы информационной безопасности АС

8.1 Угрозы информационной безопасности и их источники

Угрозы безопасности информации по природе их возникновения можно разделить на два типа: естественные (объективные) и искусственные (субъективные).

Естественные угрозы - угрозы, вызванные воздействием на АС объективных физических процессов техногенного характера (аварии, неисправности, сбои) или стихийных природных явлений, которые от человека не зависят.

Искусственные угрозы - угрозы, вызванные действиями человека.

Основными источниками угроз информационной безопасности АС являются:

- непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения порядка сбора, обработки и передачи информации, а также требований ИБ, приводящие к разглашению ПДн и иных сведений ограниченного распространения;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников Фонда, допущенных к работе с АС, а также лиц, привлекаемых для обслуживания АС;
- удаленное несанкционированное вмешательство посторонних лиц из информационно-телекоммуникационной сети Интернет через легальные и несанкционированные каналы подключения сети Фонда к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам АС;
- деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и её отдельных компонентов;
- ошибки, допущенные при проектировании АС и её системы защиты, ошибки в ПО, отказы и сбои технических средств АС;
- аварии, стихийные бедствия и т.п.

Наиболее значимые угрозы безопасности информации:

- нарушение целостности (искажение, подмена, уничтожение) ИР Фонда, фальсификация документов;
- нарушение конфиденциальности (утечка, разглашение) ПДн.

Пользователи, IT-специалисты, привлекаемые Фондом для обслуживания АС и сотрудники Фонда, являются внутренними источниками случайных воздействий, т.к. имеют

непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил.

8.2 Пути реализации непреднамеренных искусственных угроз информационной безопасности в АС

Основные пути реализации непреднамеренных субъективных угроз АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному нарушению работы АС или разрушению ИР в АС (порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.);
- разглашение, передача или утрата атрибутов разграничения доступа (логинов, паролей и т.п.);
- несанкционированный запуск программ, осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- несанкционированное использование неучтенных программ (игровых, обучающих 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 т.п.);
- непреднамеренное заражение компьютера вирусами;
- пересылка данных и документов по ошибочному адресу;
- ввод ошибочных данных;
- игнорирование установленных правил и ограничений при работе в АС.

Меры по нейтрализации непреднамеренных искусственных угроз:

- организационные меры (регламентация действий, введение ограничений и запретов, удаление опасных программ, усиление ответственности и контроля, обучение);
- резервирование критичных ресурсов;
- применение физических средств, препятствующих нарушению;
- применение технических (аппаратно-программных) средств для разграничения доступа к информационным ресурсам, технологическим и инструментальным программам, а также препятствующих несанкционированному внедрению и использованию неучтенных программ;
- использование специальных программ обнаружения и уничтожения вирусов.

8.3 Пути реализации преднамеренных искусственных угроз ИБ

Основные пути реализации преднамеренных субъективных угроз АС (действия, совершаемые людьми умышленно с корыстными целями, по принуждению и т.п.):

- умышленные действия, приводящие к частичному или полному нарушению работы АС или разрушению ИР АС (порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, умышленная порча носителей информации и т.п.);
- несанкционированное копирование конфиденциальной информации на внешние носители или передача её при помощи средств телекоммуникаций (электронная почта, Internet и т.п.)
- умышленное искажение информации, ввод заведомо неверных данных;
- перехват данных, передаваемых по каналам связи и их анализ с целью получения конфиденциальной информации;
- хищение носителей информации (распечаток документов, записей, микросхем памяти и т.п.)

- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора и т.п.);

- несанкционированный доступ к информационным ресурсам АС Фонда с АРМ сотрудников Фонда;

- несанкционированная модификация ПО (внедрение программных “закладок”) с целью скрытно осуществлять доступ к информационным ресурсам Фонда;

- применение подслушивающих устройств, дистанционная фото- и видео съемка для несанкционированного получения информации.

Меры по нейтрализации преднамеренных искусственных угроз:

- организационные меры (строгая регламентация допуска, введение запретов, подбор квалифицированного персонала, усиление ответственности и контроля, обучение, организация хранения носителей информации);
- обеспечение личной безопасности сотрудников;
- резервирование критичных ресурсов;
- применение физических средств, препятствующих нарушению;
- применение специальных технических средств защиты (межсетевых экранов, средств контроля защищенности и т.п.);
- применение средств криптографической защиты (шифрования) передаваемой информации;
- регистрация получения твердых копий документов с наиболее критичной информацией;
- регистрация и анализ использования средств телекоммуникаций, оперативное реагирование на несанкционированные действия;
- применение технических (аппаратно-программных) средств для разграничения доступа к информационным ресурсам;
- использование специальных программ препятствующих перехвату паролей и других реквизитов разграничения доступа, программ, препятствующих несанкционированной модификации аппаратно-программной конфигурации АРМ.

8.4 Непреднамеренное попадание информации к третьим лицам

Возможно непреднамеренное попадание конфиденциальной информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна по причине:

- непреднамеренного прослушивания 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, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов мониторов и других средств её отображения.

8.5 Неформальная модель возможных нарушителей

Все физические лица, имеющие доступ к техническим и программным средствам Фонда, относятся к источникам угроз и могут рассматриваться как потенциальные нарушители.

Система защиты АС должна строиться исходя из предположений о следующих возможных типах нарушителей:

«Некомпетентный (невнимательный) пользователь» - пользователь АС Фонда, который может предпринимать попытки выполнения запрещенных действий для доступа к защищаемым ресурсам АС, ввода некорректных данных и т.п. действуя по ошибке, некомпетентности или

халатности без злого умысла и использующий при этом только предоставленные ему аппаратные и ПС.

“Любитель” - пользователь АС Фонда, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из интереса. Для преодоления системы защиты и совершения запрещенных действий он может совершать несанкционированные действия посредством превышения своих полномочий на доступ и использование информационных ресурсов. Помимо этого, он может пытаться использовать дополнительно специальные инструментальные и технологические ПС, самостоятельно разработанные программы или стандартные дополнительные технические средства.

“Мошенник” - пользователь АС Фонда, который может предпринимать попытки выполнения незаконных действий с ИР в корыстных целях, по принуждению или из злого умысла, использующий при этом аппаратные и ПС от своего имени или от имени другого пользователя.

“Внутренний нарушитель” - сотрудник Фонда (работающий с АС, не допущенный к работе с АС, обслуживающий и технический персонал), действующий целенаправленно из корыстных интересов, возможно, в сговоре с лицами, не являющимися сотрудниками Фонда. Он может использовать весь набор методов и средств нарушения информационной безопасности.

“Внешний нарушитель “ - постороннее лицо или пользователь АС Фонда (уволенный сотрудники Фонда, посетитель, привлеченный IT-специалист и иное лицо, с которыми Фонд взаимодействует в рамках своей уставной деятельности, а также представители преступных организаций, хакеры) действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств нарушения информационной безопасности, методов и средств взлома систем защиты, характерных для сетей общего пользования, включая удаленное внедрение программных “закладок” и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты АС.

9. Основные положения технической политики ИБ АС

9.1 Техническая политика в области обеспечения ИБ

Система обеспечения ИБ АС предусматривает комплекс организационных, программных и технических средств и мер по защите информации в процессе её обработки и хранения, при передаче информации по каналам связи, при ведении переговоров, раскрывающих сведения с ограниченным доступом.

В рамках технической политики обеспечения ИБ АС осуществляются:

- реализация разрешительной системы допуска пользователей к АС Фонда;
- реализация системы технических и организационных мер охраны;
- ограничение доступа посторонних лиц в здания и помещения, где размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация конфиденциального характера, непосредственно к самим средствам информатизации и коммуникациям;
- разграничение доступа пользователей АС и третьих лиц, привлекаемых для обслуживания АС, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- учет документов, информационных массивов, регистрация действий, контроль несанкционированного доступа и несанкционированных действий;
- предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных “закладок” и т.п.;
- межсетевое экранирование с помощью программно-аппаратных комплексов классом не ниже 3;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

- необходимое резервное копирование массивов и носителей информации с целью обеспечения целостности и доступности информации и ПДн;

- своевременное выявление и устранение источников угроз ИБ ИСПДн, вторжений, причин и условий, сопутствующих нанесению ущерба субъектам информационных отношений.

9.2 Формирование режима ИБ

Комплекс мер по формированию режима ИБ включает:

- выполнение режимных требований при работе с АС Фонда: разграничение допуска к ИР ограниченного распространения; разграничение допуска к программно-аппаратным ресурсам АС; ведение учета ознакомления пользователей АС с конфиденциальной информацией; включение в функциональные обязанности сотрудников Фонда обязательства о неразглашении и сохранности конфиденциальных сведений; исключение возможности копирования конфиденциальной информации и передачи её при помощи средств телекоммуникаций (электронная почта, Internet и т.п.); организация уничтожения информационных отходов (бумажных, магнитных и т.д.); оборудование служебных помещений сейфами, шкафами для хранения бумажных и магнитных носителей информации и т.д.

- мероприятия технического контроля: контроль проведения технического обслуживания, ремонта носителей информации и средств вычислительной техники; обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствие с меняющейся оперативной обстановкой.

- физическую охрану объектов АС

- установление в Фонде организационно-правового режима ИБ путем утверждения Политики ИБ.

10. Основные принципы построения системы защиты информации

Построение системы обеспечения ИБ АС и её функционирование осуществляется в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- достаточность;
- персональная ответственность;
- минимизация полномочий;
- гибкость системы защиты;
- простота применения средств защиты;
- обязательность контроля.

Законность

Предполагает осуществление защитных мероприятий и разработку системы ИБ АС в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», другим нормативным актам по информационной безопасности. Принятые меры информационной безопасности не должны препятствовать доступу к ИСПДн правоохранительных органов в предусмотренных законодательством случаях.

Субъекты информационных отношений должны иметь представление об ответственности за правонарушения в области систем автоматизированной обработки информации (ст. ст. 272, 273,

274 и 293 Уголовного Кодекса РФ, ст. ст. 13.11 и 13.12 Кодекса РФ об административных правонарушениях и др.)

Системность

Системный подход предполагает, что учет всех взаимосвязанных, взаимодействующих и изменяющихся элементов, условий и факторов, имеющих значение для понимания и решения проблемы обеспечения информационной безопасности АС.

Комплексность

Комплексность предполагает применение различных средств и технологий защиты АС. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Прикладной уровень защиты на уровне ОС, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты

Защита должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования. Перерывы в работе средств защиты не допускаются.

Своевременность

Предполагает упреждающий характер мер обеспечения информационной безопасности. Разработка системы безопасности разрабатывается параллельно с разработкой и развитием самой АС.

Достаточность

Состояние и стоимость реализации мер ИБ АС должны быть соизмеримы с ценностью ИР и с рисками, связанными с нарушением ИБ. Используемые меры и средства обеспечения ИБ не должны ухудшать основные показатели работы АС. Уровень требований и рекомендаций для субъектов информационных отношений должен соответствовать уровню развития информационных технологий.

Персональная ответственность

Предполагает возложение ответственности за обеспечение ИБ АС на каждого сотрудника Фонда и пользователя АС в пределах его полномочий. Распределение полномочий и обязанностей сотрудников Фонда должно обеспечить выявление круга виновных. Обязанности и полномочия сотрудников Фонда должны быть определены документально.

Минимизации полномочий

Предоставление и использование прав на доступ к информации ограниченного доступа должно быть ограничено и управляемо.

Авторизованным пользователям АС должны предоставляться минимально необходимые права на доступ к информации ограниченного доступа.

Гибкость

В процессе работы Фонда может меняться объем и категории обрабатываемой информации. Гибкость системы защиты избавит Фонд от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Простота применения средств защиты

Применение средств защиты не должно быть связано с наличием специальных знаний в области ИБ 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.

Обязательность контроля

Контроль деятельности 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.

11. Меры, методы и средства обеспечения ИБ АС

Все меры обеспечения безопасности АС делятся на:

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

11.1 Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в РФ законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом АС.

11.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились и складываются по мере распространения ПК и информационно-телекоммуникационной сети Интернет в обществе. Эти нормы не являются обязательными, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неформальные (например, общепризнанные нормы честности и т.п.), так и формальные, то есть оформленные в некоторый свод правил. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в Фонде.

11.3 Организационные (административные) меры защиты

Главная цель административных мер -сформировать политику в области обеспечения информационной безопасности и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Административные меры призваны определить процедуры и правила достижения целей и решения задач информационной безопасности и детализировать эти правила, а именно определить какова область применения политики информационной безопасности; каковы роли и обязанности должностных лиц, отвечающие за проведение политики информационной безопасности; кто имеет права доступа к информации ограниченного распространения; кто и при каких условиях может читать и модифицировать информацию и т.д.

Регламентация доступа в помещения АС

Эксплуатация защищенных серверов АС должна осуществляться в помещениях, оборудованных автоматическими замками, средствами сигнализации, исключающих возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающих физическую сохранность находящихся в помещении защищаемых ресурсов (серверов, документов, реквизитов доступа и т.п.). Размещение и установка технических средств таких серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения. Уборка помещений должна производиться с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Для хранения служебных документов с защищаемой информацией помещения снабжаются сейфами или и шкафами с замками.

Регламентация допуска сотрудников к использованию ресурсов АС

В рамках системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях; доступ, предполагает определение для всех пользователей АС, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) средств доступа.

- Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:
- каждый сотрудник пользуется только той информацией, с которой ему необходимо работать в соответствии с должностными обязанностями;
- руководитель имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники Фонда, пользователи и обслуживающий персонал АС, несут персональную ответственность за нарушения правил сбора, обработки, хранения, использования и передачи информационных ресурсов АС.

Каждый сотрудник обязан подписать «Договор о неразглашении конфиденциальной информации», а также ознакомиться с «Положением о конфиденциальной информации”

Регламентация процессов ведения баз данных и осуществления модификации информационных ресурсов

Все операции по ведению баз данных Фонда и допуск сотрудников Фонда к работе с этими базами данных строго регламентируются. Любые изменения состава и полномочий пользователей баз данных АС производятся в установленном порядке.

Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов АС

Для серверов и программных ресурсов АС должен быть определен требуемый уровень защищенности и подлежащие защите ресурсы системы (программы, АРМ) должны быть учтены.

Аппаратно-программная конфигурация АРМ, на которых обрабатывается конфиденциальная информация (с которых возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей данного АРМ функциональных обязанностей. Все неразрешенные для использования в работе устройства ввода-вывода информации (USB-, LPT-порты, CD, DVD- дисководы, устройства Flash-памяти и другие носители информации) на таких АРМ должны быть отключены (удалены) или заблокированы, не нужные для работы ПС и данные с дисков АРМ также должны быть удалены. Для упрощения сопровождения, обслуживания и организации защиты АРМ должны оснащаться программными средствами.

Должны быть предусмотрены механизмы, исключающие несанкционированное изменение конфигурации аппаратных средств, установленных на рабочих местах пользователей.

Кадровая работа (подбор и подготовка сотрудников и обслуживающего персонала, обучение пользователей)

До начала этапа эксплуатации АС её пользователи, а также необходимый обслуживающий персонал должны быть ознакомлены с перечнем сведений, подлежащих защите и своим уровнем полномочий, а также организационно-распорядительной, нормативной документацией, определяющей требования и порядок обработки информации ограниченного распространения.

Защита информации возможна только после выработки у пользователей определенной дисциплины, т.е. норм, обязательных для исполнения всеми, кто работает с АС. К таким нормам относятся запрещение любых умышленных или неумышленных действий, которые нарушают работу АС, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей.

Доведение требований по ИБ АС, допущенных к обработке защищаемой информации, должно осуществляться руководителями под личную подпись.

Лица, отвечающие за реализацию политики информационной безопасности

Ответственность за обеспечение организации и контроля ИБ информационных ресурсов, в том числе ПДн пользователей АС, обрабатываемых в Фонде возлагается на

директора Фонда, Аксенову Марину Анатольевну.

На время отсутствия ответственных необходимо назначить лиц, замещающих их согласно приказу.

Основные функции ответственных лиц при реализации Политики ИБ заключаются в следующем:

- формирование требований к системе защиты в процессе создания (развития) АС;
- распределение между пользователями АС необходимых реквизитов защиты;
- обучение пользователей АС и сотрудников Фонда правилам безопасной обработки информации;
- контроль соблюдения пользователями АС и сотрудниками Фонда правил обращения с конфиденциальной информацией в процессе её автоматизированной обработки, передачи и хранения;
- принятие мер при попытках НСД к информации.

Ответственным лицам за информационную безопасность должны быть предоставлены права:

- доступа ко всем ресурсам АС с правами, достаточными для осуществления полного контроля АС;

-доступа во все помещения, где установлена аппаратура АС;

-запрета автоматизированной обработки информации при наличии непосредственной угрозы для защищаемой информации;

-запрета включения в число действующих новых элементов АС, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз ИБ.

Уполномоченным органом по защите прав субъектов ПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки ПДн требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» (с изменениями и дополнениями),

является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Для выполнения всех перечисленных выше функций могут привлекаться IT- специалисты или специалисты сторонних организаций, работающих в сфере информационной безопасности.

Привлекаемые IT-специалисты или специалисты по ИБ осуществляют контроль реализации политики безопасности и оценку эффективности принятых мер и применяемых средств защиты информации.

Их функции заключаются в следующем:

- организация проверок надежности функционирования системы защиты;
- оценка эффективности системы контроля баз данных, серверов и сетевых устройств;
- оценка системы контроля соблюдения пользователями АС и сотрудниками Фонда установленных правил обращения с конфиденциальной информацией;
- организация проверок соблюдения пользователями АС и сотрудниками Фонда правил обращения с конфиденциальной информацией; расследование инцидентов, связанных с нарушениями правил обращения с конфиденциальной информацией.

Привлекаемым IT-специалистам и специалистам по ИБ на которых возложено выполнение перечисленных выше функций, должны обеспечиваться все условия, необходимые для выполнения этих функций.

Они должны иметь права:

- определять необходимость разработки нормативных документов, касающихся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность сотрудников Фонда;

-получать информацию от сотрудников Фонда по вопросам применения информационных технологий и эксплуатации АС;

-участвовать в испытаниях программ по вопросам оценки качества реализации требований по обеспечению информационной безопасности;

-контролировать деятельность сотрудников Фонда по вопросам обеспечения информационной безопасности (включая контроль Internet трафика, внешней и внутренней почтовой переписки, содержимого файлов на дисках ПЭВМ и в личных каталогах на серверах).

Ответственность за нарушения установленного порядка использования АС. Расследование нарушений.

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.

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

Любое грубое нарушение порядка и правил работы в АС сотрудниками Фонда и персоналом, привлекаемым для обслуживания АС должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности за действия, совершенные в нарушение правил обеспечения безопасной автоматизированной обработки информации, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Фонда.

Для реализации принципа персональной ответственности пользователей за свои действия необходима индивидуальная идентификация и аутентификация пользователей и инициированных ими процессов.

11.4 Физические средства защиты

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

11.5 Технические (программно-аппаратные) средства защиты

Технические (программно-аппаратные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС.

С учетом всех требований ИБ в состав АС включены следующие средства:

- средства аутентификации пользователей и элементов АС (компьютеров, программ, и т.п.);
- средства разграничения доступа к данным;
- средства криптографической защиты информации;
- средства регистрации обращения и контроля использования защищаемой информации;
- средства ограничения использования внешних носителей информации или фиксирования их применения;
- антивирусная защита;
- средства обнаружения вторжений.

На технические средства защиты от НСД возлагается решение следующих основных задач (в соответствии с нормативными документами ФСТЭК и ФСБ России, ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 17799):

- идентификация и аутентификация пользователей при помощи имен и/или специальных аппаратных средств;

- избирательное управление доступом к логическим дискам, каталогам и файлам;

- разграничение доступа к защищаемым данным на рабочей станции и на файловом сервере;

- ограничение перечня разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках;

- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

- регистрация действий пользователя в защищенном журнале;

- защита данных системы защиты на файловом сервере от доступа всех пользователей;

- оповещение привлеченного IT-специалиста или специалиста по ИБ о событиях НСД, происходящих на рабочей станции;

- контроль работы пользователей АС, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой рабочей станции АС.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с АС посторонних лиц обеспечена возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей). Для этого в системе хранится ряд признаков каждого пользователя, по которым этого пользователя можно опознать. В дальнейшем при входе в систему или при выполнении определенных действий в системе, пользователь обязан себя идентифицировать, т.е. указать

идентификатор, присвоенный ему в системе. Кроме того, для идентификации применяются различного рода устройства: магнитные карточки, ключи и т.п.

Аутентификация пользователей осуществляется на основе использования паролей.

Средства разграничения доступа к данным

После распознавания пользователя система должна осуществлять его авторизацию, то есть определять, какие права ему предоставлены: какие данные и как он может использовать, какие программы может выполнять, какие ресурсы системы может использовать и т.п.

Средства контроля и регистрации событий безопасности

Средства контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности.

Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов) для каждой рабочей станции;

-оперативного ознакомления IT-специалиста или специалиста по ИБ с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД.

При регистрации событий безопасности в системном журнале должны фиксироваться дата и время события, идентификатор субъекта и действие.

Желательно, чтобы средства контроля обеспечивали обнаружение и регистрацию следующих событий: вход пользователя в систему, вход пользователя в сеть; неудачная попытка входа в систему или сеть (неправильный ввод пароля); подключение к файловому серверу; запуск программы; завершение программы; попытка открытия файла недоступного для чтения; попытка открытия на запись файла недоступного для записи; попытка удаления файла недоступного для модификации; попытка изменения атрибутов файла недоступного для модификации; попытка запуска программы, недоступной для запуска; попытка чтения/записи информации с диска, недоступного пользователю; попытка запуска программы с диска, недоступного пользователю и др.

Желательно поддерживать следующие способы реагирования на факты НСД: извещение владельца информации о НСД к его данным; снятие программы (задания) с дальнейшего выполнения; извещение привлеченного IT-специалиста или специалиста по ИБ; исключение нарушителя из списка зарегистрированных пользователей и др.

11.6 Управление системой обеспечения информационной безопасности

Управление системой обеспечения ИБ в АС представляет собой целенаправленные действия (организационные, технические, программные) с целью достижения ИБ ИР АС.

Главной целью организации управления системой обеспечения информационной безопасности является повышение надежности защиты информации в процессе её обработки, хранения и передачи.

На этапе создания, ввода и модернизации АС необходимо разработать и реализовать нормативно-правовые основы и техническую базу, которые будут обеспечивать использование передовых средств и информационных технологий обработки и передачи информации; организовать взаимодействие разработчиков АС, сотрудников Фонда и пользователей АС, финансовых, материальных и иных ресурсов; создать рабочую структуру, которая будет обеспечивать решение задач ИБ при работе АС.

На этапе эксплуатации АС необходимо обязательное и неукоснительное выполнение правил и процедур, направленных на обеспечение ИБ, всеми участниками информационных отношений; своевременное выявление и пресечение посягательств на ИР АС.

Управление системой обеспечения ИБ реализуется специализированной системой, представляющей собой совокупность органов управления, нормативно-правовой базы, технических, программных средств и организационных мероприятий.

11.7 Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам или физического ее распространения участниками информационных отношений, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Контроль может проводиться привлекаемыми IT-специалистами или специалистами по информационной безопасности, имеющими лицензию на этот вид деятельности.

12. Требование к персоналу по обеспечению ИБ АС

Все сотрудник Фонда, являющиеся пользователями ИСПДн, должны знать и выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности информации и ПДн.

Ответственное лицо Фонда обязано ознакомить вновь принятого сотрудника с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации и ПДн, организовать обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн. Сотрудник Фонда должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и системами защиты информации и ПДн.

Сотрудники Фонда, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов и не допускать НСД к ним, возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Фонда должны следовать установленным процедурам поддержания режима безопасности информации и ПДн при выборе и использовании паролей.

Сотрудники Фонда должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

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

Сотрудникам Фонда запрещается разглашать защищаемую информацию, которая стала им известна в связи с исполнением должностных обязанностей, третьим лицам.

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

При завершении работы с ИСПДн работники обязаны защитить АРМ с помощью блокировки.

Сотрудники Фонда должны быть проинформированы об угрозах нарушения режима безопасности информации и ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утверждённой формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности информации и ПДн.

Сотрудники Фонда обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности

информации и ПДн, а также о выявленных ими событиях, затрагивающих безопасность информации и ПДн, директору Фонда, привлеченному IT-специалисту или специалисту по ИБ.

13. Первоочередные мероприятия по обеспечению информационной безопасности АС

Для реализации основных положений настоящей Политики целесообразно провести следующие мероприятия:

- для снижения затрат на создание системы защиты рассмотреть возможность внесения изменений в конфигурацию сетей и СВТ, технологии обработки, передачи и хранения информации;

- определить возможность использования в АС имеющихся на рынке сертифицированных средств защиты информации;

- произвести закупку сертифицированных образцов и серийно выпускаемых технических и программных средств защиты информации и их внедрение на рабочих станциях и файловых серверах сети с целью контроля изменения конфигурации аппаратных и программных средств и действиями пользователей;

-определить степень участия сотрудников Фонда в обработке (передаче, хранении, обсуждении) информации;

- разработать локальные нормативно-правовые документов по ИБ АС;

- организовать физическую защиту объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности;

- провести мероприятия по ознакомлению сотрудников Фонда с документами по ИБ АС.

14. Порядок пересмотра Политики ИБ

Внеплановый пересмотр Политики ИБ проводится в случае существенных изменений международного или национального законодательства в сфере защиты информации или по усмотрению Фонда в связи с необходимостью дополнить или скорректировать положения Политики ИБ.

При внесении изменений в положения Политики ИБ учитываются:

- уровень развития и внедрения информационных технологий в телекоммуникационной отрасли;
- рекомендации российских и международных профильных организаций в области ИБ;
- рекомендации регулирующих органов, уполномоченных в области защиты информации;
- результаты проверки эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения ИБ;
- определение стоимости мероприятий по управлению ИБ и их влияние на эффективность деятельности Фонда.