

ПРИКАЗ

29.12.2018

№ 638

Об утверждении концепции информационной безопасности

В соответствии с требованиями законодательства об информации, информационных технологиях и о защите информации, о защите персональных данных,

приказываю:

1. Утвердить концепцию информационной безопасности муниципального казенного учреждения Центр социальной помощи семье и детям (Приложение 1 к настоящему приказу).
2. Заместителям директора, главному бухгалтеру обеспечить:
 - 2.1. обеспечить ознакомление подчиненных работников с концепцией информационной безопасности;
 - 2.2. осуществлять контроль над соблюдением подчиненными работниками положений концепции.
3. Контроль над исполнением настоящего приказа возложить на заместителя директора Такленок А.В.

Директор



Н.Е. Демина

**Концепция информационной безопасности
муниципального казенного учреждения
Центр социальной помощи семье и детям**

Перечень использованных источников

Основными нормативно-правовыми актами и методическими документами, на положениях которых базируется настоящее Положение, являются:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Постановление Правительства РФ от 06.07.2008 г. № 512 «Об утверждении требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
4. Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Приказ ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г. «Об утверждении порядка проведения классификации информационных систем персональных данных».

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

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанному в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) -

участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

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

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

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

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

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

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

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

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

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

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

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

Введение

Настоящая Концепция информационной безопасности ИСПДн (далее - Концепция) разработана муниципальным казенным учреждением Центр социальной помощи семье и детям (далее по тексту - Учреждение), является локальным нормативным актом, в котором определена система взглядов на обеспечение информационной безопасности Учреждения.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Учреждениях, при обработке информации вообще, и персональных данных в частности.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения.

Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана с применением системного подхода к обеспечению информационной безопасности.

Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре.

Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждений, 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.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Учреждения;

- принятия управленческих решений и 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 Учреждения 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 Учреждения.

данных и СЗИ;

- инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

- ✓ - инструкция администратора безопасности ИСПДн;

- ✓ - инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

- ✓ - инструкция на случай возникновения внештатной ситуации;

- рекомендации по использованию программных и аппаратных средств защиты информации.

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

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Учреждения.

2. Задачи СЗПДн

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

Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только 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:

- а) к информации, циркулирующей в ИСПДн;

- б) средствам вычислительной техники ИСПДн;

- в) 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, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

2) программисты-разработчики ИСПДн: сотрудники Учреждения или сторонних организаций, которые занимаются разработкой программного обеспечения.

Разработчик ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

3) операторы ИСПДн: сотрудники структурных подразделений Учреждения, участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей, определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в отчете по результатам внутренней проверки. На основании отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в матрице доступа в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ПДн ИСПДн Учреждения и 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.

Законность предполагает осуществление защитных мероприятий и разработку

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.

Преимственность и совершенствование предполагают постоянное совершенствование мер и средств защиты информации на основе преимущественности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

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

Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Учреждения, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

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.

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 ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты: механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано

характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.2. Морально-этические меры защиты.

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

6.3. Организационные (административные) меры защиты.

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

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

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

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности.

Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение 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 Учреждения 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, 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 информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;

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 Учреждения;
- 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 (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (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 Учреждения разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- специалистами Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Контроль эффективности системы защиты ИСПДн Учреждения

Контроль эффективности СЗПДн 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 так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности 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.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ПДн проводится с использованием технических

10. Модель угроз безопасности

Для ИСПДн Учреждения выделяются следующие основные категории угроз безопасности персональных данных:

- 1) угрозы от утечки по техническим каналам;
- 2) угрозы несанкционированного доступа к информации;
- 3) угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- 4) угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных ИСПДн.

11. Механизм реализации концепции

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;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

12. Ожидаемый эффект от реализации концепции

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.