УТВЕРЖДЕНА

 приказом департамента

 социальной защиты

 Воронежской области

 от 29.03.2016 № 585 /ОД

**Концепция информационной безопасности**

**при обработке персональных данных**

**в органах социальной защиты населения Воронежской области**

Оглавление

[Введение 3](#_Toc334453392)

[Основные понятия и термины, используемые в настоящем документе 4](#_Toc334453393)

[1. Общие положения 9](#_Toc334453394)

[2. Правовые основы системы информационной безопасности 10](#_Toc334453395)

[3. Цели и задачи системы информационной безопасности 11](#_Toc334453396)

[4. Принципы организации и функционирования системы информационной безопасности 12](#_Toc334453397)

[5. Объекты защиты 14](#_Toc334453398)

[6. Система обеспечения безопасности персональных данных 15](#_Toc334453399)

[7. Мероприятия по обеспечению безопасности персональных данных 19](#_Toc334453400)

[8. Угрозы безопасности персональных данных 20](#_Toc334453401)

[8.1. Угрозы безопасности персональных данных при обработке в информационных системах 21](#_Toc334453402)

[9. Классификация информации 22](#_Toc334453403)

[9.1. Классификация информационных систем персональных данных 23](#_Toc334453404)

[10. Меры обеспечения информационной безопасности 24](#_Toc334453405)

[10.1. Правовые меры обеспечения информационной безопасности 24](#_Toc334453406)

[10.2. Организационные меры обеспечения информационной безопасности 25](#_Toc334453407)

[10.3. Физические меры обеспечения информационной безопасности 25](#_Toc334453408)

[10.4. Технические меры обеспечения информационной безопасности 25](#_Toc334453409)

[10.5. Административные меры обеспечения информационной безопасности 26](#_Toc334453410)

[11. Управление системой информационной безопасности 26](#_Toc334453411)

[12. Механизмы реализации Концепции 27](#_Toc334453412)

# Введение

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

На территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных. Основной целью государственного регулирования является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Специфика деятельности органов социальной защиты населения такова, что основным объектом социальной защиты является гражданин с его персональными данными. Персональные данные граждан могут быть представлены в различных формах. Они могут быть напечатаны или написаны на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи. Обработка персональных данных граждан в органах социальной защиты населения осуществляется как в информационных системах, так и без использования средств автоматизации.

Обязательным условием работы с персональными данными является обеспечение лицами, получающими доступ к персональным данным, конфиденциальности таких данных, за исключением случаев, предусмотренных федеральными законами.

Информационная безопасность – механизм защиты, обеспечивающий:

* конфиденциальность: доступ к информации только авторизованных пользователей;
* целостность: достоверность и полноту информации и методов ее обработки;
* доступность: доступ к информации авторизованных пользователей по мере необходимости.

Настоящая концепция информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области (далее – Концепция) разработана в целях определения основных принципов организации и функционирования информационной системы информационной безопасности персональных данных, а также основных направлений разработки информационной системы информационной безопасности, включая правовую, организационную и инженерно-техническую защиту.

# Основные понятия и термины, используемые в настоящем документе

В настоящем документе используются следующие основные понятия и термины и их определения:

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

**Автоматизированное рабочее место -** рабочее место пользователя в составе комплекса средств автоматизации.

**Аутентификация отправителя данных** – подтверждение того, что от­правитель полученных данных соответствует заявленному.

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

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

**Вспомогательные технические средства и системы** – технические сред­ства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средст­вами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персо­нальных данных.

**Доступ к информации** – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрыт­но внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, пред­меты интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

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

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

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

**Конфиденциальная информация** – требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации.

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

**Материальный носитель** – изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.

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.

Неавтоматизированная обработка персональных данных – обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

**Несанкционированный доступ** **к информации (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие установленные правила разграничения доступа.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Объект защиты** – персональные данные, информация, обрабатываемая в информационных системах персональных данных, технические средства обработки и защиты персональных данных.

**Органы социальной защиты населения** **Воронежской области** – департамент социальной защиты Воронежской области, государственные учреждения, в отношении которых департамент социальной защиты Воронежской области исполняет функции и полномочия учредителя.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В настоящем документе операторами являются органы социальной защиты населения Воронежской области.

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

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

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

**Технические средства, позволяющие осуществлять обработку персональных данных,** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

# Общие положения

Настоящая Концепция представляет собой систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты информации от противоправных действий.

Концепция направлена на формирование целостного представления о системе безопасности персональных данных в органах социальной защиты населения Воронежской области и взаимоувязку различных элементов этой системы, определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объектов.

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

Концепция определяет:

* основные цели и задачи, а также общую стратегию построения системы защиты персональных данных органов социальной защиты населения Воронежской области,
* основные требования и базовые подходы их реализации для достижения требуемого уровня безопасности информации.

Концепция является методологической основой для:

* формирования и проведения единой политики в области обеспечения безопасности персональных данных, обрабатываемых в органах социальной защиты населения Воронежской области, как без использования средств автоматизации, так и в информационных системах;
* принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативного правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз персональным данным;
* координации деятельности структурных подразделений департамента социальной защиты Воронежской области (далее – Департамент), государственных учреждений, в отношении которых Департамент исполняет функции и полномочия учредителя (далее – подведомственные учреждения), при проведении работ по развитию и эксплуатации информационных систем персональных данных с соблюдением требований обеспечения безопасности персональных данных;
* разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных при их обработке.

Настоящая Концепция не распространяется на вопросы организации обработки и обеспечение безопасности информации, отнесенной в соответствии с действующим законодательством к государственной тайне.

# Правовые основы системы информационной безопасности

Правовое регулирование вопросов обработки персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации, осуществляется следующими нормативными правовыми актами:

* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Трудовой кодекс Российской Федерации;
* постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
* постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* методические документы ФСБ России, ФСТЭК России, Роскомнадзора;
* иные нормативные правовые акты в сфере защиты информации.

# Цели и задачи системы информационной безопасности

 Главной целью системы информационной безопасности является предотвращение разглашения, утраты, утечки, искажения и уничтожения конфиденциальной информации, информации для внутреннего использования, нарушения работы технических средств обеспечения производственной деятельности, включая средства информатизации, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Основными задачами системы информационной безопасности являются:

* прогнозирование, своевременное выявление и устранение угроз безопасности персональным данным;
* отнесение информации к категории ограниченного доступа (персональных данных, иной конфиденциальной информации, подлежащей защите от неправомерного использования), к различным уровням уязвимости (опасности) и подлежащей сохранению;
* создание механизма и условий оперативного реагирования на угрозы информационной безопасности;
* эффективное пресечение угроз информационной безопасности на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
* создание условий для максимально возможного возмещения и локализации наносимого ущерба, вызванного неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на деятельность органов социальной защиты населения Воронежской области.

# Принципы организации и функционирования системы информационной безопасности

 Организация и функционирование системы информационной безопасности в органах социальной защиты Воронежской области соответствуют следующим принципам:

1. **Комплексность.** Соответствующий требованиям нормативной правовой базы уровень информационной безопасности при обработке персональных данных обеспечивается на основе комплексного подхода, предполагающего использование правовых, организационных, программно-технических и других мер обеспечения информационной безопасности.

2. **Своевременность.** Постановка задач по комплексной безопасности на ранних стадиях разработки системы информационной безопасности на основе анализа и прогнозирования угроз информационной безопасности, а также разработка эффективных мер предупреждения несанкционированного доступа к информации, обеспечивает упреждающий характер мер обеспечения безопасности.

3. **Непрерывность.** Обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования.

4. **Активность**. Способность системы информационной безопасности к развитию и совершенствованию в соответствии с изменениями условий функционирования органов социальной защиты населения Воронежской области, внедрению новых мер защиты.

5. **Законность.** Разработка системы информационной безопасности осуществляется на основе федерального законодательства в области защиты информации, нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6. **Обоснованность.** Используемые возможности и средства защиты реализуются на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствуют установленным требованиям и нормам.

7. **Экономическая целесообразность.** При разработке и внедрении мер и средств защиты обеспечивается сопоставимость возможного ущерба и затрат на обеспечение безопасности.

8. **Специализация.** К разработке и внедрению мер и средств защиты привлекаются специализированные организации, наиболее подготовленные к конкретному виду деятельности по обеспечению безопасности, имеющие опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности осуществляются профессионально подготовленными специалистами Департамента, подведомственных учреждений.

9. **Взаимодействие и координация.** Меры обеспечения безопасности осуществляются на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными органами государственного управления и правоохранительными органами.

10. **Совершенствование.** Совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, достигнутого отечественного и зарубежного опыта.

11. **Централизация управления.** Функционирование системы информационной безопасности осуществляется по единым правовым, организационным, функциональным и методологическим принципам, под централизованным управлением деятельностью системы информационной безопасности.

# Объекты защиты

К объектам, подлежащим защите от потенциальных угроз и противоправных посягательств, относятся:

* персональные данные граждан, обратившихся в органы социальной защиты населения Воронежской области, персональные данные работников органов социальной защиты населения Воронежской области, другие информационные ресурсы с ограниченным доступом, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;
* средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телефонной, факсимильной связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
* материальные средства (здания, хранилища, техническое оборудование и иные средства);
* технические средства и системы охраны и защиты материальных и информационных ресурсов.

 Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную потенциальную уязвимость с точки зрения возможного материального или морального ущерба. Исходя из этого, они классифицируются по уровням уязвимости (опасности), степени риска.

 Наибольшую уязвимость представляют информационные ресурсы.

# Система обеспечения безопасности персональных данных

Основной задачей организации обеспечения безопасности персональных данных является формирование и реализация совокупности согласованных по цели и задачам мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности персональных данных, на восстановление нормального функционирования после нейтрализации угрозы с целью минимизации ущерба от возможной реализации таких угроз.

Основными направлениями обеспечения информационной безопасности являются:

* защита информационных ресурсов (персональных данных) от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа и специальных воздействий;
* защита информации от утечки вследствие наличия физических полей за счет акустических и побочных электромагнитных излучений и наводок (ПЭМИН) на электрические цели, трубопроводы и конструкции зданий.

В рамках указанных направлений обеспечения информационной безопасности необходимы:

* реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
* ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера;
* разграничение доступа пользователей к данным информационных систем, осуществляющих обработку персональных данных;
* учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;
* криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
* снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств обеспечения производственной деятельности и информационных систем;
* снижение уровня акустических излучений;
* электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории (при необходимости);
* активное зашумление в различных диапазонах;
* противодействие оптическим и лазерным средствам наблюдения;
* проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств;
* предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

Система защиты информационных ресурсов (персональных данных) от несанкционированного доступа предусматривает:

1. **Обоснованность доступа**. Исполнитель (пользователь) должен иметь соответствующую форму допуска для ознакомления с документацией (информацией) определенного уровня конфиденциальности, при этом ему необходимо ознакомление с данной информацией или необходимы действия с ней для выполнения служебных обязанностей. Реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, которой устанавливаются полномочия сотрудников по доступу и видам обработки определенного перечня конфиденциальной информации (документов, сведений, носителей информации, информационных массивов), и которая предполагает определение для всех пользователей автоматизированных информационных систем, доступность конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью программно-технических средств доступа.
2. **Персональную ответственность**. Исполнитель (пользователь) несет ответственность за сохранность доверенных ему документов (носителей информации, информационных массивов), за свои действия в информационных системах. Реализуется с помощью:
* росписи исполнителей в журналах, карточках учета, других разрешительных документах, а также на самих документах;
* индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;
* проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, ключей, магнитных карт, электронной подписи, а также биометрических характеристик личности как при доступе в автоматизированные системы, так и в выделенные помещения (зоны).
1. **Надежность хранения**. Документы (носители информации, информационные массивы) хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение. Условие надежности хранения реализуется с помощью:
* хранилищ конфиденциальных документов, оборудованных средствами охраны в соответствии с установленными требованиями, доступ в которые ограничен и осуществляется в установленном порядке;
* выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованных сейфами и металлическими шкафами, а также ограничения доступа в эти помещения;
* использования криптографического преобразования информации в автоматизированных системах.
1. **Разграничение информации по уровню конфиденциальности**. Предупреждение отражения сведений более высокого уровня конфиденциальности в документах (носителях информации, информационных массивах) с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи.
2. **Контроль за действиями исполнителей (пользователей)**. Система контроля за действиями исполнителей с документацией и сведениями, а также в информационных системах и системах связи, реализуется с помощью:
* организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;
* регистрации (протоколирования) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;
* сигнализации о несанкционированных действиях пользователей.
1. **Целостность технической и программной среды, обрабатываемой информации и средств защиты**. Обеспечение физической сохранности средств информатизации, неизменности программной среды, определяемой предусмотренной технологией обработки информации, выполнение средствами защиты предусмотренных функций, изолированность средств защиты от пользователей.

Необходимой составляющей системы обеспечения безопасности персональных данных, иной конфиденциальной информации является обеспечение качества работ и используемых средств и мер защиты. В целях обеспечения необходимого уровня безопасности персональных данных система информационной безопасности базируется на выполнении трех условий:

* обязательная сертификация средств и систем вычислительной техники и связи по требованиям безопасности информации;
* лицензирование деятельности по оказанию услуг в области защиты информации;
* аттестация объектов информатизации по требованиям безопасности информации.

# Мероприятия по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных включают в себя:

1. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз.
2. Классификацию информации, включая информационные системы.
3. Разработку на основе модели угроз и классификации информации системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз.
4. Определение функций и обязанностей персонала в области информационной безопасности.
5. Определение правил хранения, использования, уничтожения материальных носителей информации.
6. Определение прав доступа работников к персональным данным. Организация учета лиц, допущенных к работе с персональными данными.
7. Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.
8. Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.
9. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
10. Определение требований информационной безопасности при обработке персональных данных без использования средств автоматизации.
11. Определение требований информационной безопасности при обработке персональных данных в информационных системах.
12. Контроль за соблюдением требований информационной безопасности, условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
13. Расследование событий, связанных с нарушениями информационной безопасности.

# Угрозы безопасности персональных данных

Система защиты персональных данных строится на основе анализа угроз безопасности персональных данных, заключающегося в выявлении угроз, оценке уязвимости персональных данных и вероятности возникновения угроз, а также оценке возможных последствий.

Под угрозами безопасности персональных данных понимается 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.

Основными угрозами информации являются ошибки, связанные с человеческим фактором, воровство, мошенничество или неправильное использование средств обработки информации.

## Угрозы безопасности персональных данных при обработке в информационных системах

Угрозы безопасности персональных данных при их обработке в информационных системах могут быть связаны как с непреднамеренными действиями сотрудников оператора, имеющих доступ к информационным системам, так и со специально осуществляемыми неправомерными действиями отдельных лиц, а также иными источниками угроз.

Угрозы безопасности персональных данных могут быть реализованы засчет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах информационных систем, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации), либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в информационных системах персональных данных правила разграничения доступа к информации. Этими субъектами могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Под нарушителем понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам информационных систем персональных данных, нарушители подразделяются на два типа:

* нарушители, не имеющие доступа к информационным системам персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;
* нарушители, имеющие доступ к информационным системам персональных данных, включая пользователей информационных систем, реализующие угрозы непосредственно в информационных системах персональных данных, - внутренние нарушители.

Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационным ресурсам и мер по контролю порядка проведения работ.

Угрозы несанкционированного доступа от внешних нарушителей реализуются с использованием протоколов межсетевого взаимодействия.

Для каждой информационной системы персональных данных, эксплуатируемой в органах социальной защиты населения Воронежской области, определяются угрозы безопасности персональных данных и разрабатываются частные модели угроз безопасности персональных данных.

# Классификация информации

В целях определения требований к информационной безопасности информация классифицируется для определения её приоритетности, необходимости и степени её защиты.

Информация имеет различные степени чувствительности и критичности. Некоторые виды информации могут требовать дополнительного уровня защиты или специальных методов обработки. Система классификации информации используется для определения соответствующего множества уровней защиты и потребности в специальных методах обработки.

## Классификация информационных систем персональных данных

Информационные системы классифицируются в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации информационных систем включает в себя следующие этапы:

* сбор и анализ исходных данных по информационной системе;
* присвоение информационной системе соответствующего класса и его документальное оформление.

Результаты классификации информационных систем оформляются соответствующим актом оператора.

Класс информационной системы может быть пересмотрен:

* по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
* по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

# Меры обеспечения информационной безопасности

Система обеспечения безопасности персональных данных предусматривает комплекс правовых, организационных, технических и программных мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

## Правовые меры обеспечения информационной безопасности

К правовым мерам обеспечения информационной безопасности относятся действующие нормативные правовые акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с лицами, осуществляющими обработку персональных данных.

Успешное и эффективное решение задач обеспечения безопасности достигается формированием системы внутренних нормативных актов, инструкций, положений, правил, регламентов и функциональных обязанностей сотрудников подразделений органов социальной защиты населения Воронежской области.

## Организационные меры обеспечения информационной безопасности

Организационные меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие требования к персоналу, степень ответственности персонала, статус и должностные обязанности сотрудников, ответственных за обеспечение информационной безопасности, порядок обработки персональных данных, взаимодействие специалистов в целях максимального затруднения или исключения возможности реализации угроз безопасности или снижения размера потерь в случае их реализации.

## Физические меры обеспечения информационной безопасности

Меры физической защиты предназначены для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации, предотвращения несанкционированного физического доступа, повреждения и воздействия на помещения и защищаемую информацию.

## Технические меры обеспечения информационной безопасности

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

## Административные меры обеспечения информационной безопасности

Главная цель административных мер – сформировать политику информационной безопасности, отражающую подходы к защите информации, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

К административным мерам относятся решения руководства, затрагивающие вопросы работы с персональными данными в целом. Эти решения закрепляются в политике информационной безопасности.

Административными мерами устанавливаются сфера влияния и ограничения при определении целей информационной безопасности, какими ресурсами (материальные, персонал) они будут достигнуты и определен разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем обработки персональных данных.

# Управление системой информационной безопасности

Управление системой информационной безопасности, созданной на основе принципов, определенных настоящей Концепцией, организуется с учетом существующей структуры и организации деятельности органов социальной защиты населения Воронежской области.

Принимая во внимание организацию деятельности органов социальной защиты населения Воронежской области с едиными информационными системами, обрабатывающими персональные данные, едиными информационными ресурсами (документами, информационными массивами, личными делами граждан), функционирование системы информационной безопасности организуется по единым правовым, организационным, функциональным и методологическим принципам при централизованной координации деятельности системы информационной безопасности со стороны Департамента с назначением сотрудников, ответственных за безопасность, во всех подведомственных учреждениях.

# Механизмы реализации Концепции

Реализация настоящей Концепции осуществляется посредством выполнения плана мероприятий по обеспечению безопасности персональных данных, разрабатываемого Департаментом.

Реализация Концепции включает в себя:

* координацию в Департаменте деятельности органов социальной защиты населения по обеспечению информационной безопасности;
* разработку и реализацию мероприятий, направленных на решение основных задач, сформулированных в Концепции;
* контроль обеспечения безопасности персональных данных, в том числе путем проведения плановых проверок режима защиты персональных данных;
* методическое обеспечение деятельности подведомственных учреждений в части организации работ по обеспечению информационной безопасности.

В целях создания и обеспечения функционирования системы комплексной безопасности с учетом положений настоящей Концепции разрабатываются следующие документы:

* политика информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области;
* положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
* модели угроз безопасности персональных данных;
* положение по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации;
* положение о разрешительной системе доступа к персональным данным;
* инструкции по эксплуатации средств защиты информации;
* инструкции пользователей информационных систем;
* другие документы, необходимые для обеспечения функционирования системы комплексной безопасности.

Правовыми актами Департамента, подведомственных учреждений определяются:

* перечень персональных данных, подлежащих защите;
* перечень должностей служащих, замещение которых предусматривает обработку либо доступ к персональным данным;
* лица, ответственные за организацию и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
* лица, ответственные за организацию обработки персональных данных, осуществляемой без использования средств автоматизации;
* порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных.

План мероприятий по созданию системы информационной безопасности предусматривает приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов, а также предусматривает привлечение к его выполнению специализированных организаций, имеющих практический опыт работы по рассматриваемой проблеме и лицензии на соответствующий вид деятельности.

Для осуществления эффективного управления и контроля выполнения плана мероприятий по реализации Концепции в Департаменте создаётся комиссия по обеспечению безопасности персональных данных, основными задачами которой являются координация и контроль деятельности органов социальной защиты населения Воронежской области по обеспечению информационной безопасности.