**УТВЕРЖДАЮ**

Глава администрации

Турковского

муниципального района

Саратовской области

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Д. В. Кудряшов**

10 августа 2015 года

**ПОЛИТИКА**

**в отношении обработки персональных данных**

**администрации Турковского муниципального района**

2014 г.

Оглавление

|  |  |
| --- | --- |
| Термины и определения ………………………………………………..  | 3 |
| Обозначения и сокращения……………………………………………..  | 8 |
| Введение …………………………………………………………………  | 9 |
| Общие положения ………………………………………………………. | 11 |
| Область действия………………………………………………………...  | 11 |
| Основные принципы обеспечения информационной безопасности информационных систем персональных данных администрации Турковского муниципального района ………………… | 11 |
| Система защиты персональных данных ………………………………… | 16 |
| Меры, методы и средства обеспечения требуемого уровня защищенности…………………………………………………………….. | 17 |
| Контроль эффективности системы защиты информационных систем персональных данных администрации Турковского муниципального района……………………..  | 20 |
| Пользователи информационных систем персональных данных администрации Турковского муниципального района……  | 21 |
| Требования к персоналу по обеспечению защиты ПД………………… | 23 |
| Должностные обязанности пользователей информационных систем персональных данных администрации Турковского муниципального района ……………………… | 24 |
| Ответственность пользователей информационных систем персональных данных администрации Турковскогомуниципального района…………………………………………………… | 24 |

# Термины и определения

В настоящем документе используются следующие термины и их определения:

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

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

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

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

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

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

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

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

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

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

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

Информационная система персональных данных (ИСПД) – 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 описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

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

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор** (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**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.

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

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПД – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СЗПД – система (подсистема) защиты персональных данных

СКЗИ – система криптографической защиты информации

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПД – угрозы безопасности персональных данных

# Введение

Настоящая Политика в отношении обработки персональных данных (далее – Политика) администрации Турковского муниципального района является официальным документом, в котором определена система обеспечения информационной безопасности администрации Турковского муниципального района.

Настоящая Политика определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПД) в администрации Турковского муниципального района. Политика определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации, а также требования к сотрудникам, являющимися пользователями информационных систем персональных данных в администрации Турковского муниципального района, степень их ответственности, должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в администрации Турковского муниципального района.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПД с позиции комплексного применения технических и организационных мер и средств защиты.

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

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности администрации Турковского муниципального района, а также организационных и распорядительных документов, обеспечивающих ее реализацию.

Политика является основой для:

 принятия управленческих решений и разработки практических мер по реализации политики и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПД;

 разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПД в информационных системах персональных данных администрации Турковского муниципального района.

Основными нормативными правовыми и методическими документами, на которых базируется настоящая Политика, являются:

Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

 Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;

 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»;

 приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Во исполнение настоящей Политики в администрации Турковского муниципального района утверждаются следующие локальные нормативные правовые акты:

 Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Турковского муниципального района и подведомственных организациях и предприятиях;

 перечень персональных данных, обрабатываемых в администрации

Турковского муниципального района и перечня информационных систем персональных данных;

 перечень информационных систем персональных данных администрации Турковского муниципального района;

 перечень должностей служащих администрации Турковского муниципального района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

 модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных администрации Турковского муниципального района;

 должностная инструкция ответственного за организацию обработки персональных данных в администрации Александрово-Гайско муниципального района;

 должностная инструкция ответственного за защиту информации в администрации Турковского муниципального района;

 акты определения уровня защищенности персональных данных при их обработке в информационных системах администрации Турковского муниципального района;

 план проведения периодических проверок условий обработки персональных данных в администрации Турковского муниципального района;

 правила рассмотрения запросов субъектов персональных данных или их представителей администрацией Турковского муниципального района;

 порядок доступа муниципальных служащих администрации Турковского муниципального района в помещения, в которых ведется обработка персональных данных

 иные локальные документы администрации Турковского муниципального района, принимаемые во исполнение требований действующих нормативных правовых актов Российской Федерации в области обработки персональных данных.

# Общие положения

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение, реагирование на УБПД, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

# Область действия

Выполнение положений настоящей Политики информационной безопасности является обязательным для всех сотрудников, являющихся пользователями информационных систем персональных данных администрации Турковского муниципального района.

# Основные принципы обеспечения информационной безопасности информационных систем персональных данных администрации Турковского муниципального района

**Определенность целей.** Функциональные цели и цели информационной безопасности информационных систем персональных данных администрации Турковского муниципального района должны быть явно определены. Неопределенность приводит к «расплывчатости», невозможности оценки адекватности принятых защитных мер.

**Своевременность обнаружения проблем.** Необходимо своевременно обнаруживать проблемы, потенциально способные повлиять на функциональные цели и цели информационной безопасности информационных систем персональных данных администрации Турковского муниципального района.

**Прогнозируемость развития проблем.** Необходимо выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

**Оценка влияния проблем на функциональные цели.** Необходимо адекватно оценивать степень влияния выявленных проблем на функциональные цели информационных систем персональных данных администрации Турковского муниципального района.

**Адекватность защитных мер.** Необходимо выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

**Эффективность защитных мер.** Необходимо эффективно реализовывать принятые защитные меры.

**Использование опыта при принятии и реализации решений.** Необходимо накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

**Контролируемость защитных мер.** Необходимо применять только те защитные меры, правильность работы которых может быть проверена, при этом необходимо регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на функциональные цели и цели информационной безопасности информационных систем персональных данных администрации Турковского муниципального района.

# Общие условия обработки персональных данных

 Обработка персональных данных в администрации Турковского муниципального района осуществляется на основе следующих принципов:

Обработка персональных данных должна осуществляться на законной и справедливой основе.

Обработка персональных данных должна быть ограничена достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Допускается обработка исключительно тех персональных данных, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

Не допускается обработка персональных данных, излишних по отношению к заявленным целям обработки.

При обработке персональных данных должна быть обеспечена точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Неполные или неточные данные должны быть удалены или уточнены.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законодательством.

По достижении целей обработки или в случае утраты необходимости в достижении этих целей, персональные данные должны быть уничтожены или обезличены, если иное не предусмотрено федеральным законодательством.

Администрация Турковского муниципального района при обработке персональных данных обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

. Обеспечение безопасности персональных данных достигается, в частности:

определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

восстановлением персональных данных, модифицированных или
уничтоженных вследствие несанкционированного доступа к ним;

установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Перечень персональных данных, обрабатываемых в информационных системах персональных данных администрации Турковского муниципального района, утверждается распоряжением администрации Турковского муниципального района и по мере изменения состава обрабатываемых персональных данных подлежит пересмотру и уточнению.

Субъектами персональных данных, обработка которых осуществляется в информационных системах персональных данных администрации Турковского муниципального района, являются:

сотрудники администрации Турковского муниципального района;

субъекты персональных данных, не являющиеся сотрудниками администрации Турковского муниципального района, обратившиеся с целью получения государственных или муниципальных услуг.

Цели обработки персональных данных

Целями обработки персональных данных работников администрации Турковского муниципального района являются:

организация учета персонала администрации Турковского муниципального района для обеспечения соблюдения требований действующих нормативных правовых актов;

реализация администрацией Турковского муниципального района обязательств, в рамках трудовых правоотношений (на основании заключенных с работниками администрации Турковского муниципального района трудовых договоров и действующих нормативных правовых актов), а также обязательств, связанных с трудовыми правоотношениями, предусмотренных действующим законодательством Российской Федерации;

оказание гражданам государственных и муниципальных услуг администрацией Турковского муниципального района.

Целью обработки персональных данных физических лиц является осуществление возложенных на администрацию Турковского муниципального района функций в соответствии с главой 14 Трудового кодекса Российской Федерации от 30.12.2001 г. № 197-ФЗ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 06.10.2003 г. №131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральным законом от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», другими нормативными правовыми актами Российской Федерации, подлежащими применению при осуществлении администрацией Турковского муниципального района деятельности по решению вопросов местного значения, закрепленных в Уставе Турковского муниципального района Саратовской области.

Целью обработки персональных данных представителей юридических лиц, заключивших с администрацией Турковского муниципального района договоры, является, заключение и исполнение администрацией Турковского муниципального района договора с юридическим лицом и взаимодействие с представителями юридических лиц, связанное с исполнением заключенных администрацией Турковского муниципального района договоров.

При определении объема и содержания обрабатываемых персональных данных субъектов ПД администрация Турковского муниципального района руководствуется вышеуказанными целями получения и обработки персональных данных.

Доступ работников администрации Турковского муниципального района к персональным данным, подлежащим обработке, разрешен только уполномоченным работникам в соответствии с Перечнем должностей служащих администрации Турковского муниципального района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным. При этом указанным лицам предоставляется доступ только к персональным данным, необходимым для выполнения их служебных обязанностей в пределах задач и функций их подразделений.

Порядок доступа субъекта персональных данных к его персональным данным, обрабатываемым в информационных системах персональных данных администрации Турковского муниципального района, осуществляется в соответствии с Федеральным законом № 152-ФЗ «О персональных данных» и определяется Положением об обработке персональных данных в администрации Турковского муниципального района.

Перечень информационных систем персональных данных администрации Турковского муниципального района утверждается главой администрации Турковского муниципального района.

 Организация и проведение мероприятий по обеспечению защиты персональных данных в администрации Турковского муниципального района осуществляется в соответствии с Положением по организации и обеспечении защиты персональных данных в администрации Турковского муниципального района.

Общее руководство организацией работ по защите персональных данных в администрации Турковского муниципального района осуществляет ответственный по организации и контролю мероприятий по защите персональных данных в администрации Турковского муниципального района.

В целях обеспечения мероприятий, предусмотренных действующим законодательством Российской Федерации в области обработки персональных данных, в администрации Турковского муниципального района назначен работник, ответственный за:

доведение до сведения работников администрации Турковского муниципального района положений законодательства Российской Федерации о персональных данных, локальных актов администрации Турковского муниципального района по вопросам обработки персональных данных, требований к защите персональных данных;

осуществление внутреннего контроля за соблюдением администрацией Турковского муниципального района и работниками администрации Турковского муниципального района законодательства Российской Федерации о персональных данных при обработке персональных данных в информационных системах персональных данных администрации Турковского муниципального района, в том числе требований к защите персональных данных, обрабатываемых в информационных системах персональных данных администрации Турковского муниципального района;

осуществление внутреннего контроля за соблюдением администрацией Турковского муниципального района и работниками администрации Турковского муниципального района законодательства Российской Федерации о персональных данных при обработке персональных данных без использования средств автоматизации (на бумажных носителях), а также за организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов.

Деятельность администрации Турковского муниципального района по обеспечению безопасности персональных данных контролируется уполномоченным органом по защите прав субъектов персональных данных.

# Система защиты персональных данных

Система защиты персональных данных (СЗПД), строится на основании:

 акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных;

 модели угроз безопасности персональных данных;

 руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПД в информационных системах персональных данных администрации Турковского муниципального района. На основании анализа актуальных угроз безопасности ПД, описанного в Модели угроз безопасности персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПД.

# Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных администрации Турковского муниципального района подразделяются на:

законодательные (правовые);

морально-этические;

организационные (административные);

физические;

технические (аппаратные и программные).

**Законодательные (правовые) меры защиты**

К законодательным (правовым) мерам защиты относятся действующие законы Российской Федерации, указы и нормативные акты, регламентирующие правила обращения с ПД, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПД, и являющиеся сдерживающим фактором для потенциальных нарушителей.

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

**Морально-этические меры защиты**

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

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

**Организационные (административные) меры защиты**

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования информационных систем персональных данных администрации Турковского муниципального района, использование ресурсов информационных систем персональных данных, деятельность обслуживающего персонала, 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 – сформировать основные подходы к защите информации и обеспечить их выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация подходов к защите ПД в информационных системах персональных данных администрации Турковского муниципального района состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность информационных систем персональных данных в целом. Примером таких решений могут быть:

 принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПД, определение ответственных за ее реализацию;

 формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПД;

 принятие решений по вопросам реализации программы безопасности, которые рассматриваются в администрации Турковского муниципального района Саратовской области;

 обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

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

 какова область применения политики безопасности ПД;

 каковы роли, обязанности и ответственность должностных лиц, отвечающих за проведение политики безопасности ПД;

 кто имеет права доступа к ПД;

 какие меры и средства защиты использовать;

 какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры:

 учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных администрации Турковского муниципального района; лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным;

 для выбора и реализации методов и способов защиты информации в информационных системах персональных данных администрации Турковского муниципального района требуется назначить структурное подразделение или должностное лицо (работника), ответственное за обеспечение безопасности персональных данных;

 обучение лиц, использующих средства защиты информации, применяемые в информационных системах персональных данных администрации Турковского муниципального района, правилам работы с ними;

 разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

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

 соблюдение требований регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационных систем персональных данных администрации Турковского муниципального района;

 соблюдение требований регламента доступа в помещения с компонентами информационных систем персональных данных администрации Турковского муниципального района;

 соблюдение требований инструкций пользователей информационных систем персональных данных администрации Турковского муниципального района (администратора информационной безопасности).

**Физические меры защиты**

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

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

**Технические (аппаратно-программные) средства защиты ПД**

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 (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

 обеспечена физическая целостность всех компонентов информационных систем персональных данных администрации Турковского муниципального района;

 каждый сотрудник (пользователь информационной системы персональных данных) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

 сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

 ответственным за защиту информации, осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

# Контроль эффективности системы защиты информационных систем персональных данных администрации Турковского муниципального района

Внутренний контроль осуществляется в целях определения соответствия обработки персональных данных в администрации Турковского муниципального района требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

Внутренний контроль организуется путем проведения ежегодных проверок условий обработки персональных данных в администрации Турковского муниципального района согласно графику, утверждаемому Главой администрации Турковского муниципального района. При необходимости могут проводиться внеплановые поверки.

 График проверок ежегодно, доводится до сведения всех сотрудников, осуществляющих обработку персональных данных, которые обязаны создать проверяющим необходимые для проверки условия и предоставить соответствующие документы.

 Указанные проверки осуществляются ответственным за организацию обработки персональных данных в администрации Турковского муниципального района либо комиссией, создаваемой распоряжением администрации Турковского муниципального района.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных в администрации Турковского муниципального района либо председатель комиссии докладывает Главе администрации Турковского муниципального района в форме письменного заключения.

Ответственный за организацию обработки персональных данных в администрации Турковского муниципального района контролирует устранение в срок выявленных нарушений.

Текущий контроль за соблюдением требований нормативных правовых актов, регламентирующих правила обработки персональных данных, осуществляет ответственный за организацию обработки персональных данных в администрации Турковского муниципального района

# Пользователи информационных систем персональных данных администрации Турковского муниципального района

В информационных системах персональных данных администрации Турковского муниципального района можно выделить следующие группы пользователей, участвующих в обработке ПД:

 ответственный за организацию обработки персональных данных ;

 ответственный за защиту информации (ОЗИ);

 операторы АРМ;

Ответственный за защиту информации − сотрудник, ответственный за настройку, внедрение и сопровождение информационных систем персональных данных администрации Турковского муниципального района, функционирование СЗПД. Обеспечивает функционирование подсистемы управления доступом информационной системы персональных данных и уполномочен осуществлять предоставление конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные. Обеспечивает комплексную защиты информации. Участвует в обследовании, аттестации и категорировании объектов защиты. Разработка организационно-распорядительных документов, регламентирующих работу по защите информации.

**Ответственный за защиту информации** обладает следующим уровнем доступа и знаний:

 обладает полной информацией о системном и прикладном программном обеспечении информационных систем персональных данных администрации Турковского муниципального района;

 обладает полной информацией о технических средствах и конфигурации информационных систем персональных данных администрации Турковского муниципального района;

 имеет доступ ко всем техническим средствам обработки информации и данным информационных систем персональных данных администрации Турковского муниципального района;

 обладает правами конфигурирования и административной настройки технических средств информационных систем персональных данных администрации Турковского муниципального района;

 имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационных систем персональных данных администрации Турковского муниципального района;

 имеет права доступа к конфигурированию технических средств сети;

 имеет физический доступ к техническим средствам обработки информации и средствам защиты.

**Ответственный за защиту информации** уполномочен:

Знакомиться   с   проектами  решений  руководства  администрации, касающимися его деятельности.
     Вносить    на    рассмотрение    руководства   предложения   по совершенствованию работы,  связанной  с  обязанностями,  предусмотренными настоящей инструкцией.

Получать    от    руководителей    структурных   подразделений, специалистов информацию  и  документы,  необходимые  для выполнения своих должностных обязанностей.
 Привлекать специалистов всех структурных подразделений администрации для решения, возложенных на него обязанностей (если это предусмотрено положениями о структурных подразделениях, если нет – с разрешения руководителя администрации).

Требовать от  руководства  администрации  оказания  содействия  в исполнении своих должностных обязанностей и прав

1. **Оператор АРМ** − пользователем является каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ
ИСПДн.

Оператор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

Знать и строго выполнять правила работы со СЗИ.

Соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

Во время работы с защищаемой информацией экран монитора в помещении располагать так, чтобы исключалась возможность несанкционированного ознакомления с
отображаемой на нем информацией посторонними лицами, шторы (жалюзи) на оконных проемах должны быть завешаны.

Обо всех выявленных нарушениях, связанных с обработкой ПДн обратиться к ответственному за защиту информации.

Заблокировать доступ при отсутствии визуального контроля за рабочей станцией.

# Требования к персоналу по обеспечению защиты ПД

Все пользователи информационных систем персональных данных администрации Турковского муниципального района должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемому объекту и соблюдению принятого режима безопасности ПД.

Пользователи информационных систем персональных данных администрации Турковского муниципального района должны быть ознакомлены со сведениями настоящей Политики, принятых процедур работы с элементами информационных систем персональных данных администрации Турковского муниципального района и СЗПД.

Пользователи информационных систем персональных данных администрации Турковского муниципального района, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Пользователи информационных систем персональных данных администрации Турковского муниципального района должны следовать установленным процедурам поддержания режима безопасности ПД при выборе и использовании паролей (если не используются технические средства аутентификации).

Пользователи информационных систем персональных данных администрации Турковского муниципального района должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Пользователю запрещается:

Разглашать защищаемую информацию по Перечню ПДн, подлежащих защите, третьим лицам.

Копировать защищаемую информацию на неучтенные носители информации.

Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

Самостоятельно устанавливать, тиражировать, или модифицировать
программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств ИСПДн.

Подключать личные внешние носители и мобильные устройства к техническим
средствам ИСПДн.

Отключать (блокировать) СЗИ ИСПДн.

Обрабатывать информацию и выполнять работы, не предусмотренные
Разрешительной системой доступа к информационным ресурсам, программным и
техническим средствам ИСПДн.

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты
доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки средств
ИСПДн.

При работе с ПД в информационных системах персональных данных администрации Турковского муниципального района пользователи обязаны обеспечить отсутствие возможности просмотра ПД третьими лицами с мониторов АРМ.

Сотрудники, использующие информационные системы персональных данных администрации Турковского муниципального района, должны быть проинформированы об угрозах нарушения режима безопасности ПД и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПД.

Пользователи информационных систем персональных данных администрации Турковского муниципального района обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы системы, могущих повлечь за собой угрозы безопасности ПД, а также о выявленных ими событиях, затрагивающих безопасность ПД, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПД.

# Должностные обязанности пользователей информационных систем персональных данных администрации Александров-Гайского муниципального района

Должностные обязанности пользователей информационных систем персональных данных администрации описаны в следующих документах:

инструкция ответственного за защиту информации;

инструкция ответственного за организацию обработки персональных данных;

инструкция пользователя информационной системы персональных данных администрации Турковского муниципального района.

# Ответственность пользователей информационных систем персональных данных администрации Турковского муниципального района

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 предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Ответственный по защите информации несет ответственность:

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных трудовым законодательством Российской Федерации.

За совершенные в процессе осуществления своей деятельности правонарушения - в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации.

За причинение материального ущерба - в пределах, определенных трудовым, уголовным и гражданским законодательством Российской Федерации.При нарушениях сотрудниками администрации Турковского муниципального района – пользователей информационных систем персональных данных правил, связанных с безопасностью ПД, они несут ответственность, установленную действующим законодательством Российской Федерации.

При нарушениях сотрудниками администрации Турковского муниципального района – пользователей информационных систем персональных данных правил, связанных с безопасностью ПД, они несут ответственность, установленную действующим законодательством Российской Федерации.

**Руководитель аппарата**

**администрации муниципального района О. Н. Орлова**