

**АДМИНИСТРАЦИЯ ЕКАТЕРИНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**САРАТОВСКОЙ ОБЛАСТИ**

**ПОСТАНОВЛЕНИЕ**

**от 12.07.2016 г. № 370**

р.п. Екатериновка

**Об утверждении Политики администрации
Екатериновского муниципального района
Саратовской области в отношении
обработки персональных данных**

 В соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне», Указом Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», постановлением Правительства Российской Федерации от 21 марта 2012г. № 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», на основании Устава Екатериновского муниципального района

ПОСТАНОВЛЯЮ:

 1. Утвердить Политику администрации Екатериновского муниципального района Саратовской области в отношении обработки персональных данных согласно приложению.
 2. Ответственному за организацию обработки персональных данных в администрации Екатериновского муниципального района ознакомить служащих администрации Екатериновского муниципального района, непосредственно осуществляющих обработку персональных данных, с положением настоящего постановления.
 3. Контроль за исполнением настоящего постановления возложить на заместителя главы, руководителя аппарата администрации Екатериновского муниципального района Л.В. Антошину.

**Глава администрации
Екатериновского
муниципального района С.Б. Зязин**

Приложение к постановлению администрации
Екатериновского муниципального района
от 12.07.2016 г. № 370

**Политика**

**администрации Екатериновского муниципального района**

**в отношении обработки персональных данных**

**Термины и определения**

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

**Оператор** - администрация Екатериновского муниципального района Саратовской области. Юридическое лицо, исполнительно-распорядительный орган местного самоуправления, наделенный, согласно Уставу Екатериновского муниципального района Саратовской области, полномочиями по решению вопросов местного значения и полномочиями для осуществления отдельных государственных полномочий, переданных органам местного самоуправления федеральными законами и законами Саратовской области, и не входящий в систему органов государственной власти.

**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.

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

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

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

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

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1. Введение

Политика администрации Екатериновского муниципального района в отношении обработки персональных данных (далее - Политика) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется администрация Екатериновского муниципального района в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных администрации Екатериновского муниципального района позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

1. 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 угрозы безопасности персональных данных, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1. Правовая основа документа

Настоящая Политика разработана с учетом следующих документов:

* Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
* Федеральный закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне»;
* Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных»;
* Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
* постановление Правительства Российской Федерации от 21 марта 2012г. № 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 2012г. № 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 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденные приказом Гостехкомиссии от 30 августа 2002г. № 282.
1. Объекты защиты

Основными объектами системы безопасности персональных данных в администрации Екатериновского муниципального района являются:

* информационные ресурсы с ограниченным доступом, содержащие персональные данные;
* процессы обработки персональных данных в информационных системах персональных данных администрации Екатериновского муниципального района, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.
1. Цели и задачи обеспечения безопасности персональных данных
	1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных администрации Екатериновского муниципального района являются:

* администрация Екатериновского муниципального района, как собственник информационных ресурсов;
* руководство и сотрудники администрации Екатериновского муниципального района, в соответствии с возложенными на них функциями;
* граждане, обращающиеся в администрацию Екатериновского муниципального района по вопросам, относящимся к компетенции администрации Екатериновского муниципального района.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

* своевременного доступа к необходимым им персональным данным (их доступности);
* достоверности (полноты, точности, адекватности, целостности) персональных данных;
* конфиденциальности (сохранения в тайне) персональных данных;
* защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
* разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
* возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
* защиты персональных данных от незаконного распространения.
	1. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений администрации Екатериновского муниципального района от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

* доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем персональных данных администрации Екатериновского муниципального района, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
* целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах персональных данных администрации Екатериновского муниципального района и передаваемой по каналам связи;
* конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

* 1. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности администрации Екатериновского муниципального района должна обеспечивать эффективное решение следующих задач:

* своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем персональных данных администрации Екатериновского муниципального района;
* создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
* создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
* защиту от вмешательства в процесс функционирования информационных систем персональных данных администрации Екатериновского муниципального района посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам администрации Екатериновского муниципального района (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
* обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* защиту от несанкционированной модификации используемых в информационных системах персональных данных администрации Екатериновского муниципального района программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
* защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.
	1. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

* строгим учетом всех подлежащих защите ресурсов информационных систем персональных данных администрации Екатериновского муниципального района (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
* журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;
* полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов администрации Екатериновского муниципального района по вопросам обеспечения безопасности персональных данных;
* назначением должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
* наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам администрации Екатериновского муниципального района;
* четким знанием и строгим соблюдением всеми пользователями информационных систем администрации Екатериновского муниципального района требований организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных;
* персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам администрации Екатериновского муниципального района;
* непрерывным поддержанием необходимого уровня защищенности элементов информационной среды администрации Екатериновского муниципального района;
* применением физических и технических (программно-аппаратных) средств защиты ресурсов информационных систем персональных данных и непрерывной административной поддержкой их использования;
* эффективным контролем над соблюдением пользователями информационных ресурсов администрации Екатериновского муниципального района требований по обеспечению безопасности информации;
* юридической защитой интересов администрации Екатериновского муниципального район при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.
1. Основные принципы построения системы безопасности персональных данных

Построение системы, обеспечение безопасности персональных данных администрации Екатериновского муниципального района и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

* законность;системность;комплексность;непрерывность;своевременность;преемственность и непрерывность совершенствования;разумная достаточность (экономическая целесообразность);персональная ответственность;минимизация полномочий;исключение конфликта интересов;взаимодействие и сотрудничество;гибкость системы защиты;открытость алгоритмов и механизмов защиты;простота применения средств защиты;обоснованность и техническая реализуемость;специализация и профессионализм;обязательность контроля.
	1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных администрации Екатериновского муниципального района в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации Российской Федерации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем персональных данных администрации Екатериновского муниципального района должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

* 1. Системность

Системный подход к построению системы защиты информации в администрации Екатериновского муниципального района предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем персональных данных администрации Екатериновского муниципального района, а также характер, возможные объекты и направления атак на них со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

* 1. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

* 1. Непрерывность защиты

Обеспечение безопасности персональных данных – процесс, осуществляемый руководством администрации Екатериновского муниципального района, администратором безопасности информационных систем персональных данных и сотрудниками всех уровней. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности администрации Екатериновского муниципального района, и ее эффективность зависит от участия руководства администрации Екатериновского муниципального района в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

* 1. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, включающий постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

* 1. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем персональных данных администрации Екатериновского муниципального района и системы ее защиты с учетом изменений в методах и средствах перехвата информации, а также нормативных требований по защите информации.

* 1. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем персональных данных администрации Екатериновского муниципального района. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

* 1. Персональная ответственность

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

* 1. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

* 1. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями администрации Екатериновского муниципального района. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

* 1. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе администрации Екатериновского муниципального района. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администратора безопасности информационных систем персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в администрации Екатериновского муниципального района является высокая культура работы с информацией. Все сотрудники администрации Екатериновского муниципального района должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

* 1. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления администрацией Екатериновского муниципального района своей деятельности. В число таких изменений входят:

* изменения организационной и штатной структуры администрации Екатериновского муниципального района;
* изменение существующих или внедрение принципиально новых информационных систем;
* новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

* 1. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

* 1. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

* 1. Обоснованность и техническая реализуемость

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

* 1. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами администрации Екатериновского муниципального района (ответственным специалистом по технической защите информации).

* 1. Обязательность контроля

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

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

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками администрации Екатериновского муниципального района, должны немедленно доводиться до сведения главы администрации Екатериновского муниципального района и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

1. Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов
	1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы администрации Екатериновского муниципального района подразделяются на:

* правовые; морально-этические;технологические; организационные (административные); физические; технические (аппаратурные и программные).
	+ 1. **Правовые меры защиты**

К правовым мерам защиты относятся действующие законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем персональных данных администрации Екатериновского муниципального района.

* + 1. **Морально-этические меры защиты**

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или администрации Екатериновского муниципального района в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы.

* + 1. **Технологические меры защиты**

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

* + 1. **Организационные (административные) меры защиты**

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

* 1. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения безопасности персональных данных, отражающую подходы к защите персональных данных, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в администрации Екатериновского муниципального района целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность администрации Екатериновского муниципального района в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

* определение ролей и обязанностей должностных лиц, отвечающих за проведение политики безопасности персональных данных;
* разграничение прав доступа к персональным данным и т.д.

Политика нижнего уровня должна:

* предусматривать регламент информационных отношений, исключающих возможность произвольных или несанкционированных действий в отношении информационных ресурсов;
* определять принципы и методы разграничения доступа к персональным данным;
* выбирать программно-технические (аппаратные) средства противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.
	1. Регламентация доступа в помещения

Компоненты информационных систем администрации Екатериновского муниципального района должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, автоматизированных рабочих мест и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем администрации Екатериновского муниципального района, запираются на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

* 1. Регламентация допуска сотрудников к использованию информационных ресурсов

Допуск пользователей к работе с информационными системами персональных данных администрации Екатериновского муниципального района и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

* каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходимо работать в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информационных систем персональных данных.

Все сотрудники администрации Екатериновского муниципального района и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов информационных систем.

Обработка персональных данных в компонентах информационных систем персональных данных администрации Екатериновского муниципального района должна производиться в соответствии с утвержденными технологическими инструкциями.

* 1. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников администрации Екатериновского муниципального района, с которых возможен доступ к ресурсам информационных систем персональных данных, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационных систем персональных данных и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

* 1. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

* 1. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем персональных данных администрации Екатериновского муниципального района, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в администрации Екатериновского муниципального района.

Все пользователи информационных систем персональных данных администрации Екатериновского муниципального района должны быть ознакомлены с организационно–распорядительными документами по обеспечению безопасности персональных данных, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

* 1. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем персональных данных администрации Екатериновского муниципального района

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению главы администрации Екатериновского муниципального района.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

* индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
* проверка подлинности пользователей (аутентификация) на основе паролей;
* реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).
	1. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности администрации Екатериновского муниципального района используются следующие средства защиты:

* физические средства;технические средства;средства идентификации и аутентификации пользователей;средства разграничения доступа;средства обеспечения и контроля целостности;средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационных систем персональных данных администрации Екатериновского муниципального района, независимо от их вида и формы представления информации в них.

* + 1. Физические средства защиты

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

Для обеспечения физической безопасности компонентов информационных систем персональных данных администрации Екатериновского муниципального района необходимо осуществлять ряд организационных и технических мероприятий, включающих проверку оборудования, предназначенного для обработки персональных данных, на введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных, а также оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

* + 1. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

* средства разграничения доступа к данным;средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач: идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств; регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам; защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ; регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

* защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.
	+ 1. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем персональных данных администрации Екатериновского муниципального района посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

* путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);путем проверки знания ими паролей;путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.
	+ 1. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

* на контролируемую территорию;в отдельные помещения;к компонентам информационной среды администрации Екатериновского муниципального района и элементам системы защиты персональных данных (физический доступ);к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);к активным ресурсам (прикладным программам, задачам и т.п.);к операционной системе, системным программам и программам защиты.
	+ 1. Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов систем персональных данных администрации Екатериновского муниципального района предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

* средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
* средствами электронной подписи;
* средствами подсчета контрольных сумм (для используемого программного обеспечения).
	+ 1. Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

* ведения и анализа журналов регистрации событий безопасности (системных журналов);
* получения твердой копии (печати) журнала регистрации событий безопасности;
* упорядочения журналов, а также установления ограничений на срок их хранения;
* оперативного оповещения администратора информационной безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

* дата и время события;
* идентификатор субъекта, осуществляющего регистрируемое действие;
* действие (тип доступа).
	1. Контроль эффективности системы защиты

Контроль эффективности системы защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.