Утверждена

приказом Министерства земельных и имущественных отношений

Республики Татарстан

от «10» мая 2016 г. № 227-пр

**ПОЛИТИКА**

**безопасности персональных данных в информационных системах**

**персональных данных Министерства земельных и имущественных**

**отношений Республики Татарстан**

г. Казань

2016

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

В настоящем документе используются следующие сокращения:

|  |  |
| --- | --- |
| **Сокращение** | **Полное наименование** |
| **УФСБ России по РТ** | Управление Федеральной службы безопасности России по Республике Татарстан |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |
| **Роскомнадзор** | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций России |
| **МИС РТ** | Министерство информатизации и связи Республики Татарстан |
| **Министерство** | Министерство земельных и имущественных отношений Республики Татарстан |
| **ГУП «ЦИТ РТ»** | Государственное унитарное предприятие Республики Татарстан «Центр информационных технологий Республики Татарстан» |
| **ИТ** | Информационно – технологическая инфраструктура |
| **НСД** | Несанкционированный доступ |
| **ПДн** | Персональные данные |
| **ПТК** | Программно-технический комплекс |
| **СЗПДн** | Система защиты персональных данных |
| **СКЗИ** | Средство криптографической защиты информации |
| **УБПДн** | Угрозы безопасности персональных данных |
| **ИСПДн** | Информационная система персональных данных |
| **СЗИ** | Система защиты информации |
| **ПДТК** | Постоянно действующая техническая комиссия по защите государственной тайны |

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Информационная система – совокупность содержащихся в базах данных

информации и обеспечивающих ее обработку информационных технологий и

технических средств.

Информационная система персональных данных – 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.

Нарушитель безопасности персональных данных – физическое лицо случайно или преднамеренно совершающее действия, следствием которых является нарушение заданных характеристик безопасности персональных данных при их обработке в информационной системе 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.

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.

Система защиты персональных данных – совокупность организационных мер и средств защиты информации, включающих средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно – технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии.

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1**.1. Назначение Политики**

Политика защиты персональных данных в информационных системах персональных данных Министерства является документом, определяющим общие принципы обеспечения безопасности ПДн и организационно – технические меры по защите ПДн в ИСПДн Министерства.

Настоящая Политика разработана на основе анализа требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты ПДн, с учетом современного состояния и стратегии развития информационных технологий, целей, задач и правовых основ создания и эксплуатации информационных систем, режимов функционирования, а также на основе анализа УБПДн.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению защиты персональных данных в ИСПДн Министерства, а также нормативных и методических документов, обеспечивающих жизненный цикл СЗПДн Министерства.

Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн ИСПДн Министерства от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на сотрудников Министерства назначенных приказом Министерства.

1.2. **Правовые основы обеспечения безопасности ПДн в ИСПДн Министерства**

Политика разработана в целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Министерства.

Правовую основу Политики составляют Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации, Федеральные законы РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ и Республики Татарстан, нормативные правовые акты (приказы, распоряжения) федеральных органов исполнительной власти, органов власти Республики Татарстан обеспечения безопасности и технической защиты информации.

**2. СФЕРА ДЕЙСТВИЯ И ОБЛАСТЬ РАСПРОСТРАНЕНИЯ ПОЛИТИКИ**

Сфера действия Политики распространяется на все подразделения Министерства.

Областью распространения Политики являются информационные системы персональных данных Министерства.

**3. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**

**ПЕРСОНАЛЬНЫХ ДАННЫХ**

Основной целью обеспечения безопасности персональных данных является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности ПДн.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту персональных данных и может проявляться в виде:

- нанесения вреда здоровью субъекта персональных данных;

- незапланированных и (или) непроизводительных финансовых или

материальных затрат субъекта;

- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;

- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с персональными данными.

Основной задачей обеспечения безопасности персональных данных, при их обработке в информационных системах персональных данных Министерства, является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно – технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения.

**4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В**

**ИНФОРМАЦИОННЫХ СИСТЕМАХ МИНИСТЕРСТВА**

4.1. **Категории субъектов персональных данных**

Персональные данные, которые обрабатываются в информационных системах Министерства, подразделяются на две категории:

- персональные данные сотрудников Министерства;

- персональные данные физических лиц, которые обратились в Министерство либо с целью получения услуг, либо с целью трудоустройства.

4.2. **Цели обработки персональных данных**

В основе определения целей обработки персональных данных лежит принцип законности их обработки.

Целями обработки персональных данных сотрудников являются содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности сотрудников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества.

При определении целей обработки персональных данных иных категорий субъектов персональных данных, необходимо соблюдать законы и иные нормативно – правовые акты.

4.3. **Характеристики безопасности персональных данных**

Персональные данные, обрабатываемые в информационных системах Министерства, должны обладать свойством конфиденциальности, а также могут рассматриваться и другие характеристики безопасности. В частности, к таким характеристикам относятся: целостность, доступность, неотказуемость, учетность (подконтрольность), аутентичность (достоверность), адекватность.

Для обеспечения заданных характеристик безопасности ПДн данных необходимо реализовать минимальный и достаточный набор организационно –технических мер.

**5. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН В ИСПДН МИНИСТЕРСТВА**

Построение СЗПДн Министерства и ее функционирование должны

осуществляться в соответствии со следующими основными принципами:

- законность;

- системность;

- комплексность;

- непрерывность;

- своевременность;

- преемственность и непрерывность совершенствования;

- разумная достаточность и адекватность;

- персональная ответственность;

- минимизация полномочий;

- гибкость;

- открытость алгоритмов и механизмов защиты;

- научная обоснованность и техническая реализуемость;

- специализация и профессионализм;

- знание своих партнеров и работников;

- наблюдаемость и оцениваемость;

- обязательность контроля и оценки.

5.1. **Законность**

Защита ПДн в ИСПДн Министерства основывается на положениях и

требованиях существующих законов, стандартов и нормативно – методических

документов по защите ПДн.

5.2. **Системность**

Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн Министерства.

5.3. **Комплексность**

Безопасность ПДн обеспечивается комплексом программно – технических средств и поддерживающих их организационных мер, реализованных Министерством. Применение различных средств и технологий защиты информации должно перекрывать все существенные (значимые) каналы реализации угроз безопасности ПДн и не содержать слабых мест в согласовании применяемых средств и технологии защиты информации.

СЗПДн должна строиться с учетом не только всех известных каналов проникновения и НСД к ПДн, но и с учетом возможности повышения уровня защиты по мере выявления новых источников УБПДн, развития способов и средств их реализации в ИСПДн.

СЗПДн Министерства строится на основе единой технической политики, с использованием функциональных возможностей информационных технологий, реализованных в информационной системе и имеющихся систем и средств защиты в соответствии с разработанными типовыми моделями угроз.

5.4. **Непрерывность**

Защита ПДн должна обеспечиваться на всех технологических этапах обработки ПДн и во всех режимах функционирования, в том числе при проведении регламентных работ.

5.5. **Своевременность**

Принимаемые меры по обеспечению безопасности ПДн должны носить упреждающий характер.

Министерство принимает необходимые меры по защите ПДн до начала обработки ПДн, которые должны обеспечить надлежащий уровень безопасности

ПДн.

СЗПДн разрабатывается одновременно с разработкой и развитием ИСПДн Министерства, что позволяет учитывать требования по безопасности ПДн при проектировании и модернизации ИСПДн. 5.6. **Преемственность и непрерывность совершенствования**

Предполагают постоянное совершенствование мер и средств защиты ПДн на основе результатов анализа функционирования ИСПДн и СЗПДн с учетом выявления новых способов и средств реализации УБПДн, отечественного и зарубежного положительного опыта в сфере защиты информации.

Министерство должно определять действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности ПДн с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать возможным негативным последствиям.

5.7. **Разумная достаточность и адекватность**

Состояние и стоимость реализации мер защиты должно быть соизмеримы с рисками, связанными с обработкой и характером защищаемых ПДн.

Анализ рисков нарушения безопасности ПДн проводится в целях определения влияния системы защиты информации на вероятность реализации угроз безопасности ПДн с учетом уязвимостей (дефектов) ИТ – инфраструктуры Министерства.

Программно – технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн Министерства.

5.8. **Персональная ответственность**

Ответственность за обеспечение безопасности ПДн в ИСПДн Министерства возлагается на каждого сотрудника в пределах его полномочий.

Распределение обязанностей и полномочий работников Министерства должно обеспечивать выявление виновных лиц в случаях нарушения безопасности ПДн.

Роли и обязанности сотрудников должны быть определены и документально подтверждены в соответствии с организационной политикой в области защиты информации. 5.9. **Минимизация полномочий**

Предоставление и использование прав доступа к ПДн должно быть ограничено и управляемо.

Пользователям должны предоставляться минимальные права доступа к ПДн в ИСПДн только в соответствии с производственной необходимостью.

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

Пользователю должны быть запрещены все операции с ПДн за исключением тех, которые разрешены явно.

5.10. **Гибкость**

В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категория обрабатываемых Министерством ПДн.

Для обеспечения возможности варьирования уровня защищенности ПДн, СЗПДн Министерства должна обладать определенной гибкостью.

5.11. **Открытость алгоритмов и механизмов защиты**

Защита ПДн не должна осуществляться только за счет сокрытия структуры, технологий и алгоритмов функционирования СЗПДн.

Знание указанных характеристик СЗПДн не должно давать возможности преодоления защиты возможными нарушителями безопасности ПДн, включая разработчиков средств защиты.

5.12. **Научная обоснованность и техническая реализуемость**

Уровень рекомендаций и требований по защите ПДн должен соответствовать имеющемуся уровню развития информационных технологий и средств защиты информации.

При создании и эксплуатации СЗПДн необходимо ориентироваться на лучшие современные отечественные и зарубежные технические решения и практику защиты информации. 5.13. **Специализация и профессионализм**

Реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн должна осуществляться профессионально подготовленными специалистами Министерства.

5.14. **Знание своих партнеров и работников**

Министерство должен обладать информацией о своих партнерах, позволяющей минимизировать вероятность реализации УБПДн, источники которых связаны с человеческим фактором.

Министерство должно реализовывать кадровую политику (тщательный подбор персонала и мотивация работников), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими сотрудниками.

5.15. **Наблюдаемость и оцениваемость обеспечения безопасности**

**персональных данных**

Предлагаемые Министерством меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен федеральными органами исполнительной власти и органами власти Республики Татарстан, осуществляющими функции по контролю и надзору в пределах своих полномочий.

5.16. **Обязательность контроля и оценки**

Неотъемлемой частью работ по защите ПДн является оценка эффективности системы защиты.

С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн Министерством должны быть определены процедуры для постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля должны регулярно анализироваться.

Приложение 1. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1) Доктрина информационной безопасности Российской Федерации.

Утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895

2) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных

данных»

3) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации,

информационных технологиях и о защите информации»

4) Указ Президента Российской Федерации от 06.03.1997 № 188 «Об

утверждении перечня сведений конфиденциального характера»

5) Трудовой кодекс Российской Федерации

6) Гражданский кодекс Российской Федерации

7) Постановление Правительства Российской Федерации от 01.11.2012

№ 1119 «Об утверждении требований к защите персональных данных при их

обработке в информационных системах персональных данных»

8) Постановление Правительства Российской Федерации от 15.09.2008

№ 687 «Об утверждении Положения об особенностях обработки персональных

данных, осуществляемой без использования средств автоматизации»

9) Постановление Правительства Российской Федерации от 06.07.2008

№ 512 «Об утверждении требований к материальным носителям биометрических

персональных данных и технологиям хранения таких данных вне информационных

систем персональных данных»

10) Приказ Федеральной службы по техническому и экспортному контролю от

18.02.2013 № 21 «Об утверждении Состава и содержания организационных и

технических мер по обеспечению безопасности персональных данных при их

обработке в информационных системах персональных данных»

11) Приказ Федеральной службы по техническому и экспортному контролю от

11.02.2013 № 17 «Об утверждении требований о защите информации, не

составляющей государственную тайну, содержащейся в государственных

информационных системах»