АДМИНИСТРАЦИЯ ГОРОДА РЯЗАНИ

РАСПОРЯЖЕНИЕ

13 января 2020 г. № 8-р

Об утверждении Политики информационной безопасности информационных систем в администрации города Рязани

В целях обеспечения информационной безопасности информационных систем в администрации города Рязани, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом 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», руководствуясь статьями 39, 41 Устава муниципального образования – городской округ город Рязань:

1. Утвердить Политику информационной безопасности информационных систем в администрации города Рязани (далее – Политика) согласно приложению к настоящему распоряжению.

2. Руководителям структурных подразделений администрации города Рязани и муниципальных казенных учреждений города Рязани, имеющих доступ к информационным системам администрации города Рязани, обеспечить выполнение положений Политики.

3. Признать утратившим силу распоряжение администрации города Рязани от 16.03.2018 № 458-р «Об утверждении Политики информационной безопасности информационных систем в администрации города Рязани».

4. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации В.С. Бурмистрова.

Глава администрации Е.Б. Сорокина

ПРИЛОЖЕНИЕ
к распоряжению администрации города Рязани
от 13 января 2020 г. № 8-р

Политика
информационной безопасности информационных систем
в администрации города Рязани

1. Общие положения

1.1. Информационная безопасность информационных систем в администрации города Рязани (далее – информационная безопасность) – это состояние защиты конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах в администрации города Рязани.

1.2. Политика информационной безопасности информационных систем в администрации города Рязани (далее – Политика) определяет защищаемую информацию и основные меры защиты информации, принимаемые в администрации города Рязани.

1.3. Политика регламентирует вопросы защиты информации, обрабатываемой в информационных системах (далее – ИС) в администрации города Рязани.

1.4. При реализации Политики должны соблюдаться требования технических регламентов и нормативных правовых актов федеральных, региональных органов государственной власти, администрации города Рязани, регулирующих вопросы создания, эксплуатации информационных систем и защиты информации.

2. Защищаемая информация

В соответствии с требованиями настоящей Политики защите подлежит следующая информация, обрабатываемая в ИС, не содержащая сведений, составляющих государственную тайну (далее – информация):

2.1. «Открытая информация» – информация, официально распространяемая администрацией города Рязани и не имеющая ограничений доступа:

– информация, размещаемая на официальном сайте администрации города Рязани;

– информация, обрабатываемая с помощью автоматизированных информационных технологий, официально предоставляемая администрацией города Рязани внешним потребителям.

Меры защиты «Открытой информации» должны обеспечивать целостность и доступность информации.

2.2. «Внутренняя информация» – информация, обрабатываемая в ИС администрации города Рязани.

Меры защиты «Внутренней информации» должны обеспечивать целостность и доступность информации для работников администрации города Рязани.

2.3. «Конфиденциальная информация» – информация, ограничение доступа к которой установлено в соответствии с требованиями действующего законодательства, а также правовыми актами администрации города Рязани в порядке, установленном действующим законодательством:

– персональные данные;

– служебная информация.

Меры защиты «Конфиденциальной информации» должны обеспечивать целостность, доступность, конфиденциальность информации.

3. Угрозы безопасности информации

3.1. Угрозы безопасности информации – это совокупность потенциально возможных процессов и событий, реализация которых может нанести ущерб защищаемой информации.

3.2. Для ИС в администрации города Рязани характерны следующие особенности:

– возрастающий удельный вес автоматизированных процедур в общем объеме процессов обработки информации;

– территориальная распределенность ИС;

– усложнение режимов функционирования ИС;

– долговременное хранение информации на машинных носителях;

– одновременный доступ к информации большого числа пользователей.

В связи с этим существует необходимость в обеспечении целостности, доступности и конфиденциальности информации, обрабатываемой в ИС.

Угрозы для информации, обрабатываемой в ИС, исходят:

– от утечки по техническим каналам;

– от использования протоколов межсетевого взаимодействия;

– от специальных программ-вирусов;

– от несанкционированного доступа;

– от несанкционированного изменения и удаления информации;

– от временного прекращения доступа к информации.

3.3. Наиболее опасные источники угроз и пути их реализации:

3.3.1. «Внутренние, непреднамеренные источники» – случайные действия работников структурных подразделений администрации города Рязани (далее – работники).

Основные пути реализации «Внутренних, непреднамеренных источников» угроз:

– непреднамеренное разглашение, передача или утрата атрибутов разграничения доступа;

– некомпетентное использование средств защиты информации;

– несанкционированный запуск программ, способных при некомпетентном использовании вызывать изменение и удаление информации.

3.3.2. «Внутренние, преднамеренные источники» – преднамеренные действия работников. Основные пути реализации «Внутренних, преднамеренных источников» угроз:

– преднамеренное разглашение, передача атрибутов разграничения доступа;

– несанкционированное распространение и использование информации;

– хищение информации;

– копирование носителей информации;

– несанкционированное использование терминалов;

– блокирование и отключение средств защиты информации;

– несанкционированное внедрение и использование программ, способных привести к потере и искажению информации;

– несанкционированное изменение и удаление информации;

– преднамеренное включение в библиотеки программ специальных блоков типа «троянских коней».

3.3.3. «Внешние источники» – преднамеренные или непреднамеренные действия со стороны лиц, не являющихся работниками.

Основные пути реализации «Внешних источников» угроз:

– получение атрибутов разграничения доступа;

– несанкционированный доступ к информации, ее распространение и использование;

– злоумышленный вывод из строя средств защиты;

– несанкционированное изменение и удаление информации;

– воздействие на ИС программных и технических средств, позволяющих выполнить обращение к объектам доступа в обход средств защиты;

– блокирование и отключение средств защиты информации;

– незаконное подключение к аппаратуре или линиям связи ИС.

4. Меры защиты информации

4.1. В целях реализации Политики разрабатывается нормативная и методическая документация, регламентирующая вопросы информационной безопасности, принимаются организационные и технические меры защиты информации.

4.2. Принимаемые в администрации города Рязани меры защиты информации должны быть адекватны угрозам безопасности информации.

4.3. В структурных подразделениях администрации города Рязани должны обеспечиваться организационные и технические меры защиты информации.

4.4. Организационные меры защиты информации:

4.4.1. Перечень ИС, предназначенных для обработки защищаемой информации, должен быть утвержден правовым актом администрации города Рязани.

4.4.2. Регламентация вопросов информационной безопасности, связанных с работниками, должна включать:

– ознакомление работников с положениями законодательства Российской Федерации, региональных органов государственной власти, нормативных правовых актов администрации города Рязани, регулирующих отношения по вопросам защиты информации;

– письменное оформление обязательства работников о неразглашении конфиденциальной информации;

– письменное оформление оператором ИС доступа работников к информации и операциям с информацией. Необходимость предоставления работникам доступа к информации и операциям с информацией определяется руководителем структурного подразделения, оператором ИС.

4.4.3. Порядок доступа к ресурсам информационно-телекоммуникационной сети определяется в соответствии с правовыми актами администрации города Рязани.

4.4.4. Пользование глобальной информационной сетью Интернет и электронной почтой должно осуществляться в соответствии с правовыми актами администрации города Рязани.

4.4.5. Доступ к программным средствам обработки информации должен производиться в соответствии с правовыми актами администрации города Рязани.

4.4.6. Антивирусная защита программных средств обработки информации должна обеспечиваться в соответствии с правовыми актами администрации города Рязани.

4.4.7. Парольная защита информационно-телекоммуникационной сети, программных средств обработки информации должна обеспечиваться в соответствии с правовыми актами администрации города Рязани.

4.5. Технические меры защиты информации:

4.5.1. Разграничение прав доступа пользователей и обслуживающего персонала ИС (далее – персонал) к информации, программным и техническим средствам, средствам защиты информации ИС.

4.5.2. Ограничение доступа персонала в помещения, где размещены средства хранения и обработки информации, носители информации, коммуникационное оборудование.

4.5.3. Регистрация действий персонала ИС, контроль несанкционированного доступа и действий персонала и посторонних лиц.

4.5.4. Учет и надежное хранение машинных носителей конфиденциальной информации, их обращение, исключающее хищение, подмену, уничтожение.

4.5.5. Резервирование средств хранения и обработки информации, дублирование информации и машинных носителей информации.

4.5.6. Использование сертифицированных, серийно выпускаемых в защищенном исполнении технических средств обработки, хранения и передачи информации.

4.5.7. Использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости.

4.5.8. Использование сертифицированных средств защиты информации.

4.5.9. Защита цепей электропитания.

4.5.10. Использование защищенных каналов связи.

4.5.11. Размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр.

4.5.12. Организация защиты помещений и технических средств ИС с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение технических средств и носителей информации.

4.5.13. Предотвращение внедрения в ИС программ-вирусов, программных закладок.

4.5.14. Оснащение автоматизированных рабочих мест программными средствами, средствами защиты информации и конфигурирование их в соответствии с возложенными на работников обязанностями.

5. Ответственность за обеспечение информационной безопасности

5.1. Структурные подразделения администрации города Рязани принимают меры защиты информации и несут ответственность за выполнение требований настоящей Политики и документов, регламентирующих информационную безопасность, действующих на ее основе.

5.2. Управление делами аппарата администрации города Рязани несет ответственность за реализацию и актуализацию Политики, организует и контролирует деятельность структурных подразделений администрации города Рязани по обеспечению информационной безопасности, проводит проверку информационной безопасности ИС.

6. Проверка информационной безопасности

6.1. Проверка информационной безопасности проводится с целью определения соответствия мер защиты информации текущим угрозам безопасности информации и реализации Политики.

6.2. Проверка информационной безопасности организуется управлением делами аппарата администрации города Рязани.