АДМИНИСТРАЦИЯ ГОРОДА РЯЗАНИ

РАСПОРЯЖЕНИЕ

06 июля 2010 г. № 1201-р

Об утверждении Политики информационной безопасности
автоматизированных информационных систем
администрации города Рязани

В целях обеспечения информационной безопасности автоматизированных информационных систем администрации города Рязани, руководствуясь статьями 39, 41 Устава муниципального образования – городской округ город Рязань Рязанской области:

1. Утвердить прилагаемую Политику информационной безопасности автоматизированных информационных систем администрации города Рязани.

2. Руководителям структурных подразделений при создании и эксплуатации автоматизированных информационных систем обеспечить выполнение положений настоящей Политики.

3. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Т.В.Гредневу.

Глава администрации О.В.Шишов

УТВЕРЖДЕНА
распоряжением администрации города Рязани
от «06» июля 2010 г. № 1202-р

Политика информационной безопасности автоматизированных информационных систем администрации города Рязани

1. Общие положения

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

1.2. Политика информационной безопасности автоматизированных информационных систем 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 автоматизированных информационных системах администрации города Рязани (далее – АИС).

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

2. Защищаемая информация

В соответствии с требованиями настоящей Политики защите подлежит следующая информация, обрабатываемая в АИС, 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 АИС администрации города Рязани.

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

2.3. «Конфиденциальная информация» – информация, ограничение доступа к которой установлено в соответствии с требованиями действующего законодательства, а так же нормативными 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 АИС администрации города Рязани характерны следующие особенности:

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

– территориальная распределенность АИС;

– интеграция в базах данных информации различного назначения;

– усложнение режимов функционирования АИС;

– долговременное хранение информации на машинных носителях;

– одновременный доступ к информации большого числа пользователей;

– интенсивный обмен информацией между АИС.

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

Угрозы для информации, обрабатываемой в АИС, исходят:

– от утечки по техническим каналам;

– 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 сотрудников структурных подразделений администрации города, муниципальных предприятий и учреждений (далее – сотрудники).

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 сотрудников.

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 сотрудниками.

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 АИС 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 АИС.

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, муниципальных предприятиях и учреждениях, обрабатывающих в защищаемую информацию, должны обеспечиваться организационные и технические меры защиты информации.

4.4. Организационные меры защиты информации:

4.4.1. Создание, модернизация и эксплуатация АИС, обрабатывающих защищаемую информацию, должны осуществляться в соответствии с Регламентом создания и эксплуатации автоматизированных информационных систем администрации города Рязани, утвержденным постановлением администрации города Рязани от 30.05.2008 № 2866.

4.4.2. АИС, предназначенные для обработки защищаемой информации, должны быть зарегистрированы в Реестре информационных ресурсов и систем муниципального образования – город Рязань, в соответствии с Положением о реестре информационных ресурсов и систем муниципального образования – город Рязань, утвержденным постановлением главы администрации города Рязани от 03.11.2005 № 4003.

4.4.3. Работы по проектированию и монтажу информационно-телекоммуникационных сетей организуются в соответствии с Регламентом обеспечения подразделений администрации города Рязани средствами вычислительной и множительной техники, комплектующими и расходными материалами, утвержденным постановлением главы администрации города Рязани от 23.07.2008 № 4054, и производятся специализированными организациями.

4.4.4. Ремонт технических средств АИС должен производиться в соответствии с Регламентом ремонта и технического обслуживания средств вычислительной техники,

копировальных аппаратов и телекоммуникационного оборудования, утвержденным постановлением администрации города Рязани от 19.03.2007 № 762.

4.4.5 Регламентация вопросов информационной безопасности, связанных с сотрудниками должна включать:

– письменное оформление обязательства сотрудников о неразглашении конфиденциальной информации;

– письменное оформление оператором АИС доступа сотрудников к информации и операциям с информацией. Необходимость предоставления сотрудникам доступа к информации и операциям с информацией определяется руководителем структурного подразделения, оператором АИС;

– включение в должностные инструкции сотрудников обязанностей по защите информации и ответственности за нарушение мер защиты информации.

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

4.4.7. Информационный обмен между подразделениями, юридическими и физическими лицами должен осуществляться в соответствии с Положением об информационных ресурсах муниципального образования – город Рязань, утвержденным постановлением главы администрации города Рязани от 03.11.2005 № 4003.

4.4.8. Пользование глобальной информационной сетью «Интернет» и электронной почтой должны осуществляться в соответствии с нормативными правовыми актами администрации города Рязани.

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

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

4.5. Технические меры защиты информации.

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

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 АИС, 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 физической защиты помещений и технических средств АИС 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 АИС программ-вирусов, программных закладок.

4.5.14. Оснащение автоматизированных рабочих мест программными средствами и конфигурирование их в соответствии с возложенными на сотрудников обязанностями, согласно Паспорту установки программного обеспечения на компьютер.

5. Ответственность за обеспечение информационной безопасности

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

5.2. Отдел автоматизированных средств обработки информации и управления несет ответственность за реализацию и актуализацию Политики, организует и контролирует деятельность структурных подразделений администрации города, муниципальных предприятий и учреждений по обеспечению информационной безопасности, проводит аудит информационной безопасности АИС.

6. Аудит информационной безопасности

6.1. Аудит информационной безопасности проводится с целью определения соответствия мер защиты информации, текущим угрозам безопасности информации и реализации настоящей Политики в администрации города Рязани.

6.2. Аудит информационной безопасности организуется отделом автоматизированных средств обработки информации и управления.