УДК 004 **Информационные технологии**

Рысаев Ильшат Шавалиевич
Башкирский государственный университет
г.Уфа, Российская Федерация
Саитов Салават Ленатович
Башкирский государственный университет
г.Уфа, Российская Федерация

ОБЩИЕ ВОПРОСЫ УПРАВЛЕНИЯ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНАХ МЕСТНОГО САМОУПРАВЛЕНИЯ

Аннотация: рассматриваются общие вопросы управления системой защиты информации в органах местного самоуправления, вызванные высоким темпом развития информационных технологий, большим объемом данных, обрабатываемых в информационных системах и, как следствие, возникновение новых угроз безопасности этих сведений, а значит и требований, предъявляемых системе информационной безопасности.

Ключевые слова: защита информации, информация ограниченного доступа, персональные данные, информационная безопасность, органы местного самоуправления.

Abstract: general issues of managing information protection systems in local governments are considered, caused by the high rate of development of information technologies, large amounts of data processed in information systems and, as a result, the emergence of new threats to the security of this information, and hence the requirements for information security system.

Keywords: information security, restricted access information, personal data, information security, local governments.

Деятельность администраций во многом зависит от эффективной работы с информацией любого вида. Сведения конфиденциального характера занимают особую роль, так как их утечка может повлечь за собой необратимые негативные последствия, в том числе и материальные. Стоит также отметить, что в органах местного самоуправления сосредоточены данные различной степени важности, вопрос ее защиты является очень серьезным и актуальным.

Изначально информацию принято подразделять на два вида: открытую (общедоступную) и закрытую (ограниченного доступа). Сведения с грифом: персональные данные, для служебного пользования и т.д. - относят ко второму виду. Следовательно, обеспечение безопасности таких сведений должно быть на соответствующем уровне.

Для эффективного обеспечения информационной безопасности необходимо комплексно проанализировать все возможные каналы утечки информации, а также выявить наиболее вероятные сценарии несанкционированного доступа со стороны злоумышленника. На основании полученных результатов проектируется система защиты информации. Она представляет собой совокупность средств и методов, объединенных целевым назначением обеспечения состояния защищенности сведений, обрабатываемых в автоматизированной системе обработки данных (АСОД) [1, с.10].

Согласованное взаимодействие средств и методов защиты является важной составляющей эффективного обеспечения информационной безопасности.

Заинтересованность органов исполнительной власти в информационной сфере обуславливается созданием условий для гармонично развивающейся муниципальной инфраструктуры. С одной стороны, ее целью является реализация прав и свобод человека и гражданина, то есть осуществление беспрепятственного доступа к открытой информации. С другой стороны, необходимо обеспечить защиту сведений конфиденциального характера согласно действующему законодательству Российской Федерации.

Сравнительно недавно в Гражданский кодекс было введено понятие «цифровые права», где таковыми признаются обязательственные и иные права, содержание и условие осуществления которых определяются правилами информационных систем. Исходя из этого, можно сделать вывод, что новых способов, технических средств и методов для защиты этих прав в настоящее время не применяется. Носители информации в материальной форме подлежат защите физической, данные в электронной форме будут храниться на электронных носителях информации и их безопасность будет обеспечиваться техническими средствами АСОД.

Необходимость повышенного внимания к вопросам защиты информации в орга6нах местного самоуправления обуславливаются следующими факторами [2, с. 66]:

- зависимость эффективной работы администраций районов от их способности обеспечить доступность, целостность и своевременность информации;
- использование информационных систем, обрабатывающих большие объемы сведений различной степени важности, а также уязвимость данных систем от возможности несанкционированного доступа, в том числе и в результате непреднамеренных действий, повлекших за собой утечку информации;
- возрастающее количество преступлений в сфере информационных технологий.

Существует три основных признака классификации данных, подлежащих защите: по принадлежности (праву собственности), по степени секретности, а также по содержанию [3, с. 76].

Стоит также обратить внимание на широкое использование сети Интернет в органах местного самоуправления. Этот факт повышает вероятность реализации угроз защищенности информационных ресурсов. Одним из наиболее известных каналов утечки информации является электронная почта. Письма, содержащие персональные данные

государственных служащих или другие сведения ограниченного доступа, могут стать лёгкой добычей для злоумышленников. Кроме того, реализация угрозы может произойти не только от целенаправленных действий, но и по неосторожности самих работников государственного или муниципального органа. Данная проблема может быть решена путём правового регулирования использования глобальной сети. Должен быть установлен порядок и условия обмена информацией в сети с целью защиты законных прав собственников этих сведений [4, с. 90].

Техническая часть защиты информации в рамках данной статьи подробно рассматриваться не будет, однако следует отметить следующее: при использовании сети Интернет для передачи информации ограниченного доступа (кроме сведений, содержащих государственную тайну) должны использоваться механизмы шифрования данных. При обработке сведений, содержащих информацию, составляющую государственную тайну, на автоматизированных рабочих местах подключение к сети строго запрещено.

Основной целью защиты информации в органах местного самоуправления является предотвращение реализации угроз безопасности информации путём:

- минимизации вероятности утечки, хищения, утраты, искажения, подделки сведений и блокирования доступа к ним;
- обеспечения правового режима документированной информации как объекта собственности;
- защиты прав субъектов в информационных процессах при разработке, производстве и применении информационных систем.

Объективная оценка защиты информации основывается на постоянном и действенном контроле её состояния.

Контроль состояния системы защиты информации в органах местного самоуправления производится уполномоченными органами. Он заключается в проверке соответствия системы требованиям безопасности, в периодическом контроле защищенности и в оценке эффективности принятых мер по

информационной безопасности. Данные мероприятия проводятся с использованием специализированных программных и технических средств контроля [5, с. 754].

Таким образом, были рассмотрены общие вопросы обеспечения информационной безопасности в органах местного самоуправления. Система защиты сведений ограниченного доступа должна балансировать между конституционными правами человека и гражданина на информационное обеспечение в полной мере и законодательством Российской Федерации, регулирующим доступ к сведениям конфиденциального характера. Другими словами, система защиты информации должна учитывать интересы граждан как потребителей информации, а также интересы граждан как владельцев информации. Кроме того, невозможно обойти вопрос и о правомерности, эффективности принятых мер, а также их экономической целесообразности.

Библиографический список:

1. Воробьева О.В. Особенности совершенствования информационной безопасности районной (муниципальной) администрации // Парадигмальные основания государственного управления, сравнительный анализ опыта регионов стран СНГ. Сборник научных статей IV международной научной конференции – 2015. - С. 174-178.

2. Бузов Г.А. Защита от утечки информации по техническим каналам // Учебное пособие Г.А. Бузов, С.В. Калинин, А.В.Кондратьев. - М.: Горячая линия - Телеком, 2015. - С. 416.

3. Гришина, Н.В. Организация комплексной системы защиты информации // Н.В. Гришина.- М.: Гелиос АРВ, 2017.

4. Ханнанова Т.Р., Гарифуллина А.Ф. Развитие государственных и муниципальных услуг в цифровой экономике // Экономика и управление: научно-практический журнал. 2018. №6 (144). С. 90-93.

5. Ханнанова Т.Р., Гарифуллина А.Ф. Актуальные вопросы развития государственных и муниципальных услуг населению в условияхцифровой экономик // Финансовая экономика. 2018. №5. С.753-755.