КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО В МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЯХ: МЕТОДЫ ЗАЩИТЫ ДОКУМЕНТОВ В АДМИНИСТРАЦИИ ГОРОДА ОРЛА

Чихачёва Д.М.
Орловский государственный институт искусств и культуры
Орёл, Россия

В настоящее время вопросы организации работы с конфиденциальными документами организации и методы их защиты достаточно актуальны, так как в современном развитии экономики России и в условиях ужесточения конкурентной борьбы на рынке, ценные и конфиденциальные документы организации всё чаще становятся объектом пристального внимания со стороны конкурентов и подвергаются различным формам шпионажа и атак.

Документ является конфиденциальным, если он содержит, хотя бы один из информационных показателей, отнесенных Перечнем [1] к тайне учреждения. Использование любых конфиденциальных сведений запрещается в нешифрованной переписке, телеграммах, телетайпограммах, факсограммах, электронных сообщениях, в телефонных переговорах, общении с посетителями, в средствах массовой информации и т.п.

Персональную ответственность за сохранность и правильное использование конфиденциальных документов, их обработку, рассмотрение, исполнение и хранение несут руководители всех рангов. Сотрудники учреждений несут персональную ответственность за обеспечение конфиденциальности доверенных им сведений, соблюдение требований по работе с конфиденциальными документами и базами данных, сохранность используемых ими документов и других материалов, отнесенных перечнями к секретам учреждения.

Выполнение технологических стадий, процедур и операций по обработке и хранению конфиденциальных документов возлагается на службу конфиденциальной документации (КД), подчиненной непосредственно первому руководителю учреждения или руководителю службы безопасности [4, с. 31].

В целях предупреждения разглашения сведений конфиденциального характера в системе исполнительных органов государственной власти Орловской области Губернатором выносится специальное постановление об утверждении правил обращения с информацией ограниченного доступа [2]. Правила устанавливают порядок обращения с носителями информации ограниченного доступа в муниципальных учреждениях. Под «носителями информации ограниченного доступа» понимаются материальные объекты, в том числе физические поля, в которых информация ограниченного доступа находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Перечень сведений конфиденциального характера администрации г. Орла разрабатывается на основании Перечня сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.97 №188 [1], рассматривается на заседаниях постоянно действующей технической комиссии по защите государственной тайны администрации Орловской области и утверждается Губернатором области.

К методам защиты документов ограниченного доступа, практикуемым в администрации г. Орла, относятся:

а) аппаратные методы защиты, к которым относятся различные электронные устройства:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- устройства измерения индивидуальных характеристик человека с целью его идентификации;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

б) программные методы защиты, к которым относятся специальные программы, предназначенные для выполнения функций защиты, включаемые в состав программного обеспечения систем обработки данных. По функциональному назначению они делятся на следующие группы:

- идентификация технических средств, задач и пользователей;
- определения и ограничения дней и времени работы пользователей;
- контроль работы технических средств и пользователей;
- регистрация работы технических средств и пользователей при обработке информации ограниченного доступа;
- уничтожения информации в запоминающих устройствах после её использования;
- сигнализации при несанкционированных действиях;
- вспомогательные программы различного назначения: контроль работы механизма защиты, проставление грифа секретности на выдаваемых документах.

в) резервное копирование, которое заключается в хранении копии программ на носителе;

г) криптографическое шифрование информации, заключающееся в преобразовании защищаемой информации к непригодному для восприятия человеком виду;

д) физические меры защиты, к которым принадлежат различные устройства и сооружения, а также мероприятия, затрудняющие или делающие невозможным

проникновение потенциальных нарушителей в места доступа к защищаемой информации. Это меры физической изоляции сооружений с аппаратурой автоматизированной системы; оборудование входных дверей специальными замками, позволяющими регулировать доступ в помещения; организация системы охранной сигнализации и др.

е) организационные мероприятия по защите информации, которые включают нормативно-правовые акты, регламентирующие процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным. Организационные мероприятия создают надежный механизм защиты информации в администрации. Причины, по которым организационные мероприятия играют повышенную роль в механизме защиты, заключается в том, что возможности несанкционированного использования информации в значительной мере обуславливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью пользователей или персонала систем обработки данных. Влияние этих аспектов практически невозможно избежать или локализовать с помощью аппаратных и программных средств, криптографического закрытия информации и физических мер защиты. Для этого в администрации г. Орла используется совокупность организационных, организационно-технических и организационно-правовых мероприятий, которые исключают возможность возникновения опасности утечки конфиденциальной информации [3, с.4].

Техническая защита конфиденциальной информации в администрации г. Орла предусматривает комплекс организационных и технических мер, направленных на закрытие каналов утечки информации. Анализ и оценка источников угроз безопасности информации в администрации представлены в «Руководстве по защите информации от технических разведок и ее утечки по техническим каналам в администрации г. Орла». Техническая защита конфиденциальной информации в муниципальном учреждении осуществляется в порядке, установленном Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30.08.2002 №282. Выполнение перечисленных требований обеспечивает достаточный уровень защищенности конфиденциальных документов как в Администрации г. Орла, так и в любых учреждениях, работающих с конфиденциальными документами.

Список источников и литературы

1. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 6 марта 1997г. № 188) (с изменениями от 23 сентября 2005 г.) // Собрание законодательства РФ. – 2005. - №39. – С. 3925.

2. Положение о порядке обращения с информационными ресурсами конфиденциального характера в исполнительных органах местного самоуправления, муниципальных предприятиях и учреждениях г. Орла. - Орёл, 2008. – 11 с.
3. Положение о порядке работы сотрудников администрации г. Орла с конфиденциальной информацией от 28 декабря 2007 года. - Орёл, 2007. – 10 с.
4. Фатьянов, А.А. Концептуальные основы обеспечения безопасности на современном этапе / А.А. Фатьянов // Безопасность информационных технологий. - 2008. - № 1. - С. 26-40.