УДК 614.2

С.К. Варлатая, М.В. Шаханова

Проблемы защиты и обработки конфиденциальных документов

В настоящее время автоматизированные системы являются основой обеспечения практически любых бизнес-процессов как в коммерческих, так и в государственных организациях. Вместе с тем повсеместное использование автоматизированных систем для хранения, обработки и передачи информации приводит к обострению проблем, связанных с их защитой. Подтверждением этому служит тот факт, что за последние несколько лет в России и в ведущих зарубежных странах наблюдается тенденция увеличения числа информационных атак, приводящих к значительным финансовым и материальным потерям. Одной из наиболее опасных угроз конфиденциальной информации является утечка хранящейся и обрабатываемой внутри автоматизированных систем конфиденциальной информации. Всё это заставляет более пристально рассмотреть возможные каналы утечки конфиденциальной информации и предложить спектр технических решений, позволяющих предотвратить утечку данных.
Ключевые слова: Конфиденциальность, информация, документ, защита информации, риск.

Все информационные ресурсы фирмы постоянно подвергаются объективным и субъективным угрозам утраты носителя или ценности информации.

Риск угрозы дестабилизирующего воздействия любым (открытым и ограниченного доступа) информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам проявляется повышенный интерес со стороны различного рода злоумышленников.

В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использования в своих целях.

Проблемой создания системы защиты конфиденциальных документов является также угроза безопасности информационных ресурсов ограниченного распространения – это несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат — овладение информацией и противоправное ее использование или совершение иных дестабилизирующих действий. Целями и результатами несанкционированного доступа могут быть не только овладение ценными сведениями и их использование, но и их видоизменение, модификация, уничтожение, фальсификация, подмена и т.п.

Одна из основных проблем обработки конфиденциальных документов – это утрата информационных ресурсов ограниченного доступа, которая может наступить при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации; возникновении риска угрозы, организованной злоумышленником, или при случайно сложившихся обстоятельствах; наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией.

Эти условия могут включать: отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов; неэффективную систему защиты информации или отсутствие этой системы, что образует высокую степень уязвимости информации; непрофессионально организованную технологию обработки и хранения конфиденциальных документов; неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе; отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа; отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информацион-

ными ресурсами ограниченного доступа; бесконтрольное посещение помещений фирмы посторонними лицами.

Многие руководители отделов информационной безопасности, защищая корпоративную сеть предприятия, зачастую считают необходимым лишь выполнить то, что стоит у них в плане инвестиций, и переключиться на следующую задачу. Например, защищая периметр сети, обычно озадачиваются лишь выбором межсетевых экранов и схемой их установки. Далее экраны приобретаются в стандартной комплектации. Предусматривается режим их работы, производятся конфигурирование и настройки (обычно они остаются выполненными по умолчанию). Акт сдачи-приема работ подписан, межсетевые экраны работают, сеть защищена – все, можно переключаться на следующую задачу.

А дальше наблюдается следующая картина: администратор в отделе информационной безопасности, отвечающий за настройки экранов, не назначается, а сами экраны, установленные в центре обработки данных, никому на хранение не передаются, при этом пароль к консоли экрана известен всем сотрудникам, работающим в центре обработки данных. Такой подход к решению вопроса защиты сети приводит к тому, что буквально через 2 месяца межсетевые экраны будут защищать корпоративную сеть лишь на 30–40% от своих реальных возможностей, поскольку все, что можно выключить в их настройках, будет выключено с целью увеличения пропускной способности сети.

Можно даже не говорить о системах анализа содержимого, предназначенных для блокирования каналов утечки конфиденциальной информации под видом Веб-трафика, или системах анализа почтового трафика. И если их администрированием не занимается сотрудник отдела информационной безопасности, то они просто со временем будут выключены, чтобы не мешали, а трафик в каждом случае будет перенаправлен через обычные функциональные серверы.

Еще одна проблема защиты и обработки конфиденциальных документов – отсутствие взаимопонимания между сотрудниками отдела информационной безопасности и сотрудниками отдела информационных технологий.

Зачастую на предприятии можно встретить не только картину противостояния этих двух отделов, но и откровенно враждебные настроения их сотрудников по отношению друг к другу. Попытки свалить друг на друга максимально возможную ответственность, оставляя за собой лишь функции контроля, приводят в итоге не только к непониманию роли совместного выполнения задач по сохранению конфиденциальной информации, но и к созданию серьезных предпосылок к ее утрате.

Проблема безопасности информации в ЭВМ и локальной сети требует эффективной взаимосвязи машинной и внемашинной защиты конфиденциальных сведений. В этой связи важное, актуальное значение имеет защита технических носителей конфиденциальной информации (машиночитаемых документов) на внемашинных стадиях их учета, обработки и хранения. Именно на этих стадиях особенно велика вероятность утраты машиночитаемого документа. Подобная проблема несущественна для носителей, содержащих открытую информацию. Для сохранности носителей электронных конфиденциальных документов, находящихся вне машины, в настоящее время эффективно используются зарекомендовавшие себя принципы и методы обеспечения безопасности документов в традиционной технологической системе.

В настоящее время наиболее широко используется смешанная технологическая система обработки и хранения конфиденциальных документов, совмещающая традиционную и автоматизированную технологии. Выборочно автоматизируются: справочная и поисковая работа по бумажным документам, процедура составления и изготовления документов и учетных форм, контроль исполнения, сервисные задачи. Остальные стадии и процедуры выполняются в русле традиционной, делопроизводственной технологии (распределение бумажных документов, их рассмотрение, исполнение, оперативное и архивное хранение документов). В силу специфики обрабатываемых сведений о документах и самих документов автоматизированные системы делопроизводственной ориентации имеют в большинстве случаев информационно-справочный характер. Недостаток смешанной технологии состоит в неполном использовании преимуществ и функциональных возможностей компьютерной технологии, отчего сохраняются рутинные делопроизводственные операции, которые мешают совершенствовать документооборот.

Следовательно, традиционные и автоматизированные технологические системы обработки и хранения конфиденциальных документов представляют собой сложные комплексы, решающие задачи как документационного обеспечения необходимой информацией управленческой и производственной деятельности, так и одновременно достаточно надежной защиты документов от несанкционированного доступа и других возникающих угроз безопасности информационных ресурсов фирмы.

Литература

1. Варлатая С.К. Защита и обработка конфиденциальных документов: учеб.-метод. комплекс / С.К. Варлатая, М.В. Шаханова. – Владивосток: Изд-во ДВГТУ, 2009. – 276 с.

2. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

3. Бутакова Н.Г. Защита и обработка конфиденциальных документов / Н.Г. Бутакова, В.А. Семененко. – М.: Московский государственный индустриальный университет, 2008. – 283 с.

Варлатая Светлана Климентьевна
Дальневосточный государственный технический университет
Декан факультета информационных и компьютерных технологий, к.т.н., профессор

Шаханова Марина Владимировна
Дальневосточный государственный технический университет
Ст. преподаватель факультета информационных и компьютерных технологий
Эл. адрес: marinavl2007@yandex.ru

S.K. Varlatay, M.V. Shakhanova

The problems of the defence and processing of confidential documents

Nowdays the automatized systems are becoming the basis of providing of every business process in commercial and state institutions. At the same time the use of these systems for storing, processing and transmission of information leads to the aggravation of problems, connected with its defence. The acknowledgement of this fact is the tendency of increasing the informational attacks leading to considerable financial and material problems in Russia and the biggest European countries during some latest years. One of the most dangerous threat for confidential information is the leakage of processing information in automatized systems. It makes us look thoroughly at possible canals of leaking this information and suggest the spectrum of technical decisions, allowing to confirm the leakage of data.

Keywords: confidentiality, information, document, information security, risk.
