УДК 004.75

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

Бадекина-Рейзмир Екатерина Сергеевна, Коршак Татьяна Петровна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, badekina_k@mail.ru

В работе представлена информация о проблемах информационной безопасности организации, которая внедряет систему электронного документооборота, рассмотрены уровни СЭД, которые необходимо защищать, а так же определены основные способы и механизмы обеспечения их защиты.

ВСТУПЛЕНИЕ

При внедрении системы электронного документооборота (СЭД) нельзя забывать о безопасности системы – желающих полазить в чужих документах достаточно. Уже много лет пишутся целые книги о промышленном шпионаже, компьютерных преступлениях, а наиболее практичные уже не один год реализуют написанное на практике.

УРОВНИ СЭД ПОДЛЕЖАЩИЕ ЗАЩИТЕ

Базовый элемент любой СЭД – документ, внутри системы это может быть файл, а может быть запись в базе данных. Говоря о защищенном документообороте, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. В этом случае все сводится к уже банальной задаче защиты данных от несанкционированного доступа. Здесь есть большое заблуждение, ведь речь идет именно о защите системы, а не только о защите данных внутри нее. Это значит, что нужно защитить также ее работоспособность, обеспечить быстрое восстановление после повреждений, сбоев и даже после уничтожения. Система – это как живой организм, не достаточно защитить только содержимое его клеток, необходимо защитить также связи между ними и их работоспособность. Поэтому к защите системы электронного документооборота необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД. Начиная от защиты физических носителей информации, данных на них, и заканчивая организационными мерами. Для этого, при обеспечении информационной безопасности в СЭД, необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД:

- аутентификация пользователей системы;
- распределение прав доступа для сотрудников-пользователей СЭД;
- поддержка электронной цифровой подписи документов;
- шифрование писем и документов;
- ведение истории и статистики работы с документами;
- аудит работы пользователей в системе;
- обеспечения юридической значимости электронного документа [1].

ОСНОВНЫЕ СПОСОБЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ

Определив основной перечень уровней защиты СЭД, можно определить основные способы и механизмы обеспечения их защиты. Механизмы аутентификации могут быть различными, наиболее широко применяются такие криптографические алгоритмы, как RSA. Контроль доступа, дополняющий аутентификацию. Логический контроль доступа позволяет определять для каждого файла и для каждой прикладной программы правомочных пользователей и их права, таким образом контроль доступа решает, частично проблему аутентификации и распределение прав доступа. Конфиденциальность, обычно достигается криптографическими методами. Сохранение целостности информации – метод защиты от искажения или уничтожения чего – либо в данном сообщении. Использует сжатие информации и криптографию, методы восстановления, обеспечивающие работоспособность системы после устранения возникших проблем с безопасностью. Ведение учетных журналов позволяет воспроизвести последовательность выполнения операций со стороны центральной системы или со стороны терминала. Хронология, дает возможность избежать повтора последовательности операций. Система безопасности отдельного информационного комплекса. Позволяет удостовериться, что совокупность систем делает только то, что должны делать. Чтобы добиться этого, прибегают к сертификационной оценке программного и аппаратного обеспечения.[2]

ВЫВОДЫ

На основе вышеизложенного можно сделать следующие выводы: подходы к защите электронного документооборота должен быть комплексным, необходимо оценивать возможные угрозы и риски СЭД и величину возможных потерь от реализованных угроз. Как уже говорилось, защиты СЭД не сводится только лишь к защите документов и разграничению доступа к ним. Остаются вопросы защиты аппаратных средств системы, персональных компьютеров, принтеров и прочих устройств; защиты сетевой среды, в которой функционирует система,

защита каналов передачи данных и сетевого оборудования, возможно выделение СЭД в особый сегмент сети. Комплекс организационных мер играют роль на каждом уровне защиты, в него входят и инструктаж, и подготовка обычного персонала к работе с конфиденциальной информацией. Особой частью организационных мер нужно выделить изменения в должностных инструкциях, инструкции по использованию средств активной и пассивной защиты конфиденциальной информации, регламентные работы с персоналом, особенности работы администратора безопасности. К сожалению, организационные мероприятия по защите конфиденциальной информации на ряду, с техническими средствами информации, зачастую отодвигают на задний план, что при электронном документообороте является неотъемлемой составной информационно безопасности организации. [3]

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://www.cnews.ru
2. http://inf-bez.ru, http://ecm-journal.ru
3. http://www.mtron.ru