амплитуда колебаний на всех рассматриваемых участках снова увеличивается до значений, имеющих место при технологическом толчке механизмов головной части вследствие усиления влияния динамических процессов, возникающих при изменении скорости линии. Незначительное увеличение рабочей скорости, примерно на 7,5 м/мин, не дает видимых изменений. При выходе линии на максимальную рабочую скорость 200 м/мин амплитуды колебаний на всех рассматриваемых участках уменьшаются до допустимых значений за время 0,1 с.

В результате проведенных экспериментов установлено, что для исключения процесса складкообразования необходимо обеспечить демпфирование колебаний в полосе. Для достижения этой цели необходимо разработать математические и имитационные модели электромеханической системы ЛНГЦ с учетом изменяющихся свойств полосы и разработать технические решения, позволяющие решить эту проблему.

СПИСОК ЛИТЕРАТУРЫ

1. Светличный А., Лейковский К. Информационные и управляющие системы в металлургии // Современные технологии автоматизации. 2006. №3. С. 18-26.
2. Дубровский Е. Система контроля технологических параметров на литейных установках Ревдинского завода по обработке цветных металлов // Современные технологии автоматизации. 2007. № 1. С. 12 – 18.

УДК 004

Актуальные технологии защиты от утечки конфиденциальной информации

Б.Х. ШОДЫРОВА, *ст. преподаватель,*
Г.Т. ДАНЕНОВА, *к.т.н., доцент,*
Б.С. ЖЕКЕНОВА, *инженер ДУП,*
Карагандинский государственный технический университет

Ключевые слова: *информация, безопасность, компьютеры, системы, сервер, сеть, интернет, защита, шифрование, конфиденциальность, данные, автоматизация, схемы, доступ, пользователь, техническое решение, данные, ресурсы, топология, терминальный доступ.*

Информационной безопасности уделяют большое внимание. В ряде вузов введены или вводятся новые специальности, связанные с подготовкой кадров по проблемам информационной безопасности. Вместе с тем важно, чтобы каждый специалист, занимающийся разработкой вычислительной техники или программного обеспечения, или просто использующий ее в качестве пользователя, был знаком с проблемами информационной безопасности. Растущие потоки информации являются следствием развития общества и, в свою очередь, существенно влияют на его дальнейшее продвижение. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и внутренних [1].

Можно выделить следующие возможные каналы утечки конфиденциальной информации:

– несанкционированное копирование конфиденциальной информации на внешние носители и вынос её за пределы контролируемой территории предприятия. Примерами таких носителей являются флоппи-диски, компакт-диски CD-ROM, Flash-диски и др.;

– вывод на печать конфиденциальной информации и вынос распечатанных документов за пределы контролируемой территории. Необходимо отметить, что в данном случае могут использоваться как локальные принтеры, которые непосредственно подключены к компьютеру злоумышленника, так и удалённые, взаимодействие с которыми осуществляется по сети;

– несанкционированная передача конфиденциальной информации по сети на внешние серверы, расположенные вне контролируемой территории предприятия. Так, например, злоумышленник может передать конфиденциальную информацию на внешние почтовые или файловые серверы сети Интернет, а затем загрузить её оттуда, находясь дома или в любом другом месте. Для передачи информации нарушитель может использовать протоколы SMTP, HTTP, FTP или любой другой протокол в зависимости от настроек фильтрации исходящих пакетов данных, применяемых в автоматизированной системе. При этом с целью маскирования своих действий нарушитель может предварительно зашифровать отправляемую информацию или передать её под видом стандартных графических или видеофайлов при помощи методов стеганографии [2];

- хищение носителей, содержащих конфиденциальную информацию, – жёстких дисков, магнитных лент, компакт-дисков CD-ROM и др.

Считается, что в основе любой системы защиты от

атак, связанных с утечкой конфиденциальной информации, должны лежать организационные меры обеспечения безопасности. В рамках этих мер на предприятии должны быть разработаны и внедрены организационно-распорядительные документы, определяющие список конфиденциальных информационных ресурсов, возможные угрозы, которые с ними связаны, а также перечень тех мероприятий, которые должны быть реализованы для противодействия указанным угрозам. В дополнение к организационным средствам защиты должны применяться и технические решения, предназначенные для блокирования перечисленных выше каналов утечки конфиденциальной информации. Рассмотрим несколько различных способов защиты информации с учётом их преимуществ и недостатков.

Выделенный сегмент терминального доступа к конфиденциальной информации.

Один из способов защиты от утечки конфиденциальной информации заключается в организации доступа к конфиденциальной информации автоматизированной системы (АС) через промежуточные терминальные серверы. При такой схеме доступа пользователь сначала подключается к терминальному серверу, на котором установлены все приложения, необходимые для работы с конфиденциальной информацией. После этого пользователь в терминальной сессии запускает эти приложения и начинает работать с ними так, как будто они установлены на его рабочей станции (рисунок 1).

В процессе работы в терминальной сессии пользователю отсылается только графическое изображение рабочей области экрана, в то время как вся конфиденциальная информация, с которой он работает, сохраняется лишь на терминальном сервере. Один такой сервер, в зависимости от аппаратной и программной конфигурации, может одновременно обслуживать сотни пользователей. Практическое использование технического решения на основе терминального сервера позволяет обеспечить защиту от несанкционированного копирования конфиденциальной информации на внешние носители за счёт того, что вся информация хранится не на рабочих станциях, а на терминальном сервере. Аналогичным образом обеспечивается защита и от несанкционированного вывода документов на печать. Распечатать документ пользователь может только при помощи принтера, установленного в сегменте терминального доступа. При этом все документы, выводимые на этот принтер, могут регистрироваться в установленном порядке.

Использование терминального сервера позволяет также обеспечить защиту от несанкционированной передачи конфиденциальной информации по сети на внешние серверы вне пределов контролируемой территории предприятия. Достигается это путём фильтрации всех пакетов данных, направленных вовне сегмента терминального доступа, за исключением тех пакетов, которые обеспечивают передачу графического изображения рабочей области экрана на станции пользователей. Такая фильтрация может быть реализована при помощи межсетевого экрана, установленного в точке сопряжения сегмента терминального доступа с остальной частью АС. При этом сама рабочая станция может иметь беспрепятственный доступ к Интернет-ресурсам. Для обмена информацией между пользователями, работающими в терминальных сессиях, может использоваться выделенный файловый сервер, расположенный в терминальном сегменте доступа [3].

Средства контентного анализа исходящих пакетов данных.

Средства контентного анализа обеспечивают возможность обработки сетевого трафика, отправляемого за пределы контролируемой территории с целью выявления возможной утечки конфиденциальной информации. Используются они, как правило, для анализа исходящего почтового и web-трафика, отправляемого в сеть Интернет. Такие средства защиты устанавливаются в разрыв канала связи между сетью Интернет и АС предприятия таким образом, чтобы через них проходили все исходящие пакеты данных (рисунок 2).

Рисунок 1 – Схема установки терминального сервера доступа к конфиденциальным данным

Рисунок 2 – Схема установки средств контентного анализа в АС

В процессе анализа исходящих сообщений последние разбиваются на служебные поля, которые обрабатываются по критериям, заданным администратором безопасности. Так, например, средства контентного анализа позволяют блокировать пакеты данных, которые содержат такие ключевые слова, как «секретно», «конфиденциально» и др. Эти средства также предоставляют возможность фильтровать сообщения, которые направляются на внешние адреса, не входящие в систему корпоративного электронного документооборота. Преимуществом систем защиты данного типа является возможность мониторинга и накладывания ограничений как на входящий, так и исходящий поток трафика. Однако эти системы не позволяют гарантировать стопроцентное выявление сообщений, содержащих конфиденциальную информацию. В частности, если нарушитель перед отправкой сообщения зашифрует его или замаскирует под видом графического или музыкального файла при помощи методов стеганографии, то средства контентного анализа в этом случае окажутся практически бессильными.

Средства криптографической защиты конфиденциальной информации.

Для защиты от утечки информации могут использоваться и криптографические средства, обеспечивающие шифрование конфиденциальных данных, хранящихся на жёстких дисках или других носителях. При этом ключ, необходимый для декодирования зашифрованной информации, должен храниться отдельно от данных. Как правило, он располагается на внешнем отчуждаемом носителе, таком как ключ TouchMemory или USB-носитель. В случае если нарушителю и удастся украсть носитель с конфиденциальной информацией, он не сможет её расшифровать, не имея соответствующего ключа. Рассмотренный вариант криптографической защиты не позволяет заблокировать другие каналы утечки конфиденциальной информации, особенно если они совершаются пользователем после того, как он получил доступ к данным. С учётом этого недостатка компанией Microsoft была разработана технология управления правами доступа RMS (WindowsRightsManagementServices).

Ниже приводится обобщённый алгоритм использования технология RMS для формирования конфиденциальной информации пользователем «А» и последующего получения к ней доступа пользователем «Б» (рисунок 3):

На первом этапе пользователь «А» загружает с RMS-сервера открытый ключ, который впоследствии будет использоваться для шифрования конфиденциальной информации.

Далее пользователь «А» формирует документ с конфиденциальной информацией при помощи одного из приложений, поддерживающих функции RMS (например, при помощи MicrosoftWord). После этого пользователь составляет список субъектов, имеющих права доступа к документу, а также операции, которые они могут выполнять. Эта служебная информация записывается приложением в XML-файл, составленный на основе расширенного языка разметки прав доступа – eXtensiblerightsMarkupLanguage (XrML).

На третьем этапе приложение пользователя «А» зашифровывает документ с конфиденциальной информацией при помощи случайным образом сгенерированного симметричного сеансового ключа, который в свою очередь зашифровывается на основе открытого ключа RMS-сервера. С учётом свойств асимметричной криптографии расшифровать этот документ сможет только RMS-сервер, поскольку только он располагает соответствующим секретным ключом. Зашифрованный сеансовый ключ также добавляется к XML-файлу, связанному с документом.

Пользователь отправляет получателю «Б» зашифрованный документ вместе с XML-файлом, содержащим служебную информацию.

После получения документа пользователь «Б» открывает его при помощи приложения с функциями RMS.

Поскольку адресат «Б» не обладает ключом, необходимым для его расшифровки, приложение отправляет запрос к RMS-серверу, в который включается XML-файл и сертификат открытого ключа пользователя «Б».

Получив запрос, RMS-сервер проверяет права доступа пользователя «Б» к документу в соответствии с информацией, содержащейся в XML-файле. Если пользователю доступ разрешён, то тогда RMS-сервер извлекает из XML-файла зашифрованный сеансовый ключ, дешифрует его на основе своего секретного ключа и заново зашифровывает ключ на основе открытого ключа пользователя «Б». Использование открытого ключа пользователя позволяет гарантировать, что только он сможет расшифровать ключ.

На восьмом этапе RMS-сервер отправляет пользователю «Б» новый XML-файл, содержащий зашифро-

ванный сеансовый ключ, полученный на предыдущем шаге.

На последнем этапе приложение пользователя «Б» расшифровывает сеансовый ключ на основе своего закрытого ключа и использует его для открытия документа с конфиденциальной информацией. При этом приложение ограничивает возможные действия пользователя только теми операциями, которые перечислены в XML-файле, сформированном пользователем «А» [3].

В настоящее время одной из наиболее актуальных проблем в области информационной безопасности является проблема защиты от утечки конфиденциальной информации. Технические варианты решения данной проблемы, рассмотренные в статье, могут быть сгруппированы в два типа. Первый тип предполагает изменение топологии защищаемой АС путём создания изолированной системы обработки конфиденциальной информации либо выделения в составе АС сегмента терминального доступа к конфиденциальным данным. Второй вариант технических решений заключается в применении различных средств защиты АС, включая средства активного мониторинга, контентного анализа, а также средства криптографической защиты информации. Результаты анализа этих двух типов технических решений показали, что каждое из них характеризуется своими недостатками и преимуществами. Выбор конкретного средства защиты зависит от множества факторов, включая особенности топологии защищаемой АС, тип прикладного и общесистемного ПО, установленного в системе, количество пользователей, работающих с конфиденциальной информацией и многих других. При этом необходимо подчеркнуть, что наибольшая эффективность может быть получена при комплексном подходе, предусматривающем применение как организационных, так и технических мер защиты информационных ресурсов от утечки.

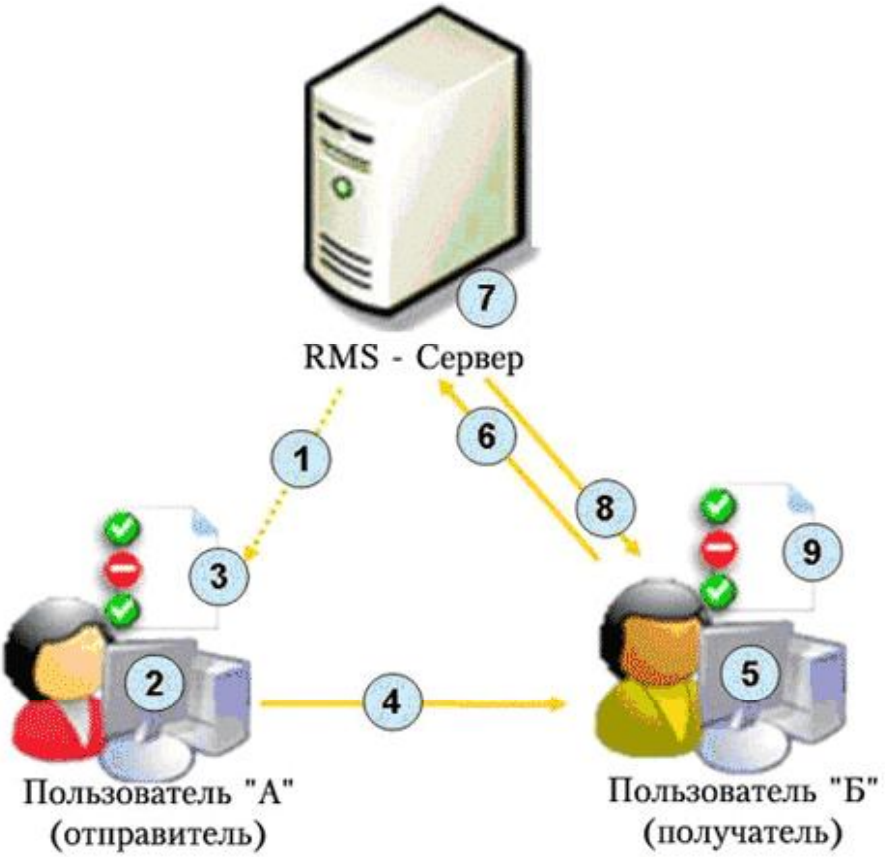

Рисунок 3 – Схема взаимодействия узлов на основе технологии RMS

СПИСОК ЛИТЕРАТУРЫ

1. Громов В.И., Васильев Г.А. Энциклопедия компьютерной безопасности: сб. М., 2007.90 с.
2. Волчинская Е.К. Защита персональных данных: Опыт правового регулирования М.: Галерея, 2010. 236 с.
3. www.localhost.ru