ЗАЩИТА ДОКУМЕНТАЛЬНОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Жук О.Ю.,

Белорусский государственный университет

Проблема защиты информации в современном обществе охватила экономическую, социальную, политическую сферы деятельности людей. Причем сегодня защита данных представляет собой сложный комплекс технических, правовых, организационных мероприятий, проводимых в целях сохранения от несанкционированного доступа информации каждого пользователя.

Вместе с новым тысячелетием появилось такое явление, как информационное противодействие. Это понятие включает в себя «процесс воздействия на компьютерную систему с использованием программно-технических средств и имеющий следствием активизацию некоторого программного средства в данной системе, приводящую к любому негативному отключению от предписанных алгоритмов работы системы» [6].

Множество способов доступа к информации, широкое использование компьютерной техники позволяют злоумышленнику практически в любой момент и в любом месте осуществлять действия, представляющие угрозу информационной безопасности.

Результаты проведенных опросов показывают, что в настоящее время среди основных угроз безопасности 43% составляют вирусы, 26% — отказ в работе важнейших корпоративных систем, 15% — атаки с целью вызвать отказ в обслуживании, 14% — проникновение извне, 11% — проникновение изнутри, 5% — нарушение целостности данных, 3% — финансовое мошенничество, 2% — хищение коммерческой информации [7].

Защита документальной информации в компьютерных системах и сетях на сегодняшний день является одним из приоритетных направлений в деятельности компаний компьютерной индустрии и является важным направлением работы любой организации, которая использует в своей деятельности информационные технологии.

Одним из аспектов проблемы является вопрос о защите электронных документов. Постепенное внедрение систем электронного документооборота в учреждениях и на предприятиях, использование информационных технологий при создании, исполнении и хранении документов поставили перед сферой документооборота и делопроизводства необходимость изучения проблем защиты документальной информации в компьютерных системах и сетях. Специалисты, работающие в данных областях, должны владеть вопросами, связанными с определением, классификацией угроз безопасности, методами и средствами защиты электронных документов.

Безбумажная технология предполагает электронное представление информации. Информационные системы осуществляют автоматическую подготовку и обмен разнообразных электронных документов: приказов, инструкций, отчетов, справочных и других рабочих документов, используемых должностными лицами и пользователями, а также циркулирующих между подразделениями учреждения и внешними организациями по средствам сетевых технологий.

Документы, обрабатываемые в компьютерной системе и имеющие электронное представление, по своей физической природе не имеют реквизитов, присущих бумажным документам. Они в значительной степени уязвимы как перед случайным искажением, так и перед злоумышленной манипуляцией. За неимением механической защиты, фальсификация электронного документа достаточно проста и может вообще не поддаваться обнаружению, причем в роли злоумышленника могут выступать законные отправители документа либо третья сторона. Электронные документы должны иметь юридически значимые реквизиты, позволяющие получателю убедиться в целостности получаемого документа, в подлинности его отправителя, а также обеспечение от подлога со стороны получателя. Как и в бумажных документах, эти реквизиты должны легко вырабатываться законным отправителем, легко проверяться законным получателем и быть сложными для подделки [5].

Одним из аспектов проблемы обеспечения безопасности документальной информации в компьютерных системах и сетях является определение, анализ и классификация возможных угроз безопасности. Перечень угроз, оценка вероятности их реализации, а также модель нарушителя служат основой для формулировки требований к системе защиты.

Угрозой интересам субъектов информационных отношений называют потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты компьютерной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов [13].

Классификация угроз может быть различной. Например, по природе их возникновения можно выделить естественные и искусственные (Гайкович В.Ю.), по отношению к информационным системам угрозы разделяют на внешние и внутренние (Володубцев С.В.), на основе объектов системы, на которые направлены угрозы, выделяют угрозы компьютерам, пользователям, документам (Уолренд Дж.) [3, 2, 10].

Для того чтобы защитить электронные документы, необходимо защитить и свой компьютер. Угрозы компьютерным системам включают:

- физическое вмешательство;
- заражение вредоносными программами;
- несанкционированное внедрение в систему.

Для защиты системы от заражения используются программы обнаружения вирусов (сканеры). Другой метод защиты — предотвращение или ограничение записи некоторыми программами в оперативную память или на диск.

Чтобы защититься от вторжений через сеть, пользователи выбирают пароли, которые трудно угадать, и что весьма желательно, периодически их нужно менять. Более того, пароли по сети следует передавать только в зашифрованном виде.

Для защиты от вторжения могут также использоваться и межсетевые экраны (firewall), компьютеры, которые просеивают трафик, попадающий в компьютерную сеть, и тем самым ограничивают прохождение через нее пакетов. Подобные средства защиты устанавливаются между сетью организации и Интернетом. Целью таких мер является ограничение возможности утечки конфиденциальной информации [10].

Основными угрозами безопасности пользователей являются:

- подмена персоналий;
- нарушение приватности.

Отправителю документа зачастую необходимо подтвердить свою личность. Так, например, при осуществлении электронного платежа получатель должен убедиться, что платеж осуществлен уполномоченной личностью, иначе он не будет признан. Аналогично отправитель должен подтвердить свою личность и права на осуществление платежа таким образом, чтобы в дальнейшем у него не было возможности отказаться от платежа, сославшись на подделку.

Аутентификация необходима и тогда, когда при обмене информацией нужно защитить себя от обмана. Основными средствами защиты в этом случае являются цифровая подпись, шифрование паролей, «электронные водяные знаки», шифрование, использование промежуточных средств [10].

Большой проблемой для пользователей является защита авторских прав. В этом случае используется метод внедрения в электронный документ специальных средств идентификации. Он является электронным эквивалентом водяных знаков на бумажных купюрах. С помощью этого способа можно защититься от случаев плагиата и нарушения прав собственности владения [10].

Говоря о нарушении тайны, мы имеем в виду те случаи, когда подслушивающий открывает способы идентификации пользователя. Для защиты от этого пользователь может воспользоваться средствами шифрования. Однако даже с использованием средств шифрования пользователь не может скрыть источник сообщения. Для решения этой проблемы используются промежуточные узлы, пересылающие сообщения по назначению. Они могут использовать конфиденциальные позывные вместо адреса получателя, так чтобы подслушивающий не мог отследить пару отправитель-получатель сообщения [10].

В целом же вопросы защиты компьютеров и пользователей целесообразно рассматривать в комплексе организационно-технических методов, средств и мероприятий по защите информации, так как именно в этом случае более детально рассматриваются проблемы несанкционированного доступа к информации, идентификация/аутентификация пользователей и ресурсов системы; разграничение доступа к ресурсам; регистрация событий и т.д.

В настоящее время существует три группы угроз электронным документам:

– угрозы, направленные на несанкционированную модификацию, нарушение целостности документа, которые включают в себя изменение служебной или содержательной части документа, подмена документа, изъятие или уничтожение документа;

– угрозы, направленные на искажение аутентичности отправителя документа. К ним относятся: незаконное присвоение идентификатора другого пользователя; формирование и отправление документа от его имени; утверждение о получении информации от некоего третьего лица, хотя она сформирована самим пользователем; повторная передача документа, созданного другим пользователем; искажение уязвимых с точки зрения аутентификации полей документа, включающих адресные данные, идентификаторы отправителя и получателя);

– угрозы, связанные с непризнанием участия. К этой группе угроз относятся: отказ от факта формирования документа; отказ от факта получения документа или заявление ложных сведений о времени его получения; утверждение, что получателю в определенное время была послана информация, которая на самом деле не посылалась или посылалась в другое время [5].

Интернет в настоящее время является удобным средством обмена информацией. В таком случае законный отправитель формирует электронный документ, называемый сообщением, и по каналу связи посылает его законному получателю. В процессе передачи возможно воздействие на сообщение со стороны злоумышленника, поэтому получателю необходимо убедиться в аутентичности сообщения: в процессе передачи сообщение не было искажено, оно поступило именно от того отправителя, который заявлен в документе.

Основными методами защиты от угроз нарушения целостности документа являются: шифрование сообщения; добавление к сообщению контрольной суммы; цифровая подпись сообщения [5].

Шифрование сообщения целесообразно применять в случаях, когда требуется обеспечить конфиденциальность, т.е. скрыть смысловое содержание документа. Оно также обеспечивает защиту документа от несанкционированного доступа при хранении и передаче по каналам связи.

Добавление контрольной суммы к сообщению рассчитывается по определенному алгоритму. Несовпадение суммы при повторном расчете получателем свидетельствует о нарушении целостности документа.

Наиболее универсальным методом обеспечения целостности сообщения является использование цифровой подписи. Она представляет собой контрольную сумму сообщения, зашифрованную с помощью несимметричного алгоритма криптопреобразования. Подпись производится с использованием личного (секретного) ключа пользователя, подписывающего документ; проверить подпись может любой пользователь, имеющий доступ к соответствующему открытому ключу [11].

Для защиты от подмены сообщений и обнаружения их изъятия может использоваться последовательная нумерация и временные метки, учитывающиеся в контрольной сумме сообщения или включенные в цифровую подпись. При этом должны предусматриваться счетчики и механизмы проверки временных интервалов.

Основным методом аутентификации источника данных является шифрование. При использовании симметричного шифрования сообщения получатель уверен в том, что сообщение поступило от заявленного отправителя, так как для этого использовался секретный ключ, известный только отправителю и получателю. Но недостатком этого метода защиты является возможность подделки сообщения самим получателем от имени отправителя, поскольку он тоже знает секретный ключ шифрования.

Более мощное средство — использование несимметричного криптопреобразования, реализуемого посредством цифровой подписи. В этом случае секретный ключ подписи известен только отправителю, и подпись однозначно его аутентифицирует.

Цифровая подпись используется также при такой угрозе, как отказ от факта формирования сообщения. Включение в цифровую подпись временных меток позволит исключить угрозу предоставления ложных сведений о времени отправки или получения сообщения. Отказ от факта получения документа можно предотвратить с помощью механизма квитирования сообщения, но при этом нужно учитывать то, что само квитирование также уязвимо перед всеми угрозами [10].

Таким образом, для всех угроз электронным документам существуют достаточно сильные криптографические методы защиты. Универсальным методом является цифровая подпись сообщения, которая позволяет обеспечить целостность и аутентификацию документа, аутентификацию источника данных.

Рассмотренные выше криптографические механизмы защиты — электронная цифровая подпись (ЭЦП) и шифрование — применяются при разработке защищенных систем электронного документооборота.

Системой подобного рода является, например, система «LanDocs». Использование ЭЦП и шифрования в системе обеспечивается подсистемой безопасности LanDocs, реализующей инфраструктуру открытых ключей (PKI), а форматы сертификатов соответствуют стандарту ITU-T X.509 [12].

В системе ЭЦП используется для подтверждения целостности, авторства документа. При подписании документов формируются две подписи: ЭЦП текста документа и ЭЦП операции, которая заверяет действие, при котором подписывался документ.

Электронная цифровая подпись применяется при операциях создания и редактирования документов, подписании сообщений, поручений по документу, отчетов по заданиям, извещений. Для определения времени подписания документа используется механизм заверки времени подписания документа timestamp. При этом защищается такой реквизит, как дата создания документа.

ЭЦП используется при совершении делопроизводственных операций: подписании, визировании, утверждении. Таким образом, защищаются реквизиты документа: подпись, гриф утверждения, виза. Несколько пользователей могут подписывать один документ, т.е. под одним документом может быть несколько подписей, полученных в результате делопроизводственных операций.

В системе реализовано автоматическое шифрование документов с уровнем доступа «конфиденциальный» посредством открытых ключей. Расшифровать документ может только владелец секретного ключа. Для восстановления доступа к документу в случае утери ключа в системе имеется механизм «мастер-ключа».

Другими примерами могут служить программный комплекс Inter-PRO, предназначенный для защиты прикладных систем, и комплекс приложений Office-PRO, разработанные российской компанией «Сигнал-КОМ» [9].

Последний комплект позволяет легко интегрировать функции криптографической защиты в стандартный интерфейс популярного пакета офисных приложений Microsoft Office: MS Word, MS Excel, MS Access, MS Outlook. Комплект обеспечивает конфиденциальность документов путем шифрования и целостность, достоверность, юридическую значимость — по средствам ЭЦП.

Основные достоинства пакета Office-PRO — его использование не предполагает изменения стандартного порядка работы с электронными документами и не требует специальных навыков работы со сторонними средствами криптографической защиты.

В Российской Федерации реализовано несколько проектов создания защищенных информационных систем. Среди них можно назвать такой, как обеспечение защищенного документооборота в системе «Налоговая отчетность через Интернет». Данная система была совместно разработана компаниями «СКБ-Контур» и «Крипто-Про» и предназначена для формирования и передачи отчетности предприятий в государственные органы через Интернет [8].

В системе используется средство криптографической защиты информации «КриптоПро CSP», которое соединяет реализацию российских криптографических алгоритмов с интерфейсом корпорации Microsoft — Microsoft Cryptography Service Provider (CSP). Данная технология разработки российских криптографических средств с интерфейсом Microsoft позволяет одновременно использовать различные криптографические алгоритмы в одном программном продукте без необходимости встраивания их специальным образом.

Система проходила опытно-промышленную эксплуатацию в Свердловской области в марте 2002 г. Все предприятия области имели возможность передавать отчеты, заверенные электронной цифровой подписью, на сервер системы, установленной в областном Управлении по налогам и сборам. С помощью специального автоматизированного рабочего места «Инспектор», встроенного в локальную сеть управления, проводилась обработка поступающих сведений. С помощью системы, таким образом, отчитался ряд предприятий с суммарной численностью рабочих около 12 тыс. человек.

Еще одним примером создания подобных систем является проект по обеспечению безопасных Интернет-транзакций в финансовой корпорации «НИКойл». Компанией была разработана концепция построения системы безопасности фронт-офисных приложений и четырехкомпонентная модель системы безопасности с использованием средств несимметричной криптографии на базе открытых ключей PKI. В качестве стандарта на средства криптографии было выбрано средство крип-

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ОБРАЗОВАНИЯ, АГРОПРОМЫШЛЕННОСТИ, БИРЖЕВОЙ СИСТЕМЕ. ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ И СОЦИАЛЬНОЙ СФЕРЫ
тографической защиты информации «КриптоПро CSP», разработанное совместно компаниями «Крипто-Про» и ГУП НТЦ «Атлас», и использование криптографического интерфейса Microsoft — Cryptographic Service Provider (CSP) [1].

Разработанная модель системы безопасности позволяла осуществлять такие операции, как создание зашифрованного канала между клиентом и сервером, организация аутентификации с использованием криптографических процедур, постановка, проверка, подписи в документе, проверка принадлежности сертификата подписи клиенту, контроль целостности документа.

Специалистами ООО «Энигма» (г. Минск) была разработана система криптографической защиты информации (СКЗИ) «Энигма КриптКБ», предназначенная для безопасного электронного документооборота между банками и его клиентами [4].

Данная система обеспечивает конфиденциальность и подлинность платежных поручений, выписок, запросов и других документов при их передачи по каналам связи, позволяет осуществлять аутентификацию участников, защиту ключевой информации, контроль целостности архивов, контроль целостности программного обеспечения и ключевой информации.

Быстрое развитие информационных технологий, а также сети Интернет обуславливают необходимость комплексного подхода к обеспечению информационной безопасности, которая должна рассматриваться как составная часть общей безопасности организаций, предприятий, учреждений. Рассмотренные способы защиты документальной информации в компьютерных системах и сетях должны использоваться вместе с другими организационно-техническими методами, средствами и мероприятиями по защите, включающими аппаратные и программные решения. Выбор конкретного набора мер защиты зависит от специфики деятельности организации (структура, численный состав работников, объем конфиденциальной информации, материальная база и др.) и проводимой политики безопасности. Причем деятельность в этом направлении должна вестись совместно со специалистами в сфере документоведения и делопроизводства, которые в современных условиях непосредственно применяют в своей деятельности разработки компьютерной индустрии.

ЛИТЕРАТУРА

1. Ануфриев В.Н. Безопасность Интернет-транзакций в электронном бизнесе // Современные подходы к обеспечению информационной безопасности. Государство в XXI веке. Информационный бюллетень Microsoft. — М., 2002. — № 17.
2. Володубцев С.В. К вопросу обеспечения безопасности социотехнических систем // Вопросы защиты информации: Научно-практический журнал. — ГУП ВИМИ, 2000. — № 4 (55).
3. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий // <http://kis-kiev.narod.ru>.
4. Годунов И.П. Криптографическая защита информации в системе «Банк-клиент» // Управление защитой информации: Научно-практический журнал. — М., Мн., 1998. — Т. 2, № 2.
5. Домарев В.В. Защита информации и безопасность компьютерных систем. — Киев: Издательство «ДиаСофт», 1999.
6. Зайцев И.А. Крючков К.И. Защита информации и компьютерные сети // Вопросы защиты информации. — М.: ВИМИ, 2001. — № 4 (55).
7. Мур. М. Аналитическая поддержка безопасности информационных систем // Международный форум по информации. — М.: ВИНТИ, 2002. — Т. 27, № 2.
8. Налоговая отчетность через Интернет // Современные подходы к обеспечению информационной безопасности. Государство в XXI веке. Информационный бюллетень Microsoft. — М., 2002. — № 17.
9. Трегубов А.В. Сертифицированные СКЗИ компании «Сигнал-КОМ» в современных системах современного документооборота // Вопросы защиты информации. — М.: ВИМИ, 2002. — № 4 (59).
10. Уолрэнд Дж. Телекоммуникационные и компьютерные сети. Вводный курс. — М.: Постмаркет, 2001.
11. Чеглаков С.И. Применение электронной цифровой подписи и шифрования в системах электронного документа оборота // Вопросы защиты информации. — М.: ВИМИ, 2002. — № 4 (59).
12. Чеглаков С.И. Реализация ЭЦП и шифрования в системе авторизации LanDocs // Вопросы защиты информации. — М.: ВИМИ, 2002. — № 4 (59).
13. <http://noff.narod.ru/tools.htm>.