Информационная безопасность

КОЛОТИЛОВ Юрий Васильевич *- доктор технических наук, профессор, академик Международной академии инвестиций и экономики строительства (МАИЭС), главный научный сотрудник Центрального научно-исследовательского и проектно-экспериментального института организации, механизации и технической помощи строительству (ЗАО ЦНИИОМТП)*

КАБУЛОВ Бахрамджан Тахирович *- кандидат технических наук, заведующий отделом прикладного математического обеспечения ОАО "KIVS" АК "Узгеобурнефтегаздобыча"*

ЛИМ Владимир Григорьевич *- кандидат технических наук, ведущий технолог ООО "Газнадзор"*

КЕРИМОВ Фейруз Юркулуевич *- кандидат технических наук, главный инженер ООО "Севертрансэкскавация"*

КУЗНЕЦОВ Петр Александрович *- кандидат технических наук, главный инженер ООО "Салют Текнолоджис Вест"*

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РЕСУРСОВ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ НОРМАТИВНО-ТЕХНИЧЕСКИХ ДОКУМЕНТОВ СТРОИТЕЛЬНОГО ПРОИЗВОДСТВА

Безопасность информационных систем – понятие чрезвычайно широкое. В общем случае можно считать, что это система правовых, организационных и технических мероприятий, нацеленных на предотвращение угроз, т.е. событий или действий, нарушающих нормальное функционирование информационно-вычислительной системы или целостность информации.

Создание и эксплуатация информационных систем должны проводиться в соответствии с требованиями действующих нормативно-технических документов и с существующим законодательством в этой области. Обеспечение информационной безопасности вычислительных систем является приоритетной задачей для любого предприятия, поскольку от сохранения конфиденциальности, целостности и доступности информационных ресурсов во многом зависит качество и оперативность принятия технических решений и эффективность их реализации. Для комплексного решения проблемы информационной безопасности необходимо рациональное сочетание законодательных, организационных и программно-технических мероприятий. Информационная система строительного предприятия может быть надежно защищена только путем внедрения продуманных и четких правил безопасности [1].

Для того чтобы обеспечить надежную защиту ресурсов системы электронного документооборота, в подсистеме информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты, главные из которых: криптографическая защита данных для обеспечения конфиденциальности, целостности и подлинности информации; технологии аутентификации для проверки подлинности пользователей и объектов сети; технологии межсетевых экранов для защиты сети предприятия от внешних угроз при подключении по открытым каналам связи; управление доступом на уровне пользователей и защита от несанкционированного доступа к информации; поддержка инфраструктуры управления открытыми ключами; технологии обнаружения вторжений для активного исследования защищенности информационных ресурсов; централизованное управление средствами информационной безопасности на базе единой политики безопасности предприятия; комплексный подход к обеспечению информационной безопасности, обеспечивающий рациональное сочетание технологий и средств информационной защиты [2, 3].

Современные технологии позволяют не только выявлять проникновение постороннего лица на охраняемую территорию, но и фиксировать перемещение защищаемого объекта (документа) за пределы территории, на которой ему положено находиться по инструкции. Последнее может быть реализовано при использовании встраиваемых в документы **RFID**-меток (**RFID - Radio Frequency Identification Tags**). Микрочипы, исполняющие роль радиочастотных меток, представляют собой миниатюрные устройства, состоящие из антенны, конденсатора и небольшой полупроводниковой микросхемы, выполняющей функции приемника, передатчика и блока памяти для хранения информации. Пассивные **RFID**-метки (в отличие от активных, снабженных автономным электропитанием) активизируются энергией, наведенной радиоизлучением сканера. Переизлучение чипа модулируется зашитой в нем информацией и воспринимается датчиком сканера на расстоянии от нескольких сантиметров до нескольких метров.

Использование **RFID**-технологии позволяет создать комплексную информационно-поисковую систему (ИПС) нормативно-технических документов (НТД), включающую в себя три основных компонента: **RFID**-метку (транспондер – сокращение от **TRANSmitter** / **resPONDER**), сканер (ридер) и компьютерную систему обработки данных. На чипе, незаметно прикрепляемом к документу, достаточно хранить идентификационный номер этого документа. Стационарные сканеры могут быть размещены в шкафах с документами или встроены в стены охраняемых помещений. Считывание информации может происходить с очень большой скоростью (сотни

меток в секунду), что позволяет осуществлять поиск и мониторинг бумажных документов в реальном режиме времени.

Основная цель системы безопасности центров обработки данных и серверов баз данных – контроль доступа. Для этого в системе поддерживается информация безопасности, связанная как с субъектом доступа (пользователи и группы пользователей), так и с объектами (наборы и базы данных, устройства отображения и вывода информации и т.д.). Система защиты информации разрешает или не разрешает доступ, запрашиваемый пользователем или программой, запущенной от его имени. Система безопасности сервера баз данных контролирует доступ к различным ресурсам сервера (базам данных и таблицам, отношениям между ними, встроенным процедурам обработки данных). Система защиты информации должна использовать набор правил для того, чтобы определить, может ли данный субъект получить доступ к данному объекту. Для информационной системы предприятия целесообразно внедрение правил обеспечения безопасности и получения полномочий, с помощью которых можно было бы эффективно реализовать доступ к секретной информации. При этом пользователи, не обладающие соответствующими полномочиями, не должны получать доступ к этой информации. Таким образом, информационная система должна быть защищена с помощью правил безопасности, ограничивающих доступ к объектам (наборы и базы данных, приложения) со стороны субъектов (пользователи системы).

Весьма ответственную роль в корпоративных информационных системах играет электронная почта. Понятие **сертификата открытого ключа и инфраструктуры открытого ключа** являются центральными для шифрования в современном Интернете. При работе с электронной почтой ключевым является понятие **цифровой подписи**. Цифровая подпись является математической операцией над совокупностью битов, которую можно выполнить только с помощью определенного ключа. Его подлинность может быть подтверждена с помощью другого, соответствующего первому, ключа.

Основой большинства механизмов защиты информации является шифрование данных. Под шифрованием информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованную (собственно шифрование) и наоборот (дешифрование). Обобщенная схема криптосистемы шифрования показана на **рис. 1.** Исходный текст передаваемого сообщения (или хранимой информации) **X** с помощью криптографического преобразования **E(X,k1)** зашифровывается с получением в результате шифртекста **Y: Y=E(X,k1)**, где **k1** – параметр функции **E**, называемый ключом шифрования.

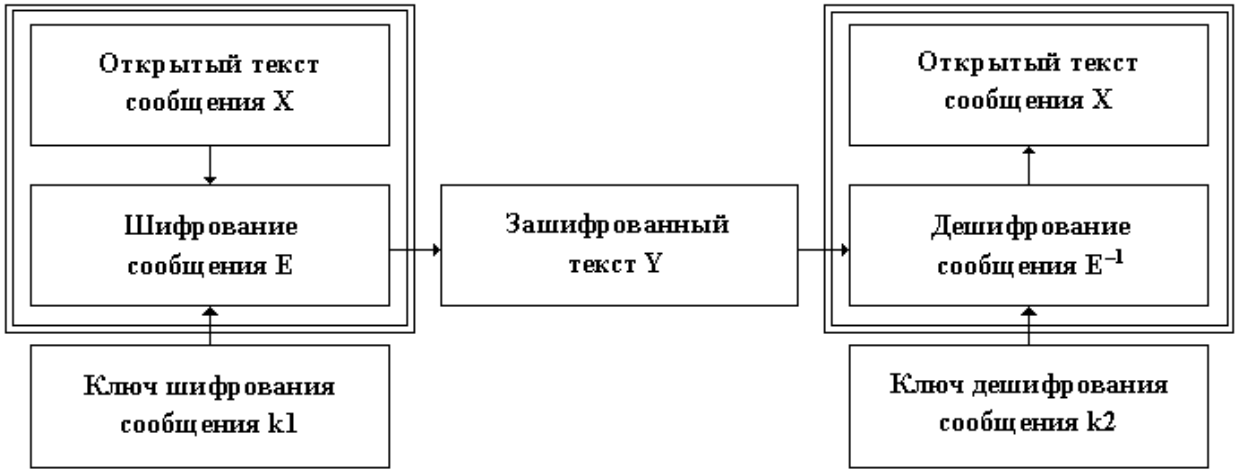

Рис. 1. Обобщенная схема криптосистемы шифрования

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с помощью конкретного ключа информация может быть расшифрована только лицами, владеющими этим ключом. Обратное преобразование информации выглядит следующим образом: $\mathbf{X=E^{-1}(Y,k2)}$. Функция $\mathbf{E^{-1}}$ является обратной к функции **E** и выполняет дешифрование шифртекста. Она также имеет дополнительный параметр в виде ключа **k2**. Ключ дешифрования **k2** должен однозначно соответствовать ключу **k1**, в этом случае полученное в результате дешифрования сообщение **X** будет эквивалентно исходному зашифрованному сообщению **X**. При отсутствии верного ключа **k2** получить исходное сообщение **X** с помощью функции $\mathbf{E^{-1}}$ невозможно.

Преобразование информации может быть симметричным или асимметричным относительно дешифрования. Соответственно существуют два класса криптосистем: симметричные криптосистемы (с единым ключом); асимметричные криптосистемы (с двумя ключами) **[4].**

Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и последующего дешифрования используются различные ключи: **открытый ключ K** используется для шифрования информации, вычисляется из секретного ключа **k**; **секретный ключ k** используется для дешифрования информации, зашифрованной с помощью парного ему открытого ключа **K.**

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца; его необходимо надежно защитить от несанкционированного доступа (аналогично ключу шифрования в симметричных криптосистемах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом: на подготовительном этапе абонент **B** (получатель) генерирует два ключа, секретный ключ $\mathbf{k_в}$ и открытый ключ $\mathbf{K_в}$, затем открытый ключ $\mathbf{K_в}$ посылается абоненту **A** (отправителю) и всем остальным абонентам или делается общедоступным, например, размещается в сети на публичном разделяемом ресурсе; на этапе обмена информацией между абонентами **A** и **B** абонент **A** зашифровывает сообщение с помощью открытого ключа $\mathbf{K_в}$ абонента **B** и отправляет шифртекст абоненту **B**, абонент **B** расшифровывает полученное сообщение при помощи своего секретного ключа $\mathbf{k_в}$. Никто другой (в том числе абонент **A**) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента **B**. Защита информации в асимметричной криптосистеме основана на секретности ключа $\mathbf{k_в}$ получателя сообщения.

В современных операционных системах, например, в **Windows 2000**, появилось новое средство защиты информации – файловая система с шифрованием (**EFS - Encrypted File System**), позволяющая хранить наборы данных на магнитных носителях информации в зашифрованном виде. Благодаря этому пользователи вычислительных систем получили простое и надежное средство предотвращения возможной утечки информации при возникновении несанкционированного доступа к информации и даже при краже жесткого диска из сервера.

Шифрование и расшифровка данных поддерживаются на уровне отдельного набора данных или директории. Все наборы данных и вложенные директории будут в этом случае автоматически шифроваться средствами операционной системы.

Файл в этом случае не нужно расшифровывать после обращения к нему – шифрование и расшифровка происходят автоматически перед записью информации на диск и после чтения с диска при помощи встроенных средств операционной системы. Файловая система с шифрованием автоматически следит за использованием шифрованных файлов и находит соответствующий ключ пользователя в специально организованном хранилище. Поскольку механизм использования ключей основан на интерфейсе **Crypto API**, ключи могут храниться по технологии **Smart card [1].**

EFS основан на шифровании с помощью открытых ключей на базе интерфейса **Crypto API.** Предполагается, что у каждого пользователя есть свой открытый ключ, известный всем, в том числе и операционной системе, и секретный ключ. Операционная система получает доступ к секретному ключу только на время работы данного пользователя в системе (например, используя технологию **Smart card**). Отметим, что зашифровать информацию посредством открытого ключа может кто угодно, однако расшифровать его после этого сможет только тот пользователь, которому известен соответствующий секретный ключ.

Каждый набор данных шифруется с помощью случайного ключа, генерируемого системой. При этом ключ шифрования не связан ни с открытым, ни с секретным ключом пользователя. Это уменьшает возможности атак, основанных на криптоанализе. В первой версии **EFS** шифрование основано на алгоритме **DES**. Алгоритм **DES** широко используется во многих криптографических системах. Это блочный алгоритм шифрования с симметричным ключом. Ключ состоит из 64 битов, но лишь 56 из них применяются непосредственно при шифровании. Оставшиеся 8 предназначены для контроля четности: они устанавливаются так, чтобы каждый из 8 байтов ключа имел нечетное значение. Шифруемая информация обрабатывается блоками по 64 бита, причем каждый блок модифицируется с помощью ключа в итерационной процедуре. При шифровании сообщения, состоящего из нескольких блоков, могут применяться несколько режимов работы **DES**. Они позволяют усилить защиту информации и различаются способом обработки исходных фрагментов. В простейшем случае (режим **Electronic Code Book**, **ECB**) 64-битные фрагменты шифруются ключом независимо друг от друга. При длине ключа в 56 битов алгоритм считается устойчивым к взлому с применением различных методов криптографического анализа. В последующем будет разрешено использование и других симметричных алгоритмов шифрования.

Ключ шифрования, знание которого необходимо для расшифровки данных, далее шифруется посредством открытого ключа пользователя. Результат такого шифрования называется полем расшифровки файла (**DDF - Data Decryption Fields**). Полученное поле записывается как атрибут вместе с самим зашифрованным файлом.

Кроме поля расшифровки, система создает поле восстановления набора данных (**DRF - Data Recovery Field**), содержащее ключ шифрования файла, зашифрованный посредством открытого ключа так называемого агента восстановления. Агент восстановления предназначен для обеспечения возможности дешифрования данных в случае утраты личного ключа пользователем. В свою очередь, агент восстановления также имеет свои собственные открытый и секретный ключи.

Достаточно высокую степень криптостойкости имеют только системы шифрования, использующие секретные ключи достаточно большого объема, сравнимого с объемом хранимых или передаваемых текстов. Системы же, в которых объем секретных ключей сравнительно невелик, вообще говоря, не обеспечивают полной защиты хранимой информации от несанкционированного доступа. Задача повышения стойкости криптосистем как с секретным, так и с открытым ключом, может быть решена путем уменьшения избыточности или рандомизации хранимой и передаваемой информации [5]. Безопасные методы управления ключами очень важны, так как многие атаки на криптосистемы имеют объектом атаки процедуры управления ключами.

В правительственных и военных системах связи используют лишь симметричные алгоритмы, так как нет строгого математического обоснования стойкости систем с открытыми ключами, как, впрочем, не доказано и обратное. Задача вычисления секретного ключа по известному открытому ключу практически неразрешима. Однако если злоумышленнику удастся построить такой алгоритм или найти способ дешифрования, не требующий решения сложной обратной задачи, то дискредитирована будет вся система и все сообщения, зашифрованные с помощью этой системы. В этом отношении симметричные криптографические системы обладают более высокой криптостойкостью, но при их использовании возникает указанная выше сложная проблема распространения секретных ключей.

Новый подход к решению проблемы, связанной с распределением ключей - разработка криптографической системы, которая не базируется на алгоритмической трудности решения за приемлемое время некоторой сложной математической задачи и, вместе с тем, позволяет передавать ключ по незащищенному каналу связи [6]. В существующих симметричных криптосистемах открытый текст с использованием секретного ключа преобразуется в криптограмму, которая затем передается получателю. В предлагаемой криптосистеме получателю вместо криптограммы передается ключ (по незащищенному каналу связи), который используется для преобразования некоторого общедоступного ресурсного текста в открытый текст. Структурная схема предлагаемой криптосистемы представлена на рис. 2.

Рис. 2. Структурная схема системы шифрования с использованием ресурсных текстов

Процесс шифрования и расшифрования в данном случае можно представить следующим образом: $\mathbf{K = E(X,ST),\ X = E^{-1}[E(X,ST),ST]}$, где **ST** – ресурсный текст. Криптографические алгоритмы, использующие одноразовые ключи, длина которых не меньше длины шифруемого сообщения, являются абсолютно надежными. Генерация и распределение таких длинных ключей представляет определенные трудности, что ограничивает использование подобных методов только исключительными случаями.

Предлагаемая криптографическая система предназначена, в основном, для защиты особо важной информации в базах данных, когда не ставятся жесткие ограничения на время шифрования и расшифрования. Вместе с тем, не следует забывать, что новые алгоритмы не рекомендуется применять без их всесторонней проверки профессионалами-криптоаналитиками.

Литература

1. Щербаков А.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических алгоритмов. – М.: Русская редакция, 2003. – 416 с.

2. Колотилов Ю.В., Кузнецов П.А., Лим В.Г. и др. Использование методов оценки информационного риска для выбора средств защиты информации в среде САПР на предприятиях строительного комплекса. - Вопросы защиты информации. – 2003. - № 3(62). - С.50-53.

3. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.

4. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.

5. Шеннон К. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. - С. 333-369.

6. Колотилов Ю.В., Кабулов Б.Т., Лим В.Г. и др. Криптографическая защита информации с использованием ресурсных текстов в информационно-поисковых системах. - Вопросы защиты информации. - 2003. - № 4(63). - С.22-28.