КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННО-ПЛАТЕЖНЫХ СИСТЕМАХ

Иванова А.А.

ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И. Носова», г. Магнитогорск, Россия

Электронные платежные системы – это технология, позволяющая производить расчеты напрямую между контрагентами с помощью электронной связи. Сегодня популярность электронных платежей растет с каждым днем.

В системах электронных платежей используются электронно-цифровые подписи и специальные методы шифрования при передаче платежных документов.

Их реализация может быть осуществлена как аппаратными, так и программными средствами.

Основными методами криптографического преобразования считаются методы перестановки и замены. Суть первого метода заключается в разбиении исходного текста на блоки, а затем в записи этих блоков и чтении шифрованного текста по разным путям геометрической фигуры. Шифрование методом замены заключается в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым ключом преобразования.

Известными стандартами в области криптографии являются комбинированный метод для шифрования данных – DES (США) и ГОСТ 28147-89, для работы с электронной цифровой подписью – RSA (США) и ГОСТ 334.10-94. В течение трех десятков лет стандарт DES считался в международной практике одним из лучших образцов криптоалгоритмов (в его основе используются комбинации перестановок, замен и операций сложения по модулю два), используемых при хранении и передаче данных в 10 вычислительных системах, в электронных системах платежей, при обмене коммерческой информацией и т.п. В последнее время стандарт DES (находит применение усиленный вариант стандарта – TripleDES – трижды шифрует информацию с помощью стандарта DES) теряет свои позиции из-за увеличения потенциальной возможности его взлома методом прямого подбора высокопроизводительными компьютерами (длина ключа у стандарта DES-64 символа, аналогичный российский стандарт значительно более стойкий – имеет ключ длиной 256 символов).

Ему на смену приходит стандарт шифрования AES, поддерживающий длину ключа до 256 символов. Сертификацией средств защиты информации занимаются ФАПСИ и Гостехкомиссия (зарубежные средства защиты информации ими не сертифицируются). На международном уровне используется стандарт ISO 15408, описывающий набор общих критериев защищенности информационной системы, из которых набираются технические условия для каждого класса средств защиты.

В системе Банка России предписано использовать криптографические средства, реализующие отечественные стандарты безопасности: ГОСТ 28147-89 на алгоритм шифрования и ГОСТ 334.11-94 на цифровую подпись.

Другим обязательным требованием по использованию криптографических средств является их сертифицированность в государственной организации, что гарантирует стойкость применяемой криптосистемы и определяет условия ее безопасной эксплуатации. Преимущественно используются аппаратно реализованные устройства криптографической защиты информации серии «Криптон» фирмы «Анкада», реализующие отечественный стандарт шифрования ГОСТ 28147-89 и имеющие сертификаты ФАПСИ.

По сравнению с чисто программными реализациями применение платы «Криптон» исключает возможность появления ключей шифрования в открытом виде в оперативной памяти компьютера. Устройства «Криптон» позволяют шифровать файлы, группы файлов и разделы на винчестерах и носителях 11 информации; защищать информацию, передаваемую по открытым каналам связи и вычислительным сетям; разграничивать и контролировать доступ к компьютеру; формировать цифровую подпись документов. Ключи шифрования могут находиться на дискетах, смарт-картах, устройствах Touch Memory, USB-брелках. Скорость шифрования достигает скорости передачи данных в сети Fast Ethernet (до 10 Мбит/с).

Среди программных продуктов, используемых для поддержки шифрования документов и электронной подписи, широко используются программы «Вебра-W» и «Вебра-OW», имеющие сертификат ФАПСИ. Следует отметить, что современные многофункциональные программные средства, такие как СУБД, ОС и др., имеют встроенные процедуры криптографической защиты информации. Существуют специализированные доступные программы, например, Best Sentry 2020, Cryptext и др., позволяющие шифровать (расшифровать) данные на основе ряда алгоритмов (стандартов) на винчестерах и различных типах носителей информации.

Достоинство программных средств шифрования:

- высокая стойкость к дешифрованию.

Недостатки программных средств шифрования:

- затраты ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т.п.);
- возможность взлома высокопроизводительными системами методом прямого подбора ключа.

Достоинства аппаратных средств шифрования:

- усиление защищенности самих криптографических средств (криптографические функции гарантированно защищены от несанкционированного доступа к ним, что препятствует возможности манипуляции ключами со стороны злоумышленника);
- повышение производительности системы за счет выполнения трудоемких криптографических операций на специализированном оборудовании.

Недостаток аппаратных средств шифрования:

- высокая стоимость оборудования и его обслуживания.

Список использованных источников

1. *Баричев С. Введение в криптографию. Электронный сборник. – М.: Вече 1998. –244 с.*
2. *Безбогов А.А., Яковлев А.В., Шамкин В.Н. «Методы и средства защиты компьютерной информации»: Учебное пособие. Тамбов: Издательство ТГТУ, 2006. – 196 с.*
3. *Ведеев Д. Защита данных в компьютерных сетях. Открытые системы. – М.: Дрофа, 1995. – № 3. – 180 с.*
4. *Златопольский Д. М. Простейшие методы шифрования текста / Д.М. Златопольский. М.: Чистые пруды, 2007.*
5. *Молдовян А. Криптография / А. Молдовян, Н.А. Молдовян, Б.Я. Советов – СПб.: Лань, 2001.*
6. *Моделирование процесса формирования экономической грамотности студентов в структуре дополнительного образования вуза / Сторожева Е.В., Валеев А.С., Кружилина Т.В., Сергеев А.Н. Сибирский педагогический журнал. – 2011. – № 12. – С. 176–182.*
7. *Петров А.А Компьютерная безопасность. Криптографические методы защиты. ДМК Москва, 2000 г.*
8. *Совершенствование качества внешнеэкономических связей предприятий в условиях интегрированного хозяйствования (на примере России и Казахстана) Елена Владимировна Сторожева монография / Е.В. Сторожева; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, ГОУ ВПО «Магнитогорский гос. ун-т». Магнитогорск, 2010.*