УДК 336.717.1

# ВЫБОР ОПТИМАЛЬНОГО АЛГОРИТМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

***С.О. Кириленко**, 5 курс*
*Научный руководитель – **О.Д. Вовчак**, д.э.н., проф.,*
*Институт магистерского и последипломного образования УБД НБУ*

Использование современных информационных технологий стало таким, что на уровне с проблемами надежности и стойкости их функционирования, возникла проблема обеспечения безопасности циркулирующей в ней информации. При таких условиях создались возможности утечки информации, нарушения ее целостности и блокирования. Поэтому сегодня важным элементом предупреждения компьютерных преступлений в банковской деятельности становится использование современных технических средств защиты информации. Среди всего спектра защиты данных от нежелательного доступа особое место занимают криптографические средства защиты, которые основываются лишь на свойствах самой информации.

Значительный вклад в исследование проблем криптографической защиты банковской информации сделаны Аниною Б.Ю., Голубевою В.А., Гуцалюком М.В., Терениною А.К. и др., однако проблема надежности и криптостойкости алгоритмов нуждается в последующем изучении.

Цель работы – выбор наиболее оптимальных, криптостойких и надежных криптографических средств защиты банковской информации и определение перспектив развития современной криптографии.

Система информационной безопасности Украины опирается на достаточно развитую нормативно правовую базу: Закон Украины «О защите информации в автоматизированных системах», Закон Украины «Об электронной цифровой подписи» и др.

По закону Украины «О защите информации в автоматизированных системах» криптографическая защита информации (КЗИ) – вид защиты информации, которая реализуется путем превращения информации с использованием специальных (ключевых) данных с целью скрывания/восстановления содержания информации, подтверждения ее подлинности, целостности, авторства и тому подобное [1]. Средства криптографической защиты информации – аппаратный, программный, аппаратно-программный или другие средства, предназначенные для криптографической защиты информации.

Криптография включает два основных направления: симметричная и асимметричная шифровка.

Современные исследования симметричных алгоритмов шифровки сосредоточены, в основном, вокруг блочных и поточных алгоритмов шифровки и их использования. Шифры Data Encryption Standard (DES) и Advanced Encryption Standard (AES) являются стандартами блочных шифров, утвержденных правительством США (однако, стандартизация DES была отменена после принятия стандарта AES).

Примерами криптосистем с открытым ключом является Elgamal (названная в честь автора, Тахира Ельгамаля), RSA (названная в честь изобретателей: Рона Ривеста, Аде Шамира и Леонарда Адлмана), Diffie-Hellman и DSA, Digital Signature Algorithm (изобретен Девидом Кравицом) [3].

Алгоритм RSA (за первыми буквами его творцов: Rivest-Shamir-Adleman) основан на свойствах простых чисел (причем очень больших). Асимметричный алгоритм RSA можно использовать для создания электронной цифровой подписи [4, с. 73].

Сравнительный анализ основных алгоритмов КЗИ приведен в таблице 1.

Таблица – Основные характеристики криптографических алгоритмов шифровки

| Характеристика | Вид криптографического алгоритма шифровки | |
|---|---|---|
| | DES (Data Encryption Standard) | RSA (Rivest-Shamir-Adleman) |
| Тип ключа | Симметричный | Асимметричный |
| Вид алгоритма | Одинключевой (открытый) | Двоключевой (открытый и секретный) |
| Функция, которая используется | Перестановка и подстановка | Поднесение к степени |
| Длина ключа | 56 бит | 1024 бит, а для особенно важных задач – 2048 бит (например, для главного Мастера Сертификатов) |
| Наименее затратный криптоанализ | Перебор по всему ключевому пространству | Разложение модуля |
| Стойкость | Теоретическая | Практическая |
| Часовые расходы на раскрытие | Столетия | Зависят от длины ключа |
| Время генерации ключей | Миллисекунды | Десятки секунд |

В современной науке достаточно перспективным является развитие квантовой криптографии и криптоанализа на основе квантовых компьютеров.

Последние разработки в области квантовой криптографии позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключа и ключевой информации. Используются все лучшие достижения по защите информации, как из классической криптографии, так и из новейшей "квантовой" области, что позволяет получать результаты, превосходящие все известные криптографические системы [2].

Можно сделать вывод, что алгоритм RSA работает приблизительно в тысячу раз медленнее алгоритма DES и нуждается в десять раз в более длинных ключах, его стойкость теоретически не доказана, однако большое преимущество RSA заключается в отсутствии необходимости организации строго засекреченной процедуры обмена ключами. Таким образом, для банковских учреждений является целесообразнее приложение алгоритма RSA.

Но наука не стоит на месте и можно с уверенностью говорить, что в ближайшем будущем вся криптографическая защита информации и распределение ключей будут базироваться на квантово-криптографических системах.

**Список использованных источников**

1. Закон Украины «О защите информации в автоматизированных системах» от 5 июля 1994 года за № 80/94 // [Электронный ресурс] / сайт "Lawua.info". – Режим доступа: http://lawua.info/jurdata/dir250/dk250019.htm/

2. Красавин В. Квантовая криптография // [Электронный ресурс] / сайт "security.strongdisk.ru". – Режим доступа: http://security.strongdisk.ru/i/42&all=1/

3. Криптография. Алгоритм RSA // [Электронный ресурс] / сайт "Kiev-security.org.ua". – Режим доступа: http://Kiev-security.org.ua/box/1/all.shtml/

4. Кушнеров А. Применение электронной цифровой подписи // Корпоративные системы. – 2007. – № 5. - с. 77-80.