конкретных предметных областях; создание методов Data Mining, способных не только извлекать из данных закономерности, но и формировать некие теории, опирающиеся на эмпирические данные; преодоление существенного отставания возможностей инструментальных средств Data Mining от теоретических достижений в этой области [1]. Применение технологии Data Mining требует больших вычислительных мощностей, поэтому дальнейшее развитие этой технологии связано с облачными вычислениями, которые предлагают масштабируемую инфраструктуру и программные средства без прямой привязки к физическим машинам, при этом экономя трудозатраты, серверные мощности и энергопотребление в моменты простоя.

Литература

1 Сайт Национального открытого университета «Интутит» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru. – Дата доступа: 10.04.2012.

2 Сайт информационных технологий [Электронный ресурс]. – Режим доступа: http://inftech.info. – Дата доступа: 10.04.2012.

Емельяненко И.И., Рябцева А.А.

БГЭУ, ФМЭО, ДАИ-2, 2 курс

КРИПТОГРАФИЧЕСКИЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации остается для банков самой критичной проблемой — утечка данных приводит к прямым материальным потерям и к ухудшению репутации. В связи с этим банковский сектор считается главным потребителем систем информационной безопасности, бюджет, выделяемый на них в кредитных организациях, значительно превышает ИБ-бюджеты компаний нефинансового сектора. Поэтому анализ криптографических способов защиты информации и оценка их эффективность являются необходимыми для современной экономики и общества. [1]

На раскрытие современных криптографически зашифрованных документов может понадобиться много лет непрерывной работы. Существует

следующая классификация криптографических алгоритмов:

1. *Алгоритмы шифрования с секретным ключом (симметричные)* – способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Подвидами данного способа шифрования являются *блочные шифры* (DES, New DES, AES, IDEA, Blowfish, Triple-DES, Twofish, RC2, CAST) и *поточные шифры* (RC4, ARC4, DESS, IBAA, JEROBOAM, ISAAK, Rabbit).

Симметричный блочный. IDEA. Высокая криптостойкость, которая обеспечивается:

- запутыванием — шифрование зависит от ключа сложным образом;

- рассеянием — каждый бит незашифрованного текста влияет на каждый бит зашифрованного текста.

Симметричный поточный. Rabbit. Высокая скорость шифрования; если же атака происходит на несколько ключей, то защищенность снижается до 96 бит.

2. Алгоритмы шифрования с открытым ключом (асимметричные) — система шифрования и электронной цифровой подписи, при которой открытый ключ передаётся по открытому (доступному для наблюдения) каналу, и используется для проверки электронной цифровой подписи и для шифрования сообщения (DSA, RSA, Эльгамаль, ECDH) [2]. DSA. Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма.

3. Хэш-функции – преобразует сообщение произвольной длины в число фиксированной длины (MD-2, MD-5, SHA-1). SHA-1. Факты успешных криптоатак неизвестны. Основная документация по разработке закрыта. [3]

Существует также криптографическая программа PGP – это гибридная криптосистема. PGP объединяет в себе лучшие стороны симметричной криптографии и криптографии с открытым ключом. [4]

Таким образом, сравнительный анализ поточных и блочных методов шифрования показывает, что более просто устроенные поточные методы уступают в производительности блочным методам шифрования. Алгоритм

симметричного шифрования можно считать достаточно проработанным и эффективным, с минимальным количеством недостатков. Какими бы недостатками и преимуществами ни обладало ассиметричное и симметричное шифрование, необходимо отметить лишь то, что наиболее совершенные решения – это те, которые удачно сочетают в себе алгоритмы обоих видов шифрования (PGP).

Литература

1. Информационные технологии в экономике [Электронный ресурс]. - Режим доступа: http://www.iteconomic.com/. – Дата доступа: 21.02.2012.

2. Новая парадигма информационной безопасности / По материалам компании Aladdin Software Security R.D. // «Банковские технологии». – 2008г. - №8. – С.102

3. Overview//Symantec Corporation [Electronic resource]. - Mode of access: http://www.symantec.com. — Date of access: 17.02.2012.

4. Криптография и шифрование // Криптография [Электронный ресурс]. - Режим доступа: http://cryptolog.ru/. - Дата доступа: 16.02.2012.

Захарова А.О.

БГЭУ, ФФБД, группа ДФК-2, 2 курс

ОЦЕНКА УРОВНЯ РАЗВИТИЯ УСЛУГ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Согласно Стратегии развития банковского сектора экономики Республики Беларусь на 2011-2015 годы, применение информационных технологий в данной сфере деятельности становится одним из главных направлений развития банков, определяющих качество и надежность предоставляемых ими услуг. Поэтому проблемы, возникающие при внедрении дистанционных банковских сервисов, имеют столь большую актуальность для банков Беларуси (РБ).

На сегодняшний день банки предлагают достаточно широкий спектр услуг,