АҢДАТПА

Диссертациялық жұмыс қазіргі алгоритмның крифтографиялық қажырлылығының байқауына арнаулы, ақпараттық жүйенің пайдаланушысының айтылмыш есептік жазбасының шифрлауы үшін. Айтылмыш жұмыстың мақсаты MD5 хеш-функция алгоритмының крифтографиялық қажырлылығының зерттеуі болып табылады. Байқау мүмкіндік игерушілік модифицирілінген алгоритм шифрлау сенімділіктің көтермелеуі үшін ақпараттық жүйе. Құрулы мақсаттың табысы үшін жұмыста криптоаналитикалық үдерістің математикалық модельдеуінің әдістері пайдаланылды, шифрлаудың және мезгілдіктің кідірісінің ұйғарымінің үдерісінің компьютерлік модельдеуінің әдісінің математикалық модельдеуінің әдістері, шифрлаудың алгоритмының крифтографиялық қажырлылығының қағидасы.

АННОТАЦИЯ

Диссертационная работа посвящена изучению криптографической стойкости современных алгоритмов, применяемых для шифрования данных учетных записей пользователей информационных систем.
Целью данной работы является исследование криптографической стойкости алгоритмов основанных на безе хеш-функции MD5. Изучение возможности использования модифицированных алгоритмов шифрования для повышения надежности информационных систем. Для достижения поставленных целей в работе использовались методы математического моделирования криптоаналитических процессов, метода компьютерного моделирования процессов шифрования и определения временной задержки, теория криптографической стойкости алгоритмов шифрования.

ABSTRACT

Dissertation work is devoted to studying of cryptographic firmness of the modern algorithms applied to enciphering of these accounts of users of information systems.
The purpose of this work is research of cryptographic firmness of algorithms based on meringue MD5 hash function. Studying of possibility of use of the modified

algorithms of enciphering for increase of reliability of information systems. For achievement of goals in work methods of mathematical modeling of cryptoanalytical processes, a method of computer modeling of processes of enciphering and definition of a temporary delay, the theory of cryptographic firmness of algorithms of enciphering were used.

Введение

В настоящее время основным способом защиты информации от несанкционированного доступа (НСД) является внедрение так называемых средств А А А (Authentication, Authorization, Accounting — аутентификация, авторизация, управление правами пользователей). При использовании этой технологии пользователь получает доступ к компьютеру лишь после того, как успешно прошел процедуры идентификации и аутентификации. Стоит учесть , что на мировом рынке ИТ-услуг сегмент А А А постоянно растет. Эта тенденция подчеркивается в аналитических обзорах IDC, Gartner и других консалтинговых фирм. Такой же вывод можно сделать , внимательно просмотрев ежегодный обзор компьютерной преступности на рисунке 1, Института компьютерной безопасности США и ФБР за 2005 год. Суммарный объем потерь за 2005 год — 130 104 542 долл. Количество предприятий-респондентов (США) — 700

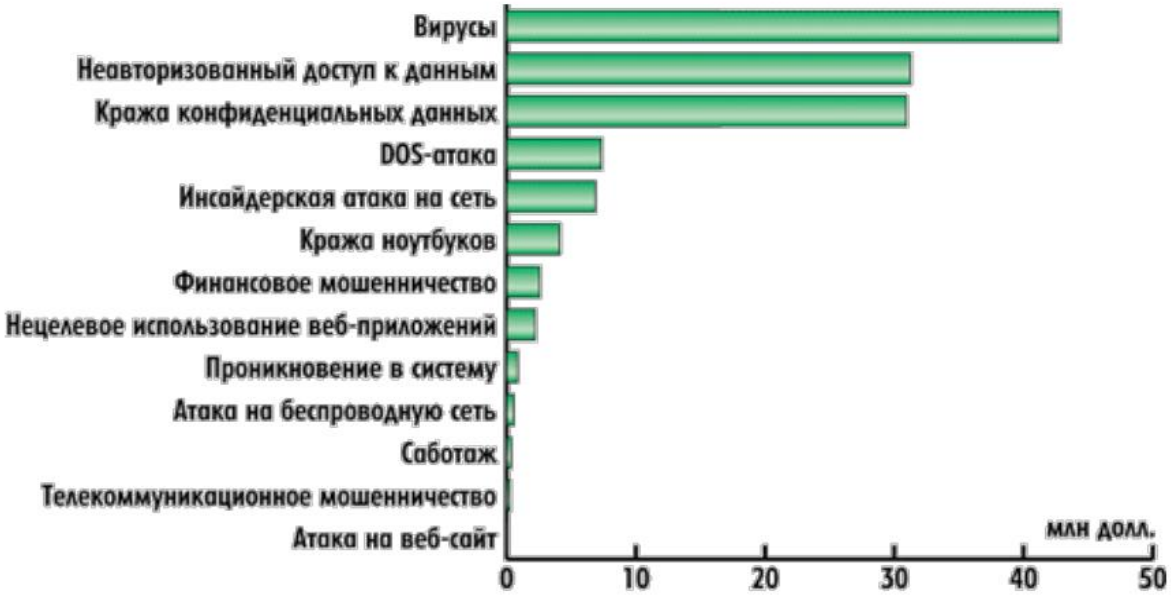

Рисунок 1 - Данные по объему потерь от разных видов атак за 2005 год, долл.

Как видно из диаграммы, ущерб от краж и конфиденциальной информации значительно увеличился. То есть каждая из опрошенных компаний потеряла