НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ "ЗАХИСТ ІНФОРМАЦІЇ" №3, 2002

УДК 681.3.004

Фомичев В.В., Кузнецов Г.В., Гусенко М.В.

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ С ЭЛЕМЕНТОМ ВЕРОЯТНОСНОГО ИЗМЕНЕНИЯ АЛГОРИТМА ШИФРОВАНИЯ

На данный момент развития информационной инфраструктуры современной цивилизации остро стоит вопрос об обеспечении защиты информационных ресурсов.

Для обеспечения защиты данных используют две группы технологических решений – аппаратные и программные. Аппаратные средства являются достаточно эффективным барьером между защищаемым объектом и потенциальным «взломщиком». Однако такое решение задачи чревато двумя основными проблемами: первая – низкая гибкость информационной инфраструктуры базирующейся на аппаратной защите; вторая – отсутствие возможности «быстрой» модернизации системы защиты к новым условиям технологического баланса «атака/защита». Поэтому программные средства защиты информации, вообще и базирующиеся на криптографических алгоритмах, в частности, являются хорошей альтернативой для аппаратной защиты, поскольку лишены выше приведенных недостатков.

Системы криптографической защиты, особенно в условиях стран с низким уровнем развития микропроцессорных технологий, становятся практически единственным способом обеспечения конфиденциальности информации в ресурсах компьютерных сетей с открытой архитектурой.

Ресурсы, которые приходиться защищать, можно разделить на две категории, по признаку состояния информационных потоков – активные и пассивные. Система криптографической защиты, рассматриваемая в этой статье, предназначена для защиты активных ресурсов компьютерных сетей.

В основе любой системы криптографической защиты лежит алгоритм криптографии. Устойчивость к взлому такой системы определяется устойчивостью применяемого в ней алгоритма. Наиболее распространенными считаются системы, работающие на основе открытого алгоритма. В таких системах уровень устойчивости определяется характеристиками алгоритма и используемого пароля.

Поскольку, все характеристики открытого алгоритма уже известны потенциальному «взломщику», то, можно сказать, что все атаки на подобные системы защиты информации сводятся к выявлению используемого пароля, поскольку это единственное варьируемое звено криптографической системы.

Авторы предлагают к рассмотрению систему криптографической защиты информации, основанную на возможности динамической замены открытого криптографического алгоритма, используемого в системе, в зависимости от текущего состояния информационного потока обслуживаемого системой.

Важным понятием в работе рассматриваемой системы криптографической защиты является - ***состояние системы***. Состояние системы определяется двумя параметрами: текущей записью состояния и активным алгоритмом.

Запись состояния формируется для каждого отдельного сеанса. Под сеансом понимают установку соглашений на передачу информации между двумя серверами, работающими под управлением рассматриваемой криптографической системы.

На рисунке 1 приведена общая функциональная схема такой криптографической системы.

Система состоит из следующих основных элементов:

1. ***Модуль входного потока*** – обеспечивает прием и структуризацию получаемых данных, в соответствии моделью OSI – транспортный уровень;

2. ***Блок принятия решений*** – система управления изменением состояния системы и обеспечения функциональных связей между ее компонентами;

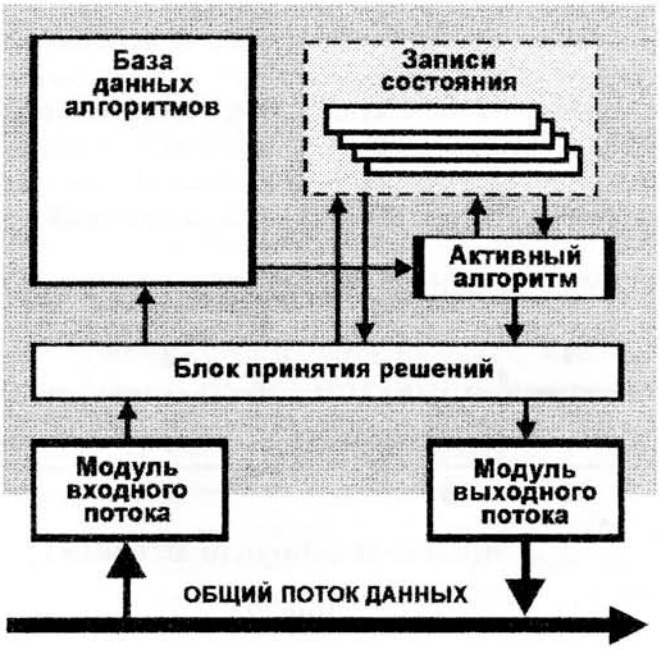

Рис. 1

3. ***Активный алгоритм*** – оверлейный модуль, в который система помещает код криптографического алгоритма перед началом его активного использования;

4. ***База данных алгоритмов*** – набор алгоритмов поставляемых с системой и формируемый уникальным образом для каждого дистрибутива системы;

5. ***Записи состояния системы*** – область данных используемых для хранения конечных состояний системы по различным сеансам;

6. ***Модуль выходного потока*** – выполняет сборку преобразованных данных для передачи их во внешний поток данных.

Первоначальная инициализация системы состоит из двух этапов: первый – создание базы данных алгоритмов поставляемых с системой; второй – создание начальной парной записи состояния для конкретного сеанса.

База данных алгоритмов формируется поставщиком системы, может содержать от одного до трех десятков криптографических алгоритмов или их версий, которые в ходе работы могут быть использованы для определения состояния системы. То есть, любой из алгоритмов фигурирующих в базе данных по команде ***Блока принятия решений*** может быть перемещен в блок ***Активного алгоритма***.

На втором этапе пользователем системы выполняется генерация начальной записи состояния системы для конкретного сеанса. Для этого пользователь локально запускает две копии системы с разных дистрибутивов и вводит любую случайную последовательность данных для их пересылки между активными копиями системы. В ходе обработки введенной информации каждый из дистрибутивов создает не парный начальный ключ, который сохраняется в записи состояния для данного сеанса.

Система разрабатывается для установки на крупные информационные узлы, используемые организациями в качестве шлюзов между внутренней информационной сетью и внешними открытыми каналами передачи данных. Естественно, внешние каналы могут быть использованы для работы с множеством удаленных серверов обслуживаемых нашей

криптографической системой. Число серверов, с которыми может работать конкретная копия системы, равна числу записей состояния сеансов хранящихся в этой системе.

Запись состояния сеанса хранит в своей структуре текущий пароль сеанса переменной длины, признак последнего, используемого в качестве активного, алгоритма из базы данных системы, а так же логическую цепочку, по которой в продолжение сеанса будут извлекаться данные из потока для модификации текущей записи состояния системы.

По ходу работы системы вносить изменения в запись состояния сеанса может ***Активный алгоритм*** и/или ***Блок принятия решений***. Логическая управляющая цепочка, на основании вида которой действует ***Блок принятия решений***, позволяет, как показано на

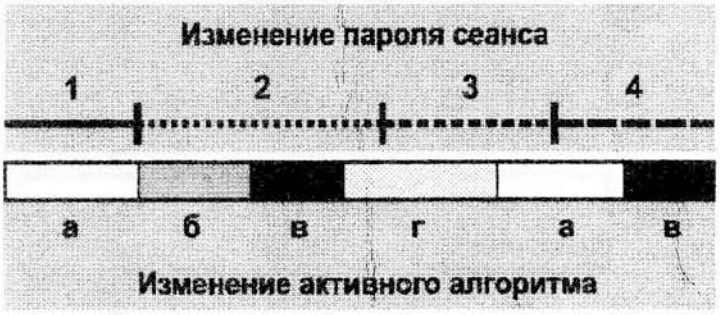

Рис. 2

рисунке 2, динамически осуществлять замену активного алгоритма шифрования, не зависимо от текущего пароля системы.

Таким образом, получается не тривиальная зависимость между активными алгоритмами шифрования и используемыми паролями, которую сложно описать простой нелинейной математической функцией. Это автоматически приводит потенциального «взломщика» к выбору атаки перебором для осуществления взлома системы, но такая атака не актуальна и не может нанести серьезный вред в целом информационному потоку обслуживаемому такой системой. Больше того, благодаря постоянному контролю над состоянием системы становиться возможным, без дополнительных программных средств, обеспечивать контроль целостности передаваемых данных и их достоверность.

Такую систему можно рассматривать как мощный транспортный конвейер, рассчитанный на организацию передачи больших объемов разнородной конфиденциальной информации в условиях централизованно неконтролируемых распределенных информационных систем работающих на базе открытых компьютерных сетей.

Основной недостаток системы, выявленный авторами, это более высокие требования к производительности аппаратного комплекса вычислительных машин по сравнению с классическими криптографическими системами. Этот недостаток вызван необходимостью параллельной работы ***Блока принятия решений*** и блока ***Активного алгоритма.***

При условии правильного подбора базы данных алгоритмов шифрования предложенная на рассмотрение система криптографической защиты информации для передачи данных в открытых сетях, по мнению авторов, может обеспечить приемлемый уровень защиты от большинства видов сетевых атак.

Список литературы:

1. H. Beker and F. Piper "Cipher Systems: The Protection of Communications" / London, Northwood Books, 1982.
2. M. Abadi and R. Needham "Prudent Engineering Practice for Cryptographic Protocols" / Research Report 125, Digital Equipment Corp Systems Research Center, Jun 1994.

3. R.J. Anderson "Solving a Class of Stream Ciphers" / Cryptologia, v. 14, n. 3, Jul 1990, pp. 285-288.

УДК 621.391:519.2

Алексейчук А. Н.

СЛУЧАЙНОЕ КОДИРОВАНИЕ В КАНАЛЕ СВЯЗИ С АДДИТИВНЫМ ШУМОМ, РАСПРЕДЕЛЕННЫМ НА КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЕ

Одним из известных эффективных способов повышения стойкости криптографических преобразований, применяемых в современных системах защиты информации, является случайное кодирование сообщений, при котором сигнал, используемый для передачи фиксированного сообщения $s \in S$, выбирается случайно из заданного множества сигналов (см., например, [1 – 4]). Достаточно общей математической моделью системы передачи информации со случайным кодированием является вероятностно-криптографическая система (ВКС) [5], представляющая собой совокупность дискретного источника, случайного кодера и произвольного дискретного канала. Указанная модель включает в себя в качестве частного случая понятие гомофонического (рандомизированного) шифра [2, 3] и может быть непосредственно использована при исследовании влияния случайного кодирования на неопределенность передаваемого сообщения [3, 5, 6], а также при анализе выходных последовательностей конечного автомата, функционирующего в условиях внешних помех и внутренних сбоев [7].

Центральной задачей анализа вероятностно-криптографических систем является разработка эффективных методов вычисления различных информационных или вероятностных характеристик реализуемых с использованием этих систем случайных отображений. Настоящая статья посвящена изучению одной из наиболее важных, с практической точки зрения, характеристик эффективности случайного кодирования дискретной информации в канале с аддитивным шумом, распределенным на конечной абелевой группе, – вероятности правильного приема сообщений оптимальным декодером канала.

Основные понятия и вспомогательные результаты.

Пусть S, X и Y – непустые конечные множества, $P_S = (p(s): s \in S)$ – распределение вероятностей (РВ) на множестве S, где $p(s) > 0$ для любого $s \in S$.

Вероятностно-криптографическая система определяется [5] как упорядоченная совокупность $\Re = (S, \sigma, W)$, состоящая из источника (S, P_S), сюръективного отображения σ: $X \to S$ и стохастической матрицы (канала) W с элементами $W(y/x)$, $y \in Y, x \in X$. Отображению σ ставится в соответствие случайный кодер – стохастическая матрица V с элементами $V(x/s)$, $x \in X, s \in S$ такая, что $V(x/s) > 0$ тогда и только тогда, когда $x \in C_s \overset{\text{def}}{=} \sigma^{-1}(s)$.

Предполагается, что источник вырабатывает случайное сообщение $s \in S$ с вероятностью $p(s)$, которое преобразуется в сообщение $x \in C_s$ с вероятностью $V(x/s)$. В свою очередь, x искажается в канале связи W и преобразуется с вероятностью $W(y/x)$ в доступное криптоаналитику выходное сообщение $y \in Y$.