ВСТРАИВАЕМАЯ СИСТЕМА ФОРМИРОВАНИЯ СИММЕТРИЧНОГО КЛЮЧЕВОГО ПРОСТРАНСТВА В СИСТЕМАХ С САМОСИНХРОНИЗИРУЮЩИМИСЯ КАНАЛАМИ СВЯЗИ

Д.М. Бильдюк, С.Б. Саломатин

Белорусский государственный университет информатики и радиоэлектроники,
кафедра радиотехнических систем
220013, Республика Беларусь, г. Минск, ул. П.Бровки, 6
телефон: (8017)293-89-83; e-mail: radno@tut.by

Материалы данной статьи относятся к области криптографической защиты информации и освещают вопросы формирования ключевого пространства встраиваемых систем защиты информации на базе симметричных алгоритмов шифрования. Отражена идея формирования самосинхронизирующегося режима шифрования, его преимущества по сравнению с классическими режимами шифрования при построении симметричного ключевого пространства.

Ключевые слова – защита информации, криптография, симметричное ключевое пространство, режим шифрования.

1 ОСНОВНОЙ ТЕКСТ

Известно, что симметричные алгоритмы шифрования могут быть использованы в различных режимах криптографического преобразования информации. Традиционно эти режимы классифицируют согласно американского стандарта FIPS 81, который уточняет подробности реализации алгоритма шифрования DES:

– электронная кодовая книга ECB (Electronic Code Book);

– сцепление блоков шифра CBC (Cipher Block Chaining);

– обратная связь по шифротексту CBF (Cipher Feed Back);

– обратная связь по выходу OFB (Output Feed Back).

Конечно, существуют и другие режимы работы симметричных алгоритмов шифрования, большинство которых являются незначительной модификацией указанных выше и применяются существенно реже. Из перечисленных режимов шифрования последние три имеют одну общую характеристику – наличие вектора инициализации (синхропосылка в алгоритме ГОСТ 28147), который используется как начальная гамма налаживаемая на шифр. Варьируя значением синхропосылки, можно получать различные шифротексты при одинаковых ключах шифрования. Хотя с другой стороны синхропосылку можно рассматривать как своеобразное удлинение ключа. Принципиально использование синхропосылки ничего не меняет, с точки зрения элементов системы и их канала связи. Т.е. требуется знание общего секрета (ключа) элементами системы на обоих концах канала связи (рисунок 1) плюс знание значения синхропосылки, которая передается по каналу связи непосредственно перед самим сообщением (или используется как часть ключа, при этом необходимо обеспечить ее конфиденциальность).

Рассмотрим систему с одним каналом связи и двумя элементами системы, и обозначим один из элементов системы главным, а второй подчиненным. Также присвоим элементам системы имена (или идентификаторы), которые будут представлять собой блоки информации размерностью равной размерности ключа. Сформируем ключ шифрования для главного элемента системы и обозначим его как мастер-ключ (МК), далее зашифруем на МК идентификатор (ID) подчиненного элемента системы и используем полученный шифротекст в качестве ключа (Kid) подчиненного элемента системы. Далее определим процедуры сеанса связи рассмотренных элементов системы следующим образом:

– Сообщение от главного к подчиненному. При отправке сообщения M подчиненному элементу главный должен обладать идентификатором подчиненного. Главный элемент шифрует ID подчиненного на своем МК, получая таким образом ключ шифрования Kid (Kid = MK(ID)) подчиненного, шифрует на Kid сообщение M (C = Kid(M)) и отправляет его подчиненному элементу системы. Подчиненный элемент, в свою очередь расшифровывает сообщение (M = Kid(C)) собственным ключом Kid.

– Сообщение от подчиненного к главному. В этом случае удобно использовать идею синхропосылки. Подчиненный шифрует сообщение собственным ключом Kid (C = Kid(M)) отправляет его главному вместе с собственным ID в качестве синхропосылки. Главный приняв сообщение шифрует синхропосылку на собственном МК (Kid = MK(ID)), полученный шифротекст использует в качестве Kid, на котором расшифровывает сообщение (M = Kid(C)).

Определенная выше система с одним синхроканалом связи и описанными процедурами сеанса связи изображена на рисунке 1.

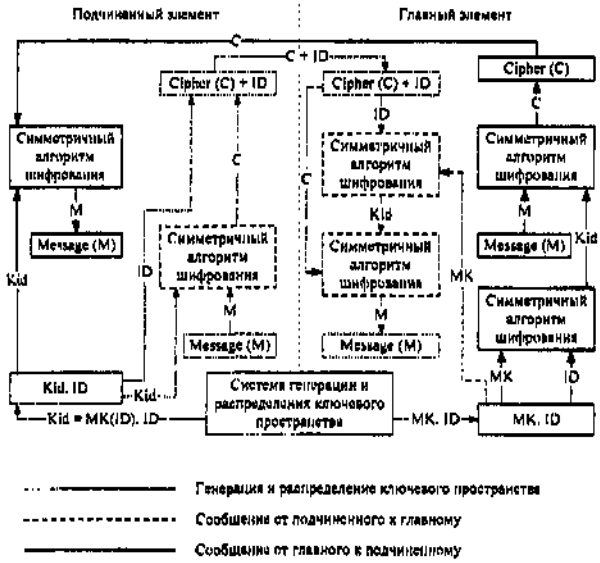

Рисунок 1.Организация самосинхронизирующегося канала в системах с одним каналом связи

Организация самосинхронизирующихся каналов связи имеет ряд преимуществ, существенность которых, особенно для клент-серверных систем, возрастает с числом элементов системы.

Рассмотрим наиболее общий случай организации систем с множеством каналов и принципом связи «многие ко многим», при использовании идеи самосинхронизирующихся каналов связи. Очевидно, что при такой организации каждый элемент системы может играть роль как клиента так сервера одновременно (причем на одном и том же канале связи), значит, в общем случае, каждый элемент системы должен обладать базой данных идентификаторов связанных с ним элементов системы. Также очевидно, что в такой системе должен быть главный элемент (или несколько равнозначных главных элементов) и подчиненные ему элементы, причем некоторые группы подчиненных элементов могут также носить характер равнозначных. Схема организации такой системы изображена на рисунке 2.

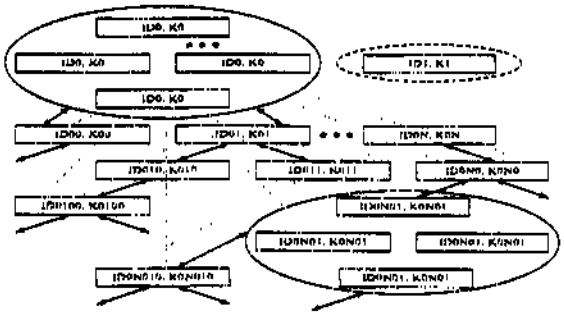

Рисунок 2. Организация самосинхронизирующегося канала в системах с множеством каналов связи

Из рисунка 2 видно, что использование самосинхронизирующихся режимов шифрования для организации ключевого пространства позволяет создавать встраиваемые криптографические системы защиты информации с любой иерархической структурой ее элементов и сложными перекрестными связями между ними. При этом такие системы имеют ряд преимуществ:

– синхронизация системы обеспечивается самим режимом шифрования симметричного алгоритма;

– повышается надежность системы и эффективность ее восстановления;

– повышается эффективность распределения ключевого пространства и его удаленной замены;

– снижаются требования к объему хранимой и защищаемой информации главных элементов системы;

– эксплуатация таких систем значительно проще и удобнее для конечного пользователя.

ЛИТЕРАТУРА

[1] Деднев М.А. Защита информации в банковском деле и электронном бизнесе. – Кудиц-образ, 2004. – 512 с.

[2] Мельников В.П. Информационная безопасность и защита информации: Уч. пос. 3-е изд. – Академия ИЦ, 2008. – 336 с.

[3] Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – БХВ-Петербуог, 2009. – 576 с.