УДК 004.056(043.2)

В.А. Марченко

Институт кибернетики имени В.М. Глушкова НАНУ, Киев

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ НА БАЗЕ НЕРАСКРЫВАЕМЫХ ШИФРОВ

В статье описываются подходы к разработке программно-аппаратных комплексов защиты, на базе алгоритмов, относящихся к классу нераскрываемых шифров. Описаны особенности алгоритма, косвенного шифрования который бы реализован внутри устройства на базе ПЦОС. Показаны подходы к адаптации нераскрываемых алгоритмов шифрования для реализации внутри аппаратной составляющей комплекса защиты. Приведены результаты испытаний, проведенные с созданным устройством на базе ПЦОС. Описаны основные недостатки решений на базе нераскрываемых шифров и алгоритма косвенного шифрования, а также приведены возможные направления их решения.

Ключевые слова: *криптография, нераскрываемые шифры, косвенное шифрование, ПЦОС.*

Введение

Успехи в развитии современных вычислительных средств привели к возможности практической реализации различных криптографических атак на современные криптографические средства защиты. Поэтому одним из наиболее перспективных направлений создания новых средств защиты является применение нераскрываемых шифров [1].

Класс нераскрываемых шифров определяется как подмножество криптографических алгоритмов, имеющих теоретически доказанную криптостойкость [2]. Таким образом, применение нераскрываемых шифров для организации защиты информации в различных информационных системах позволяет гарантировать её защищённость в независимости от появления новых вычислительных средств с большей производительностью или кардинально новыми возможностями.

Состояние проблемы

Существующие программно-аппаратные комплексы защиты информации в аппаратной составляющей в качестве алгоритма криптографических преобразований зачастую используют симметричные алгоритмы (AES) или ассиметричные (RSA). Поэтому переход на нераскрываемые алгоритмы требует решения ряда прикладных задач:

1) реализация алгоритма шифрования;

2) адаптация алгоритма под заданную аппаратную платформу;

3) организация взаимодействия полученного комплекса в рамках ИС.

Проблемы, связанные с организацией взаимодействия полученных аппаратных устройств с различными приложениями внутри защищаемой ИС, выходят за рамки вопросов, рассматриваемых в данной статье. Но следует отметить, что при реализации программной составляющей комплекса защиты следует придерживаться существующих подходов и методик интеграции аппаратных комплексов в программные приложения [3, 4].

Описание алгоритма шифрования

В качестве алгоритма, для которого разрабатывался аппаратный комплекс, был использован алгоритм косвенного шифрования [5], принадлежащий к классу нераскрываемых шифров. Суть алгоритма заключается в том, что полезная для перехвата информация вообще не передается по каналу, а передаётся образ этой информации, отображенный на объект (контейнер-ключ) используемый в качестве ключа (рис. 1). При шифровании производится перестановка байтов согласно информации хранящейся в двумерной таблице (вектор перекодировки) таким образом, получается проекция шифруемого файла на указанную таблицу. Каждый байт шифруемых данных заменяется на один из байтов в таблице.

Для реализации этого алгоритма был выбран вариант, описанный в работе [6]. Он имеет ряд особенностей, которые необходимо учитывать при разработке аппаратной составляющей защитного комплекса. Как известно [2], криптографическая стойкость для нераскрываемых шифров определяется качеством используемого ключа. Доказанную криптостойкость обеспечивает только абсолютно случайный контейнер-ключ, полученный с генератора истинно случайных значений. При этом длина этого ключа должна быть не меньше информационного сообщения, которое пересылается. Эти особенности следует учитывать при практической реализации комплекса защиты.

Изначально предполагается, что комплекс защиты может быть использован в ИС с различными требованиями к безопасности. Так в системах, где требуется максимальный уровень защиты необходимо использовать только истинно-случайные значения для контейнера-ключа.

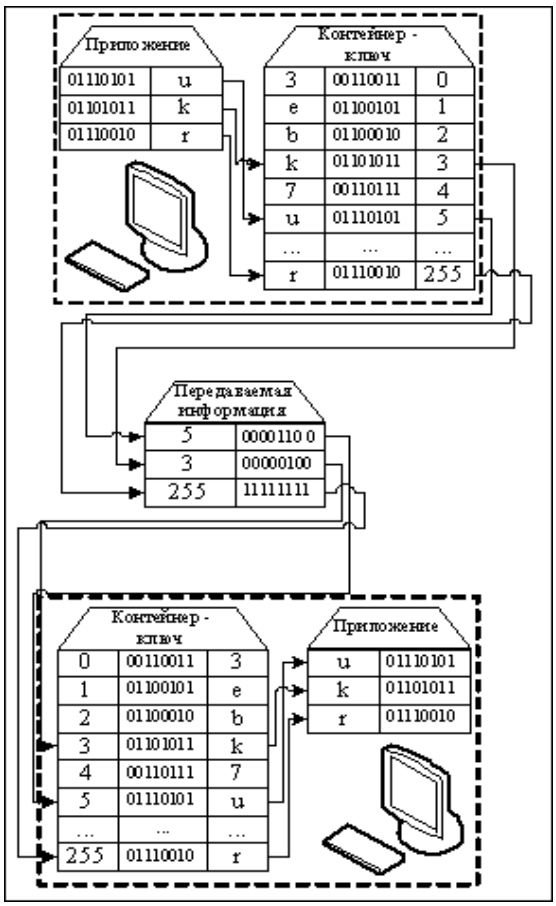

Рис. 1. Схема алгоритма шифрования

В системах, где нет подобных ограничений, допускается использование псевдослучайных алгоритмов генерации контейнера-ключа. При этом следует отметить, что условием применение того или иного генератора ПСЧ определяется требованиями защищенности ИС в которой планируется использовать программно-аппаратный комплекс защиты. То есть сертификация ИС на соответствие заданному (требуемому) уровню защищенности определяет и подмножество криптостойких генераторов ПСЧ, которые могут быть использованы в различных криптографических средствах для обеспечения необходимого уровня защищенности.

Поэтому применение этих КГПСЧ для создания ключа-контейнера позволяет выполнять требования, выдвигаемые к защищаемой ИС.

Особенности реализации предложенных алгоритмов

В алгоритме № 1 (рис. 2) заранее создается таблица перекодировки и сохраняется во флэш-памяти устройства. В данном случае предполагается использования дополнительной инфраструктуры которая обеспечивает генерацию необходимого объёма контейнера-ключа с заданными требованиями по криптостойкости. Данные контейнер-ключи записываются на флэш-носители и устанавливаются внутрь устройства.

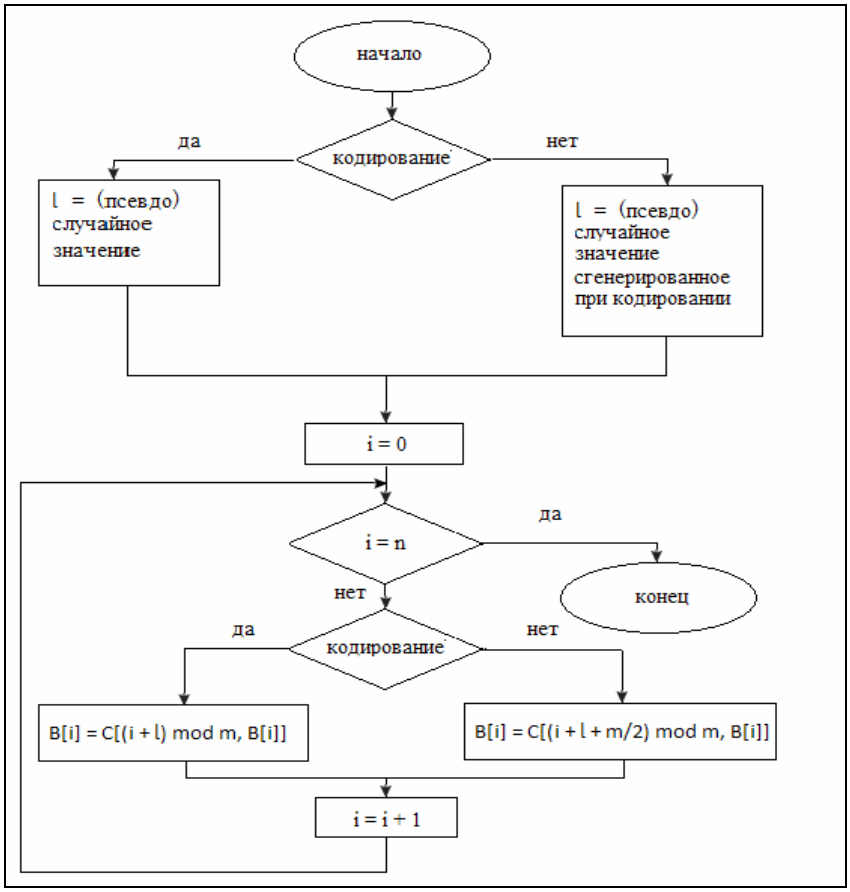

Рис. 2. Блок-схема алгоритма № 1

Указанная схема процесса обмена ключами обладает большими организационными сложностями в сравнении с существующими методами обмена ключевой информацией. Но это связанно с гарантированным уровнем безопасности, который обеспечивается применением нераскрываемых шифров. Стремительное развитие микроэлектроники позволило создать флэш карты объёмом порядка 128-512 Гбайт. И в дальнейшем доступный объем будет только увеличиваться. Соответственно накладные расходы необходимые для обеспечения синхронизации контейнер-ключа между устройствами будут уменьшаться.

В текущей реализации алгоритма шифрования кодирование и декодирование становится возможным благодаря структуре таблицы перекодировки (адаптированный контейнер-ключ), особенности которой описаны ниже.

Согласно математической модели алгоритма [6, 7] контейнер-ключ представляет собой таблицу из строк фиксированной длины. Длина строк определяется минимальной единицей адресации в применяемых вычислительных средствах, в данном случае, – это один байт. Таким образом, полная длина строки будет равняться 256 байт, как полный набор всех возможных значений выбранной единицы. Соответственно, эта строка должна содержать только уникальные значения байта из диапазона 0-255. Расположение этих значений должно быть случайно в рамках строки и не коррелировать с другими строками таблицы перекодирования.

В этой реализации ключом шифрования будет являться смещение в рамках таблицы перекодирования, с которого будут браться строки для криптографических преобразований. Процедура шифрования заключается в поиске значения элемента в выбранной строке используя указанный индекс. Процедура дешифрования заключается в решении обратной задачи, нахождения индекса элемента в строке по его значению.

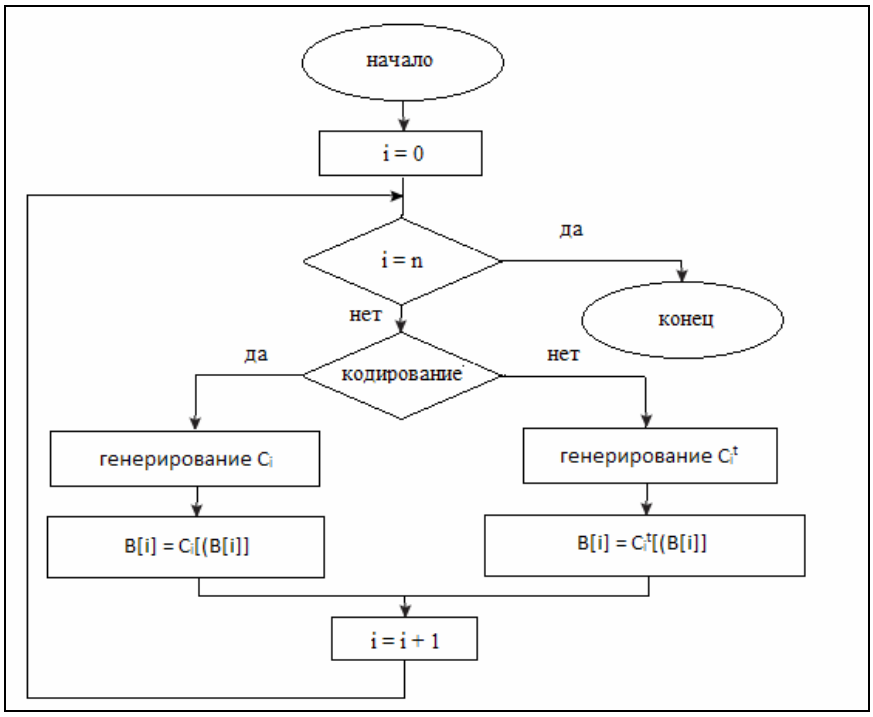

Рис. 3. Блок-схема алгоритма №2

В алгоритме №2 (рис. 3) эта таблица перекодирования создается "на лету" во время выполнения процедуры шифрования или дешифрования.

При использовании этого алгоритма процесс работы устройства состоит из двух базовых этапов:

1) синхронизация параметров генерации между устройствами;

2) выполнение криптографических преобразований.

Предполагается, что внутри устройства установлен отдельный генератор КГПСЧ, поэтому для инициализации его работы необходимо согласовать ряд параметров между устройствами. Объём данных, который нужно согласовать, соизмерим с объёмом данных ключей шифрования для современных алгоритмов шифрования.

Поэтому для процедуры согласования параметров хорошо подходят существующие алгоритмы синхронизации ключей.

Они должны выбираться исходя из требований, указанных выше. То есть алгоритм согласования параметров также выбирается из подмножества доступных алгоритмов, которые соответствуют нужному классу защищенности ИС.

После согласования запускается генератор с выбранными параметрами и начинается процедура генерации значений. Эта процедура запускается в отдельном потоке внутри устройства и не прекращается до момента отключения устройства. Возможен только её перезапуск с новыми параметрами инициализации генератора. Это позволяет реализовать режим буферизации для сглаживания всплесков объёма данных переданных для шифрования.

В реализованных алгоритмах процесс криптографических преобразований работает используя модель ассоциативной памяти [8].

Поэтому для построения реализации этой модели используются две различные таблицы перекодирования.

Из полученных значений генератора формируются строки для таблицы перекодирования которая используется для выполнения процесса шифрования. Требования к процессу формирования такие же, как и для алгоритма №1.

Формирование таблицы перекодирования, которая используется для дешифрования происходит следующим образом. Каждая строка этой таблицы генерируется с использованием данных из соответствующей строки первой таблицы. Для этого берется текущий элемент из выбранной строки, он имеет в качестве индекса значение j и содержимое со значением k. И во вторую таблицу в выбранную строку записывается значение j по индексу со значением k. Этот процесс повторяется для всех строк таблицы шифрования последовательно.

Использование двух различных таблиц позволяет реализовать симметричность процесса шифрования и дешифрования используя только стандартную элементную базу (т.е. не применяя аппаратной ассоциативной памяти). При этом увеличивается в два раза объём оперативной памяти необходимой для хранения двух таблиц, что не является критичным для современных устройств.

Результаты экспериментов

Указанные алгоритмы были реализованы внутри аппаратного устройства на базе процессоров цифровой обработки сигналов (ПЦОС). Данные процессоры были выбраны исходя из их конструктивных особенностей. Они представляют собой интегрированное устройство, состоящее из самого процессора и набора контроллеров и шин для прямого подключения периферийных устройств, таких как ОЗУ, ПЗУ, порт USB и т.п.

Ряд экспериментов, которые были проведены с полученным устройством, позволили получить некоторые оценочные характеристики производительности предложенных алгоритмов (рис. 4).

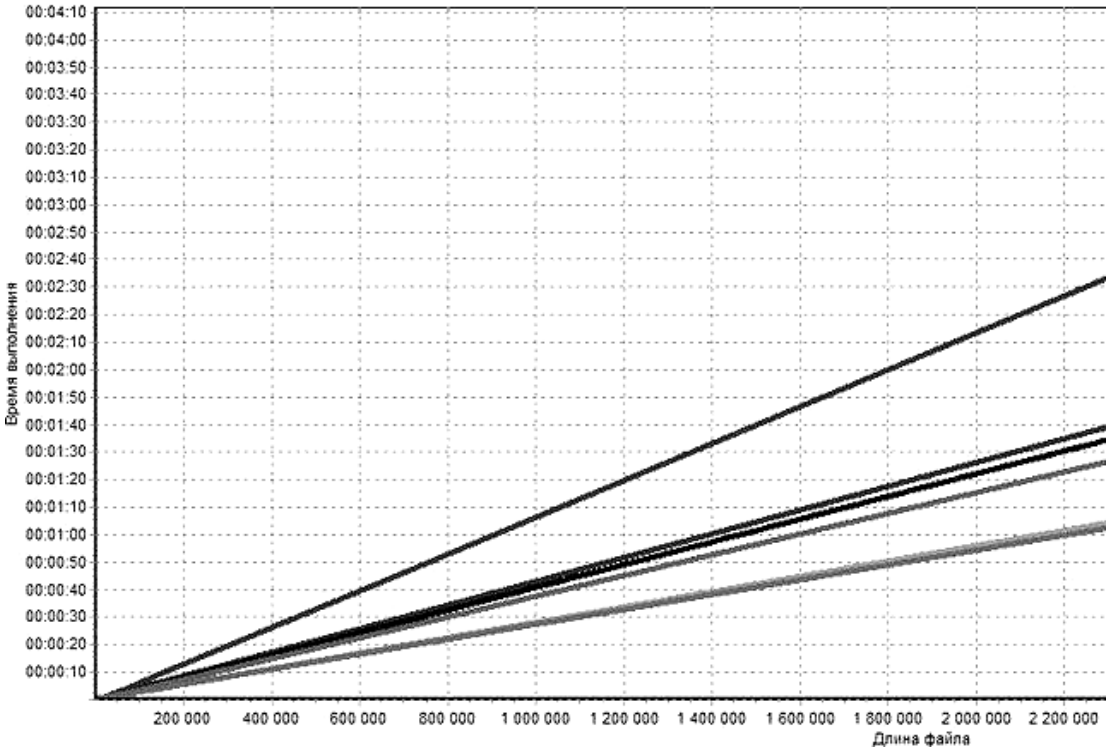

Рис. 4. График испытаний

В первую очередь следует отметить явно выраженный линейный характер зависимости длинны обрабатываемого файла и времени криптографического преобразования.

Также испытания показали невысокую скорость выполнения криптографических преобразований при использовании маломощных ПЦОС. При этом следует отметить, что ПЦОС старших серий

имеют на порядок большую производительность, что позволяет повысить общую производительность средств защиты путем простой замены процессора и соответствующей элементной базы.

Выводы

Алгоритмы шифрования, относящиеся к классу нераскрываемых шифров, в частности и метод косвенного шифрования, могут быть использованы в различных информационных системах, для обеспечения защиты информации с доказуемой криптостойкостью, хотя это и связанно с рядом технических трудностей.

Было обнаружено ряд проблем применения подобных алгоритмов в программно-аппаратных комплексах защиты информации.

В первую очередь, это объём контейнера-ключа, который соизмерим с объёмом зашифрованных данных. Поэтому для систем с максимальными требованиями к защите необходимы дополнительные мероприятия организационного характера для у правления и синхронизации контейнера-ключа между различными устройствами.

Применение КГПСЧ ограничивает криптостойкость защиты информации криптостойкостью самого генератора. Для решения данной проблемы возможно использования нескольких генераторов, но это добавляет ряд трудностей конструктивного характера.

Было обнаружено ряд проблем теоретико-прикладного характера. Так все существующие подходы к построению КГПСЧ опираются на уникальность сгенерированного числа большой разрядности, но при этом, могут иметь повторяемость байтов внутри полученного числа. Это открыло две проблемы, которые требуют дополнительных исследований.

Первая – разработка нового класса КГПСЧ, для которого помимо существующих ограничений добавляется ограничение на уникальность получаемой цепочки байт внутри числа.

Вторая – быстрое формирование строки, для таблицы преобразования используя значения КГПСЧ с повторяющимися цепочками байт.

Список литературы

1. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — М.: ГелиосАРВ, 2005. – 480 с.

2. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике / К. Шеннон. – М.: Изд. иностр. лит., 1963. – С. 333 – 369.

3. Uncover Security Design Flaws Using The STRIDE Approach / Shawn Hernan, Scott Lambert, Tomasz Ostwald, Adam Shostack // MSDN Magazine. – November 2006. – P. 68–75.

4. Cryptographic Service Providers [Электронный ресурс]. – Режим доступа к материалам: http://msdn.microsoft.com/en- us/library/aa380245%28VS.85%29.aspx.

5. Алишов Н.И. Косвенная стеганография как новый способ передачи секретной информации / Н.И. Алишов, В.А. Марченко, С.Г. Оруджева // Комп'ютерні засоби, мережі та системи: зб. наук. пр. – К.: НАНУ, Ін-т кібернетики, 2009. – № 8. – С. 105–112.

6. Зубов А. Совершенные шифры / А. Зубов. – М.: Гелиос АРВ, 2003. – 160 с.

7. Марченко В. Краткая математическая модель метода косвенного шифрования с фиксированными ключами / В. Марченко // Системи обробки інформації. – Х. : ХУПС, 2012. – № 4(102), т. 1. – С. 128-132.

8. Кохонен Т. Ассоциативные запоминающие устройства / Т.. Кохонен. – М.: Мир, 1982. – 384 с.

Поступила в редколлегию 5.05.2014

Рецензент: д-р техн. наук, проф. Н.И. Алишов, Институт кибернетики им. В.М. Глушкова НАН Украины, Киев.

РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ЗАХИСТУ НА БАЗІ ШИФРІВ ЩО НЕ РОЗКРИВАЮТЬСЯ

В.А. Марченко

У статті описуються підходи до розробки програмно-апаратних комплексів захисту , на базі алгоритмів які відносяться до класу шифрів що не розкриваються. Описано особливості алгоритму непрямого шифрування який був реалізований всередині пристрою на базі ПЦОС. Показані підходи до адаптації алгоритмів шифрування що не розкриваються для реалізації всередині апаратної складової комплексу захисту. Наведені результати випробувань, які були проведені зі створеним пристроєм на базі ПЦОС. Описано основні недоліки рішень на базі шифрів що не розкриваються і алгоритму непрямого шифрування, а також наведені можливі напрямки їх вирішення.

Ключові слова: *криптографія, непряме шифрування, шифри що не розкриваються, ПЦОС*

DEVELOPMENT SOFT-HARDWARE DATA PROTECTION SYSTEM BASED ON UNDISCLOSED ENCRYPTS

V.A. Marchenko

This article describes approaches to the development soft-hardware data protection system based algorithms belong to the class undisclosed ciphers. The features of the algorithm indirect encryption that would have been implemented in the device based on the DSP. Showing approaches to adaptation undisclosed encryption algorithms for the implementation of the hardware component of the complex data protection. The results of tests carried out with the device created based on the DSP. The basic disadvantages of solutions based on undisclosed ciphers and algorithm indirect encryption and provides possible directions for solving them.

Keywords: *cryptography, indirect encryption, undisclosed encrypt, DSP*