Васильева И.Н., Семенова С.О. Состав и характеристики аппаратных шифраторов // Образование и наука: современное состояние и перспективы развития. Сборник научных трудов по материалам Международной научно-практической конференции 31 августа 2015 – Тамбов, 2015. – С. 19-23.

Васильева И.Н., Семенова С.О.

Состав и характеристики аппаратных шифраторов

СПбГЭУ, г. Санкт-Петербург

Криптографическая защита является традиционным и наиболее надежным методом обеспечения конфиденциальности информации, как при ее хранении, так и при передаче. Криптографическая защита информации обеспечивается с помощью шифраторов, которые могут быть выполнены в виде программных, программно-аппаратных или аппаратных модулей.

Аппаратные шифраторы представляют собой, как правило, плату, подключаемую к системной плате компьютера посредством разъемов ISA или PCI. Реже устройство выполняют в виде отдельного средства защиты, обладающего корпусом с дисплеем и переключателями режимов. Так как использование отдельной платы для выполнения исключительно шифрования является нецелесообразным, производители снабжают устройства дополнительными функциями: генерация случайных чисел, контроль целостности программных файлов, контроль доступа к информации и т.д. Плата с перечисленными выше функциями представляет аппаратное средство криптографической защиты информации (СКЗИ).

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность операционной системы, называют также «электронным замком». Такое устройство должно иметь соответствующее программное обеспечение, а для корректной работы необходима его настройка администратором безопасности. При включении компьютера, устройство криптографической защиты данных будет запрашивать ключи и не позволит продолжить загрузку, пока они не будут корректно введены. В случае передачи управления компьютеру, встроенные в шифратор функции через некоторое время заблокируют работу пользователя. Это в полной мере защитит информацию от попыток несанкционированного доступа к ней.

Аппаратный шифратор – надежное, но более дорогостоящее по сравнению с программными реализациями СКЗИ. Приобретение аппаратного шифратора целесообразно, прежде всего для компаний, обрабатывающих большие объемы конфиденциальной информации, например в налоговой или банковской сфере. Заказчик может выбрать состав и функциональность устройства исходя из специфики его компании. Дополнительные функции позволят защитить информацию не только от утечек по каналу связи, но и от несанкционированного доступа к компьютерной системе.

На российском рынке СКЗИ представлены устройства компаний ОКБ САПР (Аккорд), «Анкад» (Криптон) и «Код безопасности», представляющие собой программно-аппаратные комплексы защиты информации, в состав которых входят, в том числе, аппаратные шифраторы, а также аппаратно-

программные модули доверенной загрузки, системы разграничения доступа, мониторинга и другие компоненты. Указанные СКЗИ поддерживают российские криптографические стандарты и имеют сертификаты ФСБ РФ.

СКЗИ, использующиеся в системах защиты следующих сведений, не составляющих государственную тайну: персональные данные, служебная тайна (служебная информация государственных и муниципальных органов власти), подлежат обязательной сертификации ФСБ РФ, для банковской информации такая сертификация носит рекомендательный характер (в соответствии со СТО БР ИББС).

Можно выделить минимальный набор функций, которыми должен обладать типовой шифратор:

- реализация отечественных криптоалгоритмов ГОСТ 28147–89 (ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012);
- программный интерфейс;
- возможность аутентификация пользователя;
- наличие датчика случайных чисел;
- реализация защищенного сетевого протокола;
- поддержка ввода ключей с ключевых носителей.

При проектировании аппаратного шифратора производитель может добавлять дополнительные микросхемы для обеспечения надежности процессов шифрования. Однако все аппаратные СКЗИ имеют одинаковый набор базовых функциональных модулей. Основными модулями аппаратного СКЗИ являются:

1) Блок управления. Обычно реализуется на базе микроконтроллера. Блок управления предназначен для управления работой СКЗИ: переключение режимов работы, определения состояния СКЗИ при включении и управлении в процессе работы, осуществления взаимодействия со средствами ввода ключевой информации.

2) Шифропроцессор. Представляет собой специализированную микросхему или микросхему программируемой логики (PLD– Programmable Logic Device). Шифропроцессор выполняет криптографические преобразования данных на ключах, которые хранятся в энергонезависимых банках памяти. Блок шифропроцессора состоит, как правило, из основного и дублирующего шифраторов, предназначенных для дублированного выполнения процедур шифрования. Результаты основного и дублирующего шифрования сравниваются с целью контроля исправности функционирования.

3) Блок датчика случайных чисел (ДСЧ). Предназначен для формирования запаса псевдослучайных последовательностей, используемых при генерации ключей шифрования, вычисления имитовставки и электронной подписи. Датчик случайных чисел может быть реализован как программно на базе шифропроцессора, так и физически в виде отдельной микросхемы. Принцип работы физического ДСЧ основан на выработке случайного сигнала, который преобразуется в двоичную последовательность.

4) Блок подключения внешних устройств. Управляет процессом взаимодействия СКЗИ с внешними устройствами. Обеспечивает подключение к ком-

пьютеру, обмен командами и данными между шифратором и внешними устройствами. Может быть реализован на микросхеме управления СКЗИ.

5) Блок долговременного хранения ключевой информации. Представляет собой энергонезависимую память, в которой хранятся комплекты основных и резервных ключей, файлы программного обеспечения СКЗИ, журналы с результатами контроля исправности и др. Ключевая информация хранится в зашифрованном и имитозащищенном виде. Для обеспечения целостности рассчитывается контрольная сумма, проверяемая при каждом включении устройства. Считывание и запись в блок осуществляется блоком управления СКЗИ.

6) Блок ввода ключевой информации. Предназначен для ввода в устройство ключевой информации при начальной инициализации устройства. Ключевая информация вводится с ключевых носителей типа смарт-карт с одновременным контролем ввода путем проверки контрольных сумм. Хранение ключей на смарт-картах и их ввод в устройство с помощью интерфейсов для подключения ключевых носителей позволяет обеспечить более надежную защиту.

Для повышения надежности процесса шифрования, модификации ключей и проверки правильности результатов шифрования, шифропроцессор (ЦСП) логически разделяют на несколько функциональных блоков:

1) Вычислитель – набор регистров, сумматоров, блоков подстановки, связанных между собой шинами передачи данных. Выполняет криптографические действия с данными. На вход вычислитель получает открытые данные, которые зашифровывает с помощью ключа шифрования. Зашифрованная выходная последовательность данных схожа с последовательностью случайных величин.

2) Блок управления – аппаратно реализованная логика управления вычислителем. Сбои в работе блока могут привести к некачественному шифрованию, вследствие чего, возможны утечки информации в канал связи. С целью повышения надежности шифратора используется программно-временное дублирование процесса шифрования. Два шифратора (основной и дублирующий) преобразовывают одинаковые входные данные со сдвигом в алгоритме на один шаг. Конечный результат поступает в микросхему сравнения для проверки. При несовпадении результатов данные зашифровываются повторно.

3) Буфер ввода-вывода. Необходим для повышения производительности устройства: в процессе шифрования первого блока данных, в буфер поступает следующий блок и т.д. Алгоритм вывода информации аналогичен. Такой способ передачи данных значительно увеличивает скорость процедур шифрования и дешифрования.

Наряду с доступной функциональностью важны эксплуатационные качества аппаратного СКЗИ, которые определяются скоростью выполнения операций, уровнем надежности, а в ряде случаев – и уровнем защищенности, то есть способностью противостоять целенаправленным воздействиям. Применение детекторов воздействий и дополнительного экранирования позволяет повысить защищенность шифратора, однако может существенно увеличить стоимость реализации, поэтому целесообразно лишь для отдельных сфер применения (например, в военной области).

Одним из важнейших критериев оценки аппаратных шифраторов является потоковая скорость обработки данных. Главным образом она зависит от реализованного в шифраторе криптоалгоритма. Потоковая скорость оценивается по формуле $V = F*k / n$, где F – тактовая частота микропроцессора, k – размер блока информации, подлежащей шифрованию, n – число тактов алгоритма, требующихся для шифрования одного блока информации [1].

Аппаратные шифраторы чаще всего реализуются на базе сигнальных процессоров (цифровых сигнальных процессоров, ЦСП), обладающих высоким быстродействием. Эффективность выполнения основных функций шифратора и его надежность в наибольшей степени определяется используемым ЦСП, который является центральным критическим компонентом элементной базы шифратора. Анализ рынка показывает практическое отсутствие отечественных производителей элементной базы аппаратных шифраторов, лидерами в производстве микросхем являются компании Texas Instruments, Freescale Semiconductor и Analog Devices [2].

СКЗИ должны обеспечивать заданный уровень надежности применяемых криптографических преобразований, определяемый значением допустимой вероятности неисправностей или сбоев, которые могут привести к потенциально опасным последствиям:

- утечка открытой информации в канал связи;
- утечка ключевой и криптографически опасной информации в канал связи;
- несанкционированный доступ к ключевой и криптографически опасной информации;
- попадание конфиденциальной информации, подлежащей шифрованию, к техническому персоналу в незашифрованном виде.

Надежность является комплексным свойством, которое в зависимости от назначения СКЗИ и условий его применения может включать безотказность, долговечность, ремонтопригодность и сохраняемость или определенные сочетания этих свойств. В основе определения вероятностей сбоев, приводящих к возникновению потенциально опасных событий, лежит расчет интенсивности отказов составных элементов шифратора. СКЗИ, не предназначенные для защиты сведений, составляющих государственную тайну, должны соответствовать «Требования к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» согласно положению (ПКЗ-2005), утвержденному приказом ФСБ РФ от 09.02.2005 г. № 66. Указанные требования предусматривают соответствие значений вероятностей и классов защищенности СКЗИ.

Соответствие значений вероятностей возникновения опасных событий для используемых ЦСП и значений вероятностей, регламентируемых требованиями к СКЗИ, определяет класс СКЗИ, а следовательно, возможность его применения в системах защиты конфиденциальной информации.

Литература:

1. Панасенко С.П., Ракитин В.В. Аппаратные шифраторы // Мир ПК. – 2002 – № 8 – С. 77-83.

2. Пантелейчук А.Р. Основы выбора цифровых сигнальных процессоров // Электронные компоненты. – 2010. – №6 – С. 13-17.