значимости. Функция открытия контекста генератора может быть выполнена успешно, если объект генератора успешно создан в системе и выполнены загрузочные тесты устройства.

Функция генерации последовательности случайных чисел (или чтение из генератора), используя созданный при открытии объект генератора, выполняет чтение последовательности данных из устройства. Затем получаемые блоки случайных данных фильтруются в драйвере устройства. Фильтр блоков случайных данных построен на основе методики статистического тестирования стандарта FIPS 140-1. Если статистические параметры полученных данных не удовлетворяют рассчитанным доверительным интервалам, то блок отбрасывается и выполняется повторное чтение нового блока из генератора.

В процессе работы с аппаратным генератором необходимо выполнять техническое тестирование генератора. Такую возможность предоставляет функция открытия контекста генератора.

Функция закрытия контекста аппаратного генератора выполняет удаление объекта генератора из системы, очистку системных ресурсов, занимаемых генератором, то есть непосредственное закрытие и удаление контекста аппаратного датчика.

Программная реализация алгоритма генерации псевдослучайных чисел, описанного в стандарте ANSI X9.17, включает в себя аналогичные программные компоненты, используемые в программной модели аппаратного генератора. Работа с программным генератором построена на тех же функциях, что и элементы управления аппаратным датчиком.

Функция открытия контекста программного генератора выполняет создание объекта генератора, содержащего его параметры: ключи алгоритма шифрования ГОСТ 28147-89 и текущие параметры генерации. Объект генератора создается в безопасной памяти (технология безопасной памяти). Параметры, содержащиеся в объекте, используются в процессе генерации.

Функция генерации выполняет программное формирование последовательности случайных чисел с использованием созданного объекта программного генератора. Как и в случае аппаратного генератора сформированные блоки случайных данных фильтруются программным фильтром.

Функция закрытия контекста программного генератора выполняет удаление объекта генератора из безопасной памяти. При этом параметры генератора удаляются.

Заключение

Реализованные компоненты аппаратных и программных генераторов встроены в системы защиты информации для компьютерных систем на основе программных платформ Win32®. Основная часть элементов управления реализована программно и функционирует в пользовательском режиме (user-mode), кроме драйверов аппаратных генераторов, работающих в режиме ядра (kernel-mode).

Все программные и аппаратные компоненты корректно встраиваются в аппаратную платформу и операционную систему. Встроенные компоненты функционируют стабильно, обеспечивая выполнение возложенных на них функций. Параметры выходных данных генераторов постоянно контролируются фильтрами и контроллерами. Корректность инициализации генераторов обеспечивает выполнение загрузочных тестов. Статистические параметры тестирования проверены и проанализированы на этапе отладки. Правильность и стабильность функционирования элементов управления обеспечивает постоянный контроль над качеством выходных последовательностей.

Литература: 1. FIPS PUB 140-1. Cryptographic modules security requirements // NIST, 1993. 2. А. Менезис, П. ван Оршот, С. Ватсон. Прикладная криптография // CRC Press, 1996. Глава 5. 3. ANSI X9.17. "American National Standard for Financial Institution Key Management (Wholesales)" American Bankers Association, 1985.

УДК 681.325

ПРИНЦИПЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ СЕРИИ “ГРЯДА”

Михаил Бондаренко, Иван Горбенко, Андрей Свинарев, Александр Столяр, Виктор Лапин
Харьковский государственный технический университет радиоэлектроники

Аннотация: **Рассматриваются проблемные вопросы проектирования, разработки, испытания и эксплуатации аппаратных средств защиты информации на примере устройств серии «Гряда».**

considered, taking the "Gryada" hardware series as an example.

Ключевые слова: **Аппаратные средства, защита информации, криптографические алгоритмы, надежность аппаратных средств.**

Введение

Проведенные многочисленные исследования и опыт применения средств криптографической защиты информации (КЗИ) в автоматизированных системах и сетях показывают, что требуемое качество КЗИ может быть обеспечено только при условии аппаратной реализации основных криптографических функций – криптографических преобразований, управления ключами, криптографических протоколов и т. д. На сегодняшний день разрешены и нашли применение аппаратные, аппаратно-программные и программные реализации КЗИ. Применительно к компьютерным системам программные реализации представляют собой либо одно из приложений, либо криптопровайдер с соответствующими функциями КЗИ. Программно-аппаратная реализация, как правило, состоит из программного обеспечения (ПО) и аппаратной реализации одной или нескольких функций, например, генерация ключей, защита от НСД, ускорители криптографических преобразований и т. д. Однако в обеих названных реализациях средства находятся под контролем операционной системы (ОС) и, как правило, при их работе может быть осуществлен перехват ключей, информации, паролей или нарушение протокола взаимодействия ОС со средствами КЗИ. Кроме того, если ключи и пароли вводятся с периферийных устройств, управляемых ОС, то они могут быть перехвачены (скомпрометированы) специальными встроенными в ОС средствами или с помощью вирусов. Таким образом, программные и программно-аппаратные средства КЗИ могут выполнять различные криптографические преобразования и протоколы с требуемой надежностью только при условии, если ОС защищена от указанных несанкционированных действий и вирусов и на ней реализован комплекс мероприятий по защите. В большинстве случаев выполнение названного комплекса требований, особенно в части защиты от незапланированных функций, встраиваемых в ОС различными способами, практически невозможно. Разрешение этого противоречия может быть достигнуто, если все криптографические преобразования и протоколы выполняются независимо от ОС, а ключи и пароли вводятся без участия ОС. Названные требования могут быть выполнены, если все криптографические функции – цифровая подпись, симметричное и направленное шифрование, генерация ключей и паролей, хранение ключей, создание и хранение баз сертификатов – осуществляются аппаратно или аппаратно-программно. Например, в специализированном процессоре основные принципы взаимодействия спецпроцессора и ОС должны осуществляться с использованием состоятельных протоколов их взаимодействия и информационного обмена.

Проведенные исследования показали, что указанные требования могут быть выполнены за счет создания и применения специализированных процессоров в виде аппаратных или аппаратно-программных реализаций. С этой целью в ХТУРЭ и АО "ИИТ" созданы и эксплуатируются ряд средств КЗИ серии "Гряда". Серия включает в себя процессоры (модули) "Гряда-1", "Гряда-1М", "Гряда-11", "Гряда-31", "Гряда-31М". Краткая характеристика аппаратных средств "Гряда" представлена в таблице 1.

Таблица 1

Наименование	Назначение	Интерфейс	Процессор
«Гряда-1»	Генератор случайных чисел	ISA	Нет
«Гряда-1М»	Генератор случайных чисел	RS-232	Нет
«Гряда-11»	Процессор КЗИ	ISA	ADSP 21062
«Гряда-31»	Процессор КЗИ	PCI-32	ADSP 21062
«Гряда-31М»	Процессор КЗИ	PCI-32	ADSP 21061

I Основные функции КЗИ

Основными функциями криптографической защиты, реализуемыми в "Гряде-11", "Гряде-31"и "Гряде-31М" на аппаратном уровне, являются:

- криптографическое преобразование информации с использованием стандартных криптографических алгоритмов (стандартов);
- генерация ключей цифровой подписи, симметричного и направленного шифрования;
- хранение конфиденциальных ключей и сертификатов;
- загрузка ключей с внешнего, независимого от ОС, носителя (электронная карточка touch memory и др.);
- запись сгенерированных ключей на внешний носитель или передача по состоятельному протоколу вне процессора;
- загрузка и хранение специальных данных, параметров ОС и др.;
- генерация случайных последовательностей (ключей, подписей, параметров и др.);

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

- хранение в зашифрованном виде ПО самого процессора и критичного ПО ОС;
- выполнение различных преобразований с целью обеспечения защиты от НСД;
- обеспечение целостности и конфиденциальности критичного ПО внешних ОС;
- выполнение различных фискальных функций.

Повышение уровня защиты информации и защиты от НСД осуществляется на аппаратном уровне за счёт применения следующих методов инженерной криптографии:

1) обеспечения минимально возможного взаимодействия прикладного ПО и ОС персонального компьютера (ПК) с аппаратными средствами (АС) за счёт:

- использования специального командного (процедурного) интерфейса взаимодействия прикладного ПО с АС, обеспечивающего невозможность прямого доступа прикладного ПО и ОС к ресурсам АС (памяти, процессору и т. п.) и предусматривающего обязательную первоначальную инициализацию АС с применением ключей (паролей) доступа заданной длины (не менее 8 байт);
- взаимодействия прикладного ПО (ОС) с АС через «прозрачный» для пользователя «почтовый ящик» (буфера обмена: приёмный и передающий, физически расположенные в АС и недоступные для прямого чтения/записи прикладному ПО и ОС);
- хранения криптографических алгоритмов (исполняемых модулей) в энергонезависимой памяти (ЭНП) АС в шифрованном виде (т. о. отпадает необходимость загрузки алгоритмов «извне»).

2) применения резервированного (дублированного) генератора случайных чисел для формирования физических ключей заданной длины;

3) загрузки исполняемых криптографических алгоритмов из ЭНП во встроенное ОЗУ (RAM) микропроцессора в шифрованном виде;

4) исполнения криптографических алгоритмов только из встроенного ОЗУ микропроцессора (с предварительным дешифрированием непосредственно в данном ОЗУ);

5) хранения шифрованных данных в ЭНП в структурированном виде с применением различных методов контроля (например, контрольное суммирование загружаемых программных модулей) для обеспечения контроля достоверности и целостности информации;

6) передачи данных (ключевой информации, загружаемых криптографических алгоритмов, результатов промежуточных вычислений и т. д.) по внутренним шинам АС только в шифрованном виде;

7) «прошивки» отдельных ключей (например, ключа, который используется при инициализации АС) в «железе» с обеспечением гарантированной невозможности «извлечения»;

8) применения «оперативно загружаемой схемотехники» в аппаратных ускорителях;

9) использования внешних ключей, загружаемых пользователем по отдельному интерфейсу со специальных внешних накопителей (электронная карточка ридера, например);

10) применения в АС специального защитного экрана, обеспечивающего защиту от НСД самого АС (при необходимости);

11) включения в состав АС аппаратного расширения BIOS ПК (64Кбайт), позволяющего контролировать (до загрузки ОС) целостность ОС и прикладного ПО (физически расположенного на жестком диске ПК, например).

Повышение производительности криптографических операций рассматривается только в контексте повышения уровня защиты информации и осуществляется за счёт:

- применения в качестве ядра в АС максимально адаптированных для реализации большинства криптографических алгоритмов\операций (например, RC6) современных высокопроизводительных микропроцессоров (сигнальных процессоров DSP) на основе RISC архитектуры;
- применения «оперативно загружаемой схемотехники» аппаратных ускорителей (необходимых в ряде случаев), которые на аппаратном уровне реализуют отдельные элементы криптографических алгоритмов (например, таблицу подстановок в ГОСТ-28147) или полностью криптографические алгоритмы (например, DES) и которые не совсем оптимально «ложатся» на ядро АС (микропроцессор) с точки зрения временных затрат на их исполнение;
- применения в перспективе (в отдельных обоснованных случаях) многопроцессорных структур (2-6 процессоров) на базе одного унифицированного микропроцессора.

Кроме того, основные принципы построения АС защиты информации предусматривают:

- «гибкую» адаптацию к требованиям заказчика;
- достаточно оперативную замену криптографических алгоритмов и/или ключей (при необходимости, например, при выявлении и парировании возможных информационных атак);
- функциональную универсальность АС;
- полную самотестируемость АС.

Данные свойства АС обеспечиваются за счёт:

- универсальности АС;

- универсальности системного ПО (BIOS), встроенного в АС;
- встроенных в BIOS АС тестов самопроверки.

«Гибкая» адаптация к требованиям заказчика предполагает реализацию широкого круга задач потенциальных заказчиков без изменения «железа» АС за счёт:

- применения в качестве ядра в АС максимально адаптированных для реализации большинства криптографических алгоритмов (операций) современных высокопроизводительных микропроцессоров (сигнальных процессоров DSP) на основе RISC архитектуры;
- применения «оперативно загружаемой схемотехники» аппаратных ускорителей (необходимых в ряде случаев), которые на аппаратном уровне реализуют отдельные элементы криптографических алгоритмов (например, таблицу подстановок в ГОСТ-28147-89) или полностью криптографические алгоритмы (например, DES);
- применения специальной «загружаемой схемотехники», используемой для реализации отдельных ключей (например, ключа, который используется при инициализации АС или при дешифрации шифрованных криптографических алгоритмов перед загрузкой в ОЗУ);
- хранения криптографических алгоритмов (исполняемых модулей) в энергонезависимой памяти с возможностью многократной перезаписи;
- достаточно простой адаптации/расширения системного ПО (BIOS), встроенного в АС.

Оперативная замена криптографических алгоритмов и/или ключей осуществляется при необходимости за счёт:

- применения специальной «загружаемой схемотехники», используемой на этапе инсталляции АС для реализации отдельных ключей (например, ключа, который используется при инициализации АС или при дешифрации шифрованных криптографических алгоритмов);
- хранения криптографических алгоритмов (исполняемых модулей) в энергонезависимой памяти с возможностью многократной перезаписи (изменения) на этапе инсталляции АС;
- применения «оперативно загружаемой схемотехники» аппаратных ускорителей (необходимых в ряде случаев).

Функциональная универсальность предполагает возможность использования одного и того же АС без каких либо изменений (доработок) в разных функциональных режимах, например, в режиме рабочей станции (основной режим), или в режиме центра управления и сертификации ключей.

В состав АС входят тесты самопроверки (ТСП), которые:

- обеспечивают полную проверку правильности функционирования АС как на этапе изготовления АС, так и при эксплуатации АС пользователем;
- прошиваются в BIOS АС на этапе изготовления, т. е. являются встроенными в АС;
- выполняются каждый раз после аппаратного (по включению питания) или программного сброса АС.

Кроме того, предусматривается и оперативное тестирование каждой команды (режима функционирования) АС в виде возврата в прикладную программу статуса завершения данной команды (режима функционирования) АС.

Такой подход обеспечивает:

- достижение оптимального соотношения - функциональные возможности/стоимость для широкого круга приложений и заказчиков;
- сокращение сроков модернизации системного ПО АС под конкретные проекты и заказчиков;
- оперативную замену криптографических алгоритмов, секретных ключей и т. п. в случае необходимости (например, при выявлении и парировании компрометации ключей);
- постоянный оперативный контроль работоспособности АС.

II Методы защиты от помех и излучений

Специальные требования накладывают ограничения на конструктивное исполнение АС (топологию печатной платы и т. д.) в части:

- допустимого уровня электромагнитных помех, излучаемых АС;
- помехозащищённости АС;
- защиты от электростатического разряда;
- защиты от внешних электромагнитных полей;
- защиты от электрических перегрузок;
- защиты от тепловых перегрузок (перегрева).

Электростатические разряды происходят из-за накопления заряда на выводах микросхем за счёт трибоэлектрического эффекта при трении. При соприкосновении заряженного объекта с проводящей поверхностью происходит электрический разряд, приводящий к кратковременному потоку большого

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

количества электронов в проводнике. Если при этом происходят необратимые изменения во внутренней структуре микросхемы, она выходит из строя.

Повреждения, вызываемые электростатическими разрядами:

- разрыв тонких оксидных плёнок в полупроводниковых устройствах как следствие пробоя диэлектрика;
- плавление проводников и областей металлизации как следствие перегрева при воздействии высокого напряжения;
- запирание КМОП-устройств вследствие возникновения паразитных p-n-p-n структур;
- ухудшение параметров или скрытые дефекты в структуре компонентов, не приводящие к немедленному выходу устройства из строя, но делающие работу системы неустойчивой и провоцирующие эксплуатационные отказы в жёстких условиях;
- наведение мощных электрических полей, приводящих к возникновению помех и сбоев в работе расположенных рядом электронных устройств.

Некоторые меры защиты оборудования от электростатических разрядов разработчики закладывают уже на этапе проектирования электронных схем. Сюда входят: введение специальных защитных устройств в наиболее критические точки схемы; оптимизация проекта печатной платы с целью уменьшения длин проводников и предотвращения возникновения паразитных петель, правильный выбор используемой компонентами технологии и экранировка схемы от внешних электрических полей. Для моделирования воздействия разрядов на электронные компоненты и определения реальных порогов устойчивости возможно использование различных моделей электростатических разрядов, в зависимости от назначения конечного оборудования. В число таких моделей входят: модель человеческого тела, наэлектризованного устройства, механическая модель и модель наведённого поля.

Электромагнитные помехи в системе становятся проблемой, когда имеются их источник, среда, передающая или ответвляющая помехи, и чувствительная к ним система. В идеальном случае необходимо устранить все три составляющие. Электромагнитный сигнал от источника помех передаётся на чувствительное устройство благодаря явлениям проводимости и излучения. В первом случае, помехи проникают в устройство через прямой проводящий тракт, во втором случае — через окружающую среду. Наиболее рентабельным способом снизить электромагнитные помехи является правильный подход к проектированию оборудования. Его основные составляющие: выбор правильных схемотехнических решений и соответствующих им компонентов, правильная разводка печатных плат, специальные приёмы заземления и экранировки. Эти меры позволят достичь большего соответствия жёстким стандартам по электромагнитной совместимости.

Рекомендации по устранению проблем, связанных с наличием электромагнитных помех:

- Не следует увлекаться использованием быстродействующих модулей без особой необходимости. Наличие высокой тактовой частоты в быстродействующих устройствах может стать причиной нежелательных излучений и шумов.
- Каждый “плавающий” вывод микросхемы может работать как антенна: излучать или принимать помехи, вызывающие сбои в системе. Во избежание этого рекомендуется все неиспользуемые выводы связывать с общим проводом и шиной питания системы.
- Вместо простых двусторонних плат рекомендуется использовать многослойные платы с внутренними слоями питания и заземления. Дополнительная развязка должна быть выполнена между цепями тактирования и заземления.
- Длина выводов компонентов должна быть минимальна, что позволит уменьшить их паразитную индуктивность. Паразитные индуктивные связи могут стать причиной перекрёстных искажений сигналов в различных цепях, излишних задержек и нежелательных колебаний.
- Необходимо избегать гибких соединений защитных экранов с землёй. При использовании гибкого экранированного кабеля его оплётка должна быть тщательно соединена с общим проводом, в противном случае кабель будет работать как антенна.
- Для защиты чувствительных к разрядам устройств в наиболее критических точках системы рекомендуется ставить специальные подавители помех переходных процессов и токовые ограничители.
- Для ввода всех сигналов в блоки рекомендуется использовать проходные конденсаторы или фильтры.
- Для предотвращения возникновения в проводниках стоячей волны необходимо тщательно выполнять условия согласования импедансов цепей и нагрузок.
- При прокладке кабелей в блоках и разводке проводников на печатных платах необходимо всячески снижать эффекты, связанные с наличием синфазных цепей и индуктивных связей.
- Для снижения антенных эффектов все неиспользуемые, выступающие из плат концы выводов должны быть обрезаны.

- Рядом с каждой микросхемой между выводом питания и общим проводом должны стоять блокировочные конденсаторы.
- Во избежание взаимных помех рекомендуется группировать компоненты на платах в отдельные зоны с учётом рабочих частот, уровней сигналов и уровней потребляемой мощности.
- Печатные проводники должны быть прямыми и предельно короткими. В длинных проводниках начинают проявляться различные паразитные эффекты, на высоких частотах может возникнуть резонанс.
- Следует до минимума сократить площадь петель проводников, для чего рекомендуется использовать внутренние слои питания и заземления, а также специальные оптимальные методы размещения компонентов и трассировки проводников. Наличие петель в цепях питания с большими токами может привести к мощным наводкам на другие расположенные рядом проводники.
- Для обеспечения максимальной развязки и снижения помех рекомендуется прокладывать шины синхронизации на некотором удалении от входных и выходных цепей.
- При прокладке на плате длинных сигнальных проводников между ними полезно размещать заземлённый проводник. Это позволит сократить площадь петли проводника, а значит, и взаимные наводки.
- Во избежание отражений высокочастотных составляющих сигналов не рекомендуется использовать на платах изломы проводников под углом 90°, вместо них лучше применять закругления.
- Во избежание возникновения перекрёстных искажений необходимо тщательно контролировать ширину проводников и зазоры между ними. Рекомендуется также заранее оценить значения паразитных индуктивности и ёмкости, чтобы предсказать вероятность проявления связанных с ними физических эффектов на высоких частотах. Также необходимо учитывать диэлектрические свойства многослойного материала печатной платы.

III Повышение надежности за счет использования щадящих режимов АС

Дополнительного увеличения надёжности АС можно достичь посредством выбора щадящих режимов работы отдельных улов, поскольку подавляющее большинство отказов происходит вследствие электрических и тепловых перегрузок. Разумеется, выбор нового режима работы должен производиться для групп взаимосвязанных компонентов, причём правильный выбор позволит повысить срок службы критических компонентов, по каким-либо причинам избежавших отбраковочных испытаний. В общем случае невозможно оценить все внешние факторы, воздействующие на систему в реальных условиях эксплуатации, поэтому выбор щадящего режима может стать своеобразным буфером против всех неучтённых факторов, в том числе и от электрических и тепловых перегрузок.

Твёрдых правил выбора коэффициента снижения параметров не существует. В основе его принципа лежит степень надёжности конечного оборудования и связанные с этим затраты. Следует также помнить, что наложение неоправданно жёстких требований значительно увеличивает стоимость проекта, поэтому не стоит это делать в АС, не имеющих повышенных требований к надёжности.

В дополнение к общим методам разработчик должен обратить особое внимание на наличие коммутирующих устройств, топологию печатной платы, типы корпусов используемых компонентов и наличие металлических экранов.

На работу электронной схемы влияют технология монтажа компонентов на плате, способ их размещения и соединения проводниками.

Для предотвращения повреждений компонентов токами, возникающими в результате утечки статического электричества с рук монтажника, рекомендуется прокладывать проводники подальше от краёв платы. Следует также отметить, что все самые строгие меры по защите чувствительных к электростатическим разрядам компонентов могут оказаться бессмысленными, если персонал небрежно обращается с платами. Полезно рядом с сигнальными прокладывать защитные проводники, обеспечивающие утечку заряда на землю. Во входных цепях всех чувствительных элементов рекомендуется ставить защитные элементы, например, ограничительные диоды. Для снижения уровня помех и шумов необходимо обеспечить хорошее заземление.

Выбор наиболее рентабельного коэффициента снижения параметров можно производить, исходя из личного опыта, а также опираясь на основные стандарты, особенно военные (таблица 2).

Как и в случае с отдельными компонентами, экранировка системы в целом позволяет значительно снизить вредное воздействие внешних электромагнитных помех. Принцип работы экрана заключается в поглощении или отражении электромагнитных и электростатических полей. На низких частотах магнитное поле поглощается, на высоких — отражается. Отражение на высоких частотах объясняется несоответствием между низким импедансом металла и высоким импедансом волны.

Для защиты от низкочастотных электрических полей рекомендуется использовать экраны из немагнитных материалов, например, алюминия или меди, так как они лучше отражают нежелательные поля.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Таблица 2

Компонент	Тип	Параметр	Коэффициент	Комментарии
Конденсаторы	Пластмассовые диэлектрические	Напряжение	0,75	
	Керамические		0,75	
	Танталовые электролитические (с сухим электролитом)		0,6	Если эффективный импеданс цепи составляет более 3 Ом/В
			0,4	Если эффективный импеданс составляет менее 3 Ом/В
	Танталовые электролитические (с жидким электролитом)		0,75	
	Слюдяные		0,75	
	Алюминиевые электролитические		0,8	
	Все типы	Рабочая температура	20 °С ниже максимальной	
Диоды	Все типы, включая детектирующие и опорные, стабилитроны, ограничители, диоды Шоттки и светодиоды	Температура перехода	0,75	Выбор рабочей точки должен отразиться на снижении температуры перехода
		Обратное напряжение смещения	0,9	
Транзисторы	Биполярные, полевые и МОП	Рассеиваемая мощность	0,75	Выбор рабочей точки должен отразиться на снижении температуры перехода
		Рабочее напряжение	0,8	
		Рабочий ток	0,8	
		Температура перехода	0,8	
Микросхемы	Цифровые	Напряжение питания	В допустимых пределах	
		Температура перехода	100 °С для пластмассовых корпусов	
			110 °С - для герметичных	
		Быстродействие	0,75	
		Входное напряжение	В допустимых пределах	
		Выходной ток	0,8	

Материалы с высокой магнитной проницаемостью, такие как железо, железоникелевые сплавы, мю-металлы и пермаллой, используются для защиты от низкочастотных магнитных полей. Магнитная проницаемость этих материалов снижается с ростом частоты, поэтому экраны из них на высоких частотах не эффективны. Однако, в этом случае хорошо работают экраны из меди и алюминия, так как они отражают падающую волну (из-за разницы импедансов среды и экрана). Материалы с высокой проводимостью, такие как медь или алюминий, являются полезными для экранировки от электрических полей, но для низкочастотных магнитных полей они неэффективны.

Важно обеспечить сплошной экран вокруг защищаемой системы. Для устранения утечек поля, все отверстия в экране должны иметь диаметр, не превышающий l/20 минимальной длины волны сигналов. Другими словами, не должно быть отверстий, работающих как щелевые антенны. Неиспользуемые разъёмы также могут работать как антенны, поэтому их необходимо закрывать поглощающим материалом. Все

изолирующие элементы должны иметь достаточную электрическую прочность диэлектрика, чтобы избежать пробоя под воздействием высокого электрического поля. Установка соединителей внутри углублений помогает избегать случайного контакта с объектами, заряженными статическим электричеством. Все кабели, используемые для введения сигналов внутрь экранированного корпуса, должны быть экранированными, а их оплетка должна иметь качественный круговой контакт с корпусом, что позволит избежать появления антенных эффектов.

Для длительного хранения уже собранных плат рекомендуется использовать прозрачные пластиковые пакеты с металлизированным покрытием, имеющие высокую стойкость к воздействию температуры и влажности. Высокая температура является одним из вредных факторов, воздействующих на все без исключения типы компонентов электронной схемы. Для предотвращения отказов компонентов из-за чрезмерного нагрева тепловой анализ проекта должен быть выполнен так же тщательно, как и анализ электрических схем. Предельная температура перехода для полупроводниковых устройств общего назначения составляет около 150 °С. Чем ниже рабочая температура перехода, тем выше надёжность устройства. Дополнительными источниками тепла могут быть электрические перегрузки и ряд других факторов, например, процесс пайки или близость к нагревающимся элементам, поэтому разработчик должен полностью оценить тепловое поведение системы до начала производства. На тепловую нагрузку электронных устройств большое влияние оказывает температура окружающей среды. Ситуация ухудшается в области высоких температур, а значит, при моделировании необходимо оценивать весь диапазон температур в реальных условиях эксплуатации.

Таким образом подавляющее большинство механизмов отказов является зависимым от температуры. Косвенными причинами тепловых повреждений являются электрические перегрузки и электростатические разряды, вызывающие перегорание или плавление проводников, а также карбонизация пластиковых инкапсулирующих материалов. Для предотвращения таких повреждений необходимо эксплуатировать устройство вблизи его рабочей температуры и соответствующим образом защищать от воздействия статического электричества, электромагнитных помех и тепловых перегрузок. Последние могут стать причиной термической усталости материалов, тепловых уходов параметров, появления точек перегрева и некоторых других форм тепловых повреждений, в конечном счёте приводящих к полному или частичному отказу оборудования.

Тепловой анализ проекта электронной схемы или системы является неотъемлемым этапом проектирования. Все тепловые проблемы должны быть рассмотрены на начальном этапе, пока стоимость их решения минимальна. Если отказ, связанный с тепловой перегрузкой компонента, идентифицируется на заключительных этапах работы над проектом, затраты на исправления выявленных ошибок могут оказаться весьма значительными. Необходимо выбирать компоненты, соответствующие требованиям разработки и заданным условиям эксплуатации; использовать элементы с высокой надёжностью, проверенной и подтверждённой в ходе специальных испытаний. Полупроводниковые устройства более надёжны при пониженных температурах переходов, поэтому рекомендуется выбирать их рабочие точки вдали от предельных значений параметров. Необходимо убедиться, что при использовании оборудования в самых жёстких рабочих условиях температуры переходов не превышают определённые границы.

Воздействие тепловых ударов можно использовать для оценки надёжности и отбраковки электронных компонентов и АС. Такие ускоренные испытания называются термоциклированием. Они позволяют быстро определить срок службы изделия без больших материальных и временных затрат. Испытания проходят с использованием максимально допустимых уровней сигналов. В случае полупроводниковых устройств термоциклирование в комбинации с рядом других воздействующих факторов позволяет значительно сократить длительность испытаний, направленных на выяснение скрытых дефектов. Данные, полученные в ходе таких испытаний, могут быть использованы для оценки надёжности устройств при работе в нормальных условиях эксплуатации. При ускоренных испытаниях максимальные воздействующие температуры могут колебаться в пределах от +75 до +225 °С, а влажность – в пределах от 50 до 90%, в зависимости от исполнения устройств и природы выявляемых дефектов.

Главная цель любых испытаний заключается в том, чтобы ускорить механизмы проявления отказов и выявить слабые изделия со скрытыми производственными дефектами, то есть спровоцировать случаи ранних отказов.

Для высоконадёжного оборудования необходимо использовать два уровня испытаний. На первом уровне тестированию подвергаются отдельные компоненты, на втором – система (АС) в целом в условиях, максимально приближенных к реальным условиям эксплуатации.

При ускоренных испытаниях компонент подвергается высоким уровням воздействия в сжатые временные отрезки, что значительно снижает стоимость проведения испытаний и сокращает время, необходимое для оценки надёжности. В состав таких испытаний входит термоциклирование, воздействие повышенной влажности, тепловые удары и выжигание дефектов высокой температурой. Стандартной комбинацией

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

температуры и влажности является 85 °С и 85%. Она позволяет выявить большинство скрытых дефектов, проявляющихся на ранней стадии эксплуатации, а также спровоцировать некоторые отказы в полупроводниковых устройствах. Различные исследования показывают, что компоненты, выдержавшие такого рода испытания, работают намного надёжнее.

При сертификации компонентов для высоконадёжной аппаратуры используют три основных типа испытаний: климатические, физические и электрические [1]. Промышленные стандарты выжигания дефектов в электронных компонентах приведены в документах MIL-STD-883[6], MIL-STD-750 и MIL-STD-S-19500. В таблице 3 сведены воедино различные методы отбраковки компонентов.

Таблица 3

Испытания	Выявляемый дефект
Термоциклирование	Разгерметизация корпуса, трещины в подложке, дефекты соединения кристалл-подложка
Хранение при повышенной температуре	Дефекты контактов и металлизации, доступ влаги, окисление, тепловое старение, размягчение, физические изменения
Высокотемпературное выжигание дефектов	Дефекты поверхности, металлизации и проволочных перемычек
Воздействие влажности	Поглощение влаги, коррозия, химические реакции
Солевой туман	Сопротивление коррозии, моделирование морского климата
Влагостойкость	Сопротивление коррозии, эффекты влажности
Погружение в воду	Разгерметизация корпуса, коррозия металла
Механические удары	Утечка электролита из-за разгерметизации, механические повреждения, изменение электрических характеристик, дефекты поверхности
Вибрация	Незакрепленные детали, усталость материалов, холодные пайки, механические неисправности
Испытания на ударопрочность	Механические напряжения
Стойкость к температуре пайки	Изменение электрических характеристик, термодеструкция, механические нагрузки из-за воздействия тепла
Проверка на герметичность	Дефекты герметичных корпусов
Проверка электрических параметров (после выжигания)	Дефекты поверхности, металлизации и проволочных перемычек, загрязнение ионами
Проверка электрических параметров (после выжигания)	Изменения электрических характеристик
Постоянное ускорение	Трещины в подложке, дефекты перемычек, плохая адгезия
Тепловой удар	Разгерметизация и термомеханические разрушения конструктивных элементов

На практике для обеспечения высокого качества изготовления АС (с целью выявления возможных отказов на ранних стадиях) в условиях мелкосерийного (серийного) производства необходимо на этапе производства проведение следующих испытаний:

- термоциклирование (без подачи питания на АС);
- электротермотренировка (с подачей питания на АС);
- вибрация АС;
- функционирование в нормальных условиях (тестовые проверки АС, включая проверку электрических и временных параметров);
- функционирование в климатических условиях (тестовые проверки АС при повышенной и пониженной температурах, с плавным изменением температуры);
- специальные (проверка защиты АС от НСД).

Применение всех перечисленных выше методов защиты и отбраковочных испытаний требует специального технологического оборудования, увеличивает сроки производства, регулировки (тестирования) и сдачи АС и, как следствие, требует достаточно больших материальных затрат, что естественно сказывается на конечной стоимости АС защиты информации. Поэтому, исходя из реальных условий эксплуатации, стоимости АС, требований по надёжности, защиты от НСД и других требований заказчика, необходимо выбирать оптимальный вариант методов обеспечения надёжности, применяемых при разработке АС и отбраковочных испытаниях, используемых на этапе производства АС. По результатам эксплуатации выбранная таким образом программа обеспечения качества АС может изменяться (при необходимости – схемотехника АС дорабатываться, производственные испытания – расширяться).

В технически обоснованных случаях возможно повышение надёжности АС за счёт “горячего” резервирования (дублирования/троирования) АС. При этом возможны два варианта реализации резервирования:

- установка 2-х (дублирование)/3-х (троирование) одноканальных плат АС в соответствующие свободные слоты шины ISA или PCI персонального компьютера;
- разработка специального конструктива АС со встроенными 2-мя/3-мя каналами резервирования.

В первом случае процедура функционирования такой резервированной системы заключается в последовательном взаимодействии прикладного ПО с каждым из дублированных /троированных каналов (плат) АС. Достоверная информация в этом случае определяется следующим образом:

- по статусу завершения каждого канала резервирования (в дублированной системе сначала прикладное ПО читает статус завершения режима основного канала и если команда исполнилась правильно – работает с основным каналом, если нет – работает с резервным каналом);
- алгоритмически, путём усреднения по “2 из 3“ считанной последовательно из каждого канала резервирования информации.

Во втором случае возможен как выше описанный вариант взаимодействия прикладного ПО с каналами резервирования (каждый встроенный в АС канал резервирования имеет свою адресацию в едином адресном пространстве АС), так и вариант, когда механизм резервирования реализован аппаратно в АС и “прозрачен” для прикладного ПО. Второй вариант более сложный с точки зрения технической реализации (учитывая ограниченные габаритные размеры платы АС, ограничения по рассеиваемой мощности и т. п.) и как следствие – более дорогой по стоимости.

Недостатком в обоих случаях является как правило не резервированный ПК, в который устанавливается АС.

IV Характеристика АС серии “Гряда”

Приведенные выше принципы и методы повышения уровня защиты информации (защиты от НСД), повышения производительности криптографических операций, а также методы обеспечения надёжности АС накладывают соответствующие требования на структуру АС и в рамках последней на:

- ядро АС (микропроцессор/сигнальный процессор);
- энергонезависимую память;
- аппаратный ускоритель;
- внешние интерфейсы АС;
- конструктивное исполнение АС;
- системное и прикладное ПО АС;
- защитный экран (при необходимости);
- выбор элементной базы для реализации АС.

Укрупненная структурная схема АС представлена на рис. 1.

Требования к микропроцессору (сигнальному процессору):

- архитектура – RISC + Harvard Architecture (не менее);
- рабочая частота – не менее 40 МГц;
- встроенные: умножитель, баррельный сдвигатель, регистры общего назначения (РОНы), КЭШ память (Cache memory) команд, ОЗУ(RAM), высокоскоростные каналы DMA;
- объём встроенного ОЗУ – не менее 64 Кбайта;
- разрядность арифметико-логического устройства, умножителя, сдвигателя – не менее 32 разрядов;
- время выполнения команды – не более 25 нс;
- аппаратная и программная поддержка многопроцессорных структур (от 2 до 6 процессоров);
- аппаратная и программная поддержка оверлеев.

Применение специализированных криптографических процессоров в настоящее время проблематично по следующим причинам:

- недостаточно высокие технические характеристики: производительность, объём встроенного ОЗУ (криптографический микроконтроллер DS5002FP, криптографический модуль DS2252T фирмы Dallas Semiconductor; криптографические микроконтроллеры MCS-51- AT89SC1616A,248A[7] и AVR – AT90SC4848C [8] фирмы Atmel);
- проблемы с приобретением: наличие, стоимость, лицензия, разрешение на покупку (криптопроцессор ADSP 2141 SafeNet DSP (ADSP-2141L) [9] фирмы Analog Devices и IRE);
- необходимость лазерной «прошивки» защищённого ядра криптосистемы непосредственно на фирме-изготовителе (ADSP-2141L [9] – совместный проект фирм IRE и Analog Devices Inc).

Подобным образом дело обстоит и с модулями АС защиты информации разработки фирм ближнего и дальнего зарубежья:

- «ГРИМ» [10] разработки НПЦ «ЭЛиПС», РОССИЯ и «КРИПТОН» фирмы «Анкад», РОССИЯ - недостаточные высокие технические характеристики;
- SafeNet/CryptPCI Card [11] на базе ADSP-2141L фирм Analog Devices и IRE - проблемы с приобретением, необходимость лазерной «прошивки» ADSP-2141L.

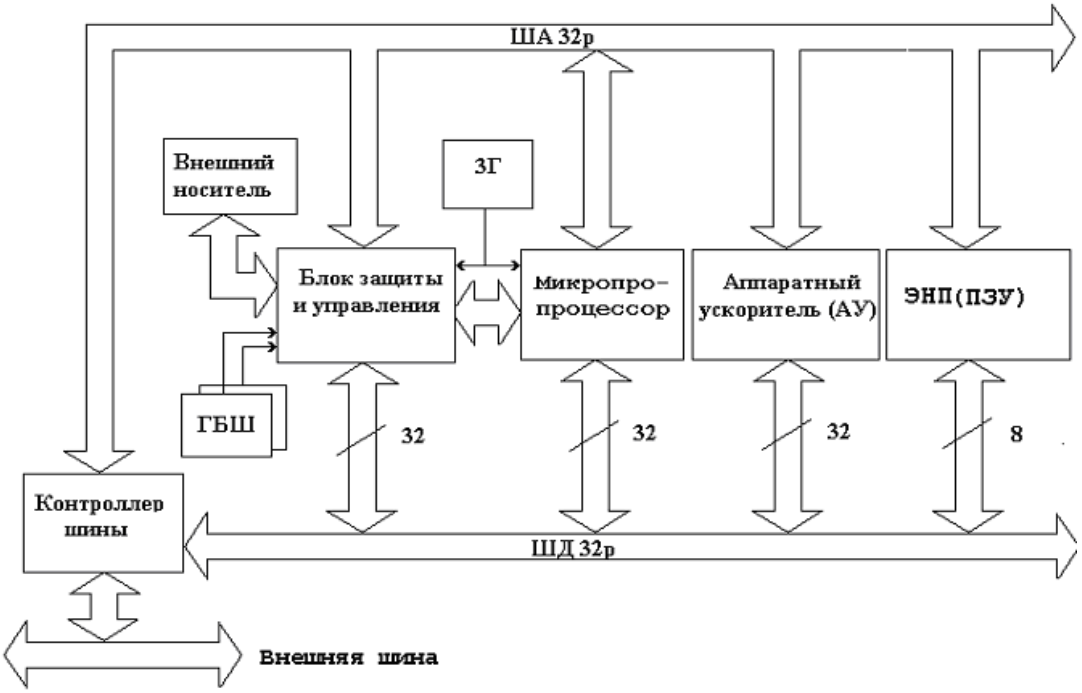

Рисунок 1 – Структурная схема устройств «Гряда-11» и «Гряда-31»

Требования к ЭНП:

- объём накопителя не менее 1Мбайта (с учётом размещения: BIOS, тестов самопроверки, расширения BIOS ПК и шифрованных криптографических алгоритмов);
- разрядность шины данных 8, 16 разрядов;
- цикл чтения не более 120 нс;
- количество циклов стирание/запись не менее 1000000.

Аппаратный ускоритель (если имеется необходимость в таковом) целесообразно реализовать на БИС FPGA типа FLEX (терминология Intel, Altera), что обеспечивает:

- возможность размещения на кристалле достаточно большого объёма аппаратных средств, требуемых для реализации того или иного криптографического алгоритма (или отдельных его частей) при сравнительно небольшой стоимости и малых размерах корпуса данных БИС;
- «динамическую загрузку» схемотехники аппаратного ускорителя каждый раз при подаче питания на АС (в не запитанном АС БИС аппаратного ускорителя «пустой»), что повышает общую защиту АС от НСД;
- возможность размещения достаточно сложной, а значит, «объёмной» схемотехники на ограниченном по геометрическим размерам конструктиве;
- возможность сопряжения схемотехники с современными высокоскоростными микропроцессорами (сигнальными процессорами);
- производительность операций кодирования и декодирования данных по алгоритмам: ГОСТ 28147-89 – 22 Мбит/сек , DES – 48 Мбит/сек, TDES – 16 Мбит/сек (в перспективе возможно увеличение производительности по DES – до 200 Мбит/сек).

Обеспечение принципа минимально возможного взаимодействия прикладного ПО и ОС ПК с АС выдвигает следующие требования к системной шине, обеспечивающей связь АС с ПК:

- разрядность шины данных – не менее 32 разряда;
- обмен блоками со скоростью – не менее 132 Мб/сек;
- обмен с квитированием;
- шина должна быть современной и распространённой в ПК.

Наиболее полно отвечает данным требованиям самая распространённая в настоящее время шина PCI-

32/33 МГц.

Контроллер интерфейса шины PCI-32/33 МГц реализует протокол шины PCI-32 с частотой 33 МГц в соответствии с спецификацией PCI V2.1 PCISIG (target) и обеспечивает режимы:

- записи/чтения 32р слов со стороны ПК по командам IN/OUT и MOV в темпе шины;
- режим прерывания по инициативе АС.

С учётом требований по защите от НСД, а также обеспечения принципа минимально возможного взаимодействия прикладного ПО и ОС ПК с АС конструктивно целесообразно выполнить АС в виде платы для ПК IBM/PC с системной шиной PCI-32/33 МГц, занимающей одно стандартное посадочное место в ПК.

Конструктивно плата представляет собой многослойную печатную плату размером не более 110 х 190 мм с ламельным разъёмом по длинной стороне платы для шины PCI-32/33 МГц.

Для реализации связи с ридером возможны два варианта:

- размещения внешнего разъёма (DB9M под RS-232C, series “A”/”B” connectors под USB) на короткой стороне платы – если ридер (под Smard Card, MiniKey, Touch Memory) расположен вне ПК;
- размещение на плате мини разъема для связи с ридером по отдельному интерфейсу – если ридер расположен внутри ПК;

В последнем случае интерфейс платы с ридером целесообразно реализовать на базе упрощенного RS-232C (три линии связи: принимаемые данные, передаваемые данные и “общий”) по чисто программному протоколу.

Поверхность платы должна быть покрыта защитным покрытием, на плате нанесена соответствующая маркировка, на ламель нанесено покрытие из золота.

Для устранения возможности НСД дополнительно на плату (со стороны расположения электронных компонентов) устанавливается специальный защитный экран. Экран устанавливается на этапе инсталляции платы. Нарушение целостности защитного экрана при эксплуатации пользователем приводит к “зависанию” ПК или получению статуса завершения “Недействительная команда” при первом же обращении со стороны ПК к плате. После чего плата должна повторно пройти этап инсталляции на специальном технологическом стенде.

Эксплуатация опытных образцов платы “ГРЯДА-31” показала следующие особенности применения АС защиты информации:

1. BIOS ПК должен поддерживать технологию Plug&Play, а именно спецификации:
   - BIOS Boot Specification ver. 1.00;
   - Plug&Play BIOS Specification ver. 1.0A;
   - PCI Specification V2.1 PCISIG.
2. Учитывая реальное положение дел по поддержке изготовленными до 1997 года ПК указанных выше спецификаций, ПК должен удовлетворять следующим требованиям:
   - Версия BIOS ПК должна иметь год разработки не ранее 1997 года (например, Award Modular BIOS 4.51G Copyright© 1984-1997);
   - ПК (а точнее, материнская плата) должен иметь год изготовления не ранее 1997 года.
3. Для взаимодействия прикладного ПО с АС необходима разработка специального драйвера под операционные системы (ОС) DOS, Windows 95, Windows 98, Windows NT.
4. Для обеспечения режима многозадачности ОС, данный драйвер должен иметь “модульную” структуру, т. е. “разбит” на ряд функций, которые последовательно вызываются прикладным ПО.

Заключение

1. Для обеспечения эффективности проекта непосредственно перед началом разработки АС защиты информации должны быть чётко определены:
   - назначение данных АС защиты информации;
   - реализуемые АС функции;
   - требования по защите информации (криптографии);
   - требования по производительности криптографических преобразований;
   - требования по защите от НСД (инженерной криптографии);
   - реальные условия эксплуатации;
   - специальные требования;
   - требования к программному обеспечению.
2. На основании п. 1. необходимо сформировать требования к АС в части:
   - выбора элементной базы (номенклатура и надёжность);
   - выбора схемно-технических решений(CPU, тактовая частота и т.д.);
   - выбора типа печатной платы (ДПП, МПП с металлизированными отверстиями);

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

- топологии (разводки) печатной платы;
- конструкции АС (защитный экран, защита от статического электричества и т. д.).

3. Для выявления ранних отказов необходимо использовать специальные методы отбраковки и «выжигания» дефектов. Используемые компоненты должны иметь должное качество и высокую надёжность.
4. При выявлении непредвиденных воздействий АС необходимо к ним адаптировать. Реальные условия эксплуатации оборудования на местах могут значительно отличаться от лабораторных. На компоненты могут воздействовать электромагнитные помехи, электростатические разряды, высокая температура и вибрация. Рабочие точки компонентов по току и напряжению, температуры переходов и рассеваемая мощность выбираются оптимально для стойкости к перегрузкам.
5. Избыточность системы должна определяться требованиями надёжности и стоимостью оборудования.
6. Помимо аппаратной надёжности используемое в системе программное обеспечение должно быть построено таким образом, чтобы возможные сбои в работе оборудования обрабатывались безопасно и не приводили к отказам всей системы.
7. Требуемый уровень надёжности необходимо обеспечивать на уровне проекта. Дополнительные меры, применяемые во время производства, хранения, тестирования, системной интеграции и эксплуатации, позволят улучшить суммарную надёжность оборудования АС.
8. Необходимо применять методы контроля качества к АС в целом. Это позволит гарантировать высокую надёжность АС на всех уровнях.

Перечисленные принципы построения АС защиты информации позволяют, с одной стороны, обеспечить оптимальные соотношения функциональные возможности/производительность криптографических преобразований/защита от СНД/стоимость, а, с другой стороны, уже на этапе разработки в максимальной степени реализовать в АС защиты информации специальные требования: допустимый уровень излучаемых АС электромагнитных помех, помехоустойчивость, защита от электростатического разряда, внешних электромагнитных помех, электрических и тепловых перегрузок.

Опытная эксплуатация АС защиты информации и дополнительные испытания (проверка электромагнитной совместимости, электрических и тепловых режимов, проверка защитных экранов и т. д.) должны подтвердить правильность выбранных решений или определить необходимые доработки АС (схемно-технические, конструктивные и т. д.).

Литература: 1. MIL-HDBK-202: Test Methods for Electronic and Electrical Component Parts. 2. Boxleitner, Warren, Electrostatic Discharge and Electronic Equipment, IEEE Press, New York, 1989. 3. Lakshminarayanan V. What causes semiconductor devices to fail? Test & Measurement World, November 1999, pp. 49–55. 4. Lakshminarayanan V. Basic steps to successful EMC design, RF Design, September 1999, pp. 35–47. 5. Lakshminarayanan V. Minimize ESD-induced failures, Advanced Packaging, August 1999, pp. 36–39. 6. MIL-STD-883E: Test Method Standard for Microcircuits. 7. 8 bit Flash Secure Microcontroller AT89ScxxxxA, Datasheet, Atmel Corp. 8. 8 bit AVR Flash Secure Microcontroller AT90ScxxxxA, Datasheet, Atmel Corp. 9. ADSP-2141L SafeNet DSP, Analog Devices Inc. 10. Бабий О., Володин А., Митько В., Спинко Е. Реализация криптографических алгоритмов на процессорах семейства ADSP 21XX , ChipNews № 1(10) 1997 г. 11. SafeNet/CryptPCI Card, IRE Inc.

УДК 681.3.06

АНАЛИЗ БЕЗОПАСНОСТИ РЕЖИМОВ БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ

Сергей Головашич, Олег Лебедев

Харьковский государственный технический университет радиоэлектроники

Аннотация: **Виконано аналіз основних режимів застосування блокових симетричних шифрів. Визначено переваги та недоліки кожного з режимів, запропоновано засоби усунення виявлених недоліків. Наведено дві схеми режимів потокового шифрування, що задовольняють запропонованим вимогам.**

Summary: **The symmetric block ciphers standard modes of operations analysis is carried out. The advantages and disadvantages of each mode is analysed, the improvement methods are suggested. The schemes of two new modes for stream encryption are proposed. These schemes completely satisfy suggested requirements.**

Ключевые слова: **Блочные симметричные шифры, режимы блочного шифрования, период гаммы шифрующей.**