G. Groesneken, H. E. Maes // IEEE Trans. on El. Dev. 1986. Vol. ED-33, № 7. P. 1028–1042.

3. Сальман, Е. Г. Изучение процессов образования и переноса заряда в слоях двуокиси кремния на кремнии / Е. Г. Сальман, В. Н. Вертопрахов, В. С. Данилович. ЦИОНТ ПИК. Деп. в ВИНИТИ : № 558-76. Новосибирск, 1975.

4. Salman, E. G. Thermally stimulated depolarisation current controlled by surface charge change / E. G. Salman, V. N. Vertoprakhov // Phys. Stat. Sol. 1988. Vol. 1008, № 2. P. 625–630.

G. V. Perov, V. I. Sedinin

INFLUENCE OF MOBILE POSITIVE CHARGE ON ELECTRONIC CONDUCTIVITY OF DIELECTRIC WITH HETEROGENEOUS BLOCKING BORDER

The correlation between size of the positive mobile charge and electronic conductivity of oxide on polycrystalline silicon is established by the experimental method of thermally stimulated polarization and depolarization of MIS-structures. The boundary conditions of the problem for the working model of mobile charge behavior in isolating layers which were generated on a rough semiconductor film, are formulated.

Keywords: mobile charge of dielectrics, heterogeneous blocking border of dielectrics with a semiconductor, oxide on polycrystalline silicon.

УДК 621.391.037.372

К. М. Волощук, Т. А. Чалкин

ПРОТОКОЛ ПРОЗРАЧНОГО ШИФРОВАНИЯ ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО КАНАЛУ «ЗЕМЛЯ–БОРТ»

Описан протокол прозрачного шифрования, разработанный для организации сеансов передачи данных по защищенному каналу связи «земля–борт». Протокол определяет место генерации, тестирования и хранения, процедуры выбора, режимы смены ключевой информации при обработке данных.

Ключевые слова: протокол прозрачного шифрования, канал передачи данных «земля–борт», модуль обработки информации.

Задача данной работы – разработать протокол прозрачного шифрования данных, передаваемых по спутниковому каналу связи «земля–борт» в рамках научно-исследовательской работы (НИР).

Актуальность работы обусловлена следующим. Целостность предназначенных для управления космическим аппаратом (КА) разовых команд (РК), а также конфиденциальность транслируемых по каналу «земля–борт» стратегически важных данных обладают высокой степенью критичности. Чтобы гарантировать заданный уровень обеспечения данных свойств защищенности информации, необходима организация защищенного канала передачи данных «земля–борт».

Для организации защищенного канала передачи данных в систему космической связи устанавливаются аппаратные модули обработки информации (МОИ), выполняющие специальную обработку (спецобработку) данных по заданному алгоритму шифрования в режиме, определенном для обработки логической единицы передаваемых данных (кадра). Данные с выхода соответствующей компьютерной системы центра управления полетами (КС ЦУП) поступают на вход МОИ, где происходит их спецобработка. Зашифрованные данные поступают на вход наземной командно-измерительной станции (КИС), выполняется формирование кадра, модулированный по соответствующему стандарту сигнал конвертируется и передается на наземную приемно-передающую систему (ППС). С ППС ЦУП сигнал транслируется и принимается ППС КА. Затем сигнал поступает в КИС КА, с выхода которой полученные зашифрованные данные передаются в МОИ, расшифровываются и поступают в бортовой компьютер (БК) КА. Передача данных с КА в ЦУП осуществляется аналогичным образом (рис. 1).

Данная криптосистема, обеспечивающая защищенный канал передачи данных «земля–борт», должна отвечать следующим техническим требованиям, обусловленным спецификой канала передачи данных:

1. Шифрование данных должно осуществляться в потоковом режиме с канальной скоростью не менее 32 кбит/с.

2. Автономная работа элементов криптосистемы, установленных на борту КА, в течение всего срока эксплуатации КА.

3. Обработка кадров данных произвольной длины.

4. Устойчивость криптосистемы к современным методам криптоанализа.

5. Криптосистема должна обеспечивать контроль целостности передаваемых данных.

6. Процесс шифрования должен быть прозрачен с точки зрения канала связи.

7. Криптосистема должна обеспечивать заданную эксплуатационную надежность, возможность резервирования МОИ.

При этом МОИ, входящий в состав системы организации защищенного канала «земля–борт» должен обеспечивать аппаратно-программную реализацию:

– зашифрования/расшифрования кадров данных переменной длины (128…1024 бит);

– процесса хранения и периодической смены элементов ключевой информации;

– генерирования сеансовой (текущей) ключевой информации;

– процедур автоматической проверки целостности передаваемых данных.

В соответствии с обозначенными требованиями для криптографической системы и заявленной спецификации МОИ были определены алгоритм шифрования и режим его работы, аппаратная платформа, принципы организации архитектуры и режимы функционирования МОИ [1], условия и процедуры выработки, замены сеансовой и долговременной ключевой информации.

На основании сравнительного анализа современных криптоалгоритмов в качестве основного алгоритма шифрования для защиты информации, передаваемой по каналу «земля–борт», был выбран ГОСТ 28147–89 [2].

Обоснования выбора алгоритма ГОСТ 28147–89 следующие:

1) действующий государственный стандарт РФ по криптографической обработке информации;

2) криптографическая стойкость: неизвестны практически реализуемые и эффективные методы осуществления атак;

3) возможность эффективной программной и аппаратной реализации на различных платформах.

В соответствии с обозначенными требованиями к криптосистеме в качестве используемого в ней режима работы алгоритма ГОСТ 28147–89 выбран режим гаммирования с обратной связью с дополнительной выработкой имитовставки для каждого кадра передаваемых данных [3].

Обоснование выбора режима объясняется следующим:

1. Режим гаммирования с обратной связью обеспечивает:

а) различие блоков шифрованных данных для одинаковых блоков исходных данных, что затрудняет криптоанализ;

б) возможность шифрования массива данных произвольного размера;

в) зацепление блоков, а следовательно, изменения в шифрованных данных распространяются на все последующие блоки исходных данных при расшифровании.

2. Режим выработки имитовставки обеспечивает:

а) возможность проверки целостности блока данных при помощи процедуры контроля имитовставки;

б) задание требуемого уровня надежности проверки целостности посредством выбора приемлемого значения размера имитовставки.

Используется двухуровневая система ключевой информации [4]:

1. Ключи шифрования:

– долговременные ключи;

– сеансовые ключи.

2. Таблицы замен.

Ключ представляет собой массив из восьми 32-битных элементов данных. Таким образом, размер ключа составляет $32 \cdot 8 = 256$ бит (32 байта) [2].

Долговременные ключи генерируются на этапе разработки криптосистемы с использованием алгоритма формирования псевдослучайной последовательности BBS (Блюма–Блюма–Шуба), проходят тестирование на отсутствие статистических закономерностей, перед началом эксплуатации записываются в постоянно запоминающееся устройство (ПЗУ) МОИ (каждому долговременному ключу соответствует уникальный указатель набора ключей), используются на протяжении всего периода эксплуатации КА. Рекомендуемая частота смены долговременных ключей – 1 раз в месяц.

Сеансовые ключи генерируются перед началом каждого сеанса шифрования и используются для шифрования только текущего кадра. Представляют собой 256-битные отрезки гаммы шифра, полученной с использованием долговременного ключа.

Таблица замен является матрицей 8×16, содержащей 4-битовые элементы. Строки таблицы замен (всего 8 строк) называются узлами замен (S-блоками). Таким образом, общий объем таблицы замен равен 8 узлов × 16 элементов / узел × 4 бита / элемент = 512 бит (64 байта) [2]. Таблицы замен вырабатываются на этапе разработки, подвергаются тестированию по заданным критериям. Конкретный набор таблиц замен определяется заказчиком перед началом эксплуатации системы и записывается в ПЗУ МОИ (каждой долговременной таблице соответствует уникальный указатель набора таблиц). Рекомендуемая частота замены таблиц замен – 1 раз в год.

Предусмотрено два режима управления заменой используемой ключевой информации (долговременных ключей и таблиц замен):

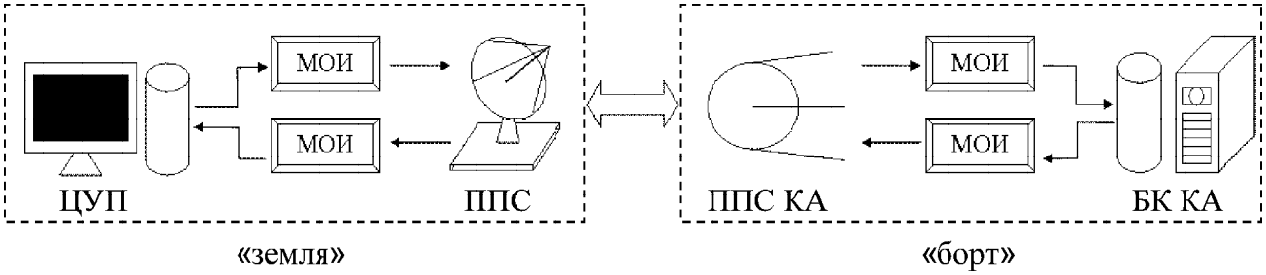

Рис. 1. Место МОИ в канале передачи данных «земля–борт»

1. Посредством директивы ЦУП и синхронной трансляции специальной команды из ЦУП на МОИ, установленный в составе наземного криптографического комплекса, и МОИ КА.

2. В автоматическом режиме в соответствии со значением счетчика объема данных, зашифрованных с использованием текущего набора долговременной ключевой информации.

В специальной команде указываются выбранные указатели набора ключей и таблиц, записанных в ПЗУ МОИ ЦУП и МОИ КА. Переключение на выбранные пары происходит синхронно в МОИ ЦУП и МОИ КА. В случае успешного выполнения директивы, команда подтверждения переключения поступает от обозначенных МОИ в ЦУП.

В обоих вариантах переключение на заданную пару происходит по специальной команде, поступающей в МОИ. В первом случае инициатором трансляции команды на микромодули является ЦУП, во втором случае – наземная криптосистема при превышении установленного порогового значения уровня объема зашифрованных данных, при этом, чем больший объем информации за определенный промежуток времени будет подвергнут шифрованию, тем чаще будет происходить переключение криптографической системы на не задействованную ранее пару долговременной ключевой информации («ключ–таблица замен»), и наоборот.

В качестве аппаратной платформы МОИ была выбрана сверхбольшая интегральная схема (СБИС) типа «радиационно-стойкая программируемая логическая интегральная схема» ПЛИС (FPGA – field-programmable gate array) на базовых матричных кристаллах (БМК) (ASIC – application specific integrated circuit) производства фирмы Actel [5].

Логическая структура МОИ состоит из двух вычислительных узлов – процессора обработки информации (ПОИ) и генератора специальной информации (ГСИ).

В состав МОИ входят 2 модуля оперативного запоминающего устройства (ОЗУ) по 4 кбайта и модуль ПЗУ.

Технологический интерфейс взаимодействия МОИ: USB.

Рабочий интерфейс взаимодействия МОИ с КИС ЦУП и КИС КА: RS-422 [1].

ПОИ выполняет непосредственно процедуры спецобработки поступающих на вход данных (зашрование/расшифрование) [1]. ГСИ используется для выработки специальной информации посредством рекуррентного генератора последовательности чисел (РГПЧ) согласно алгоритму ГОСТ 28147–89.

Модули ОЗУ (по 4 кбайта каждый) используются в качестве входного и выходного буферов соответственно. Модуль ПЗУ предназначен для хранения долговременной ключевой информации (рис. 2).

Предполагается для хранения текущего элемента специнформации длиной 256 бит использовать ячейку памяти МОИ R_current, для работы с имитовставкой – R_imito длиной 32 бит. Начальное заполнение вспомогательных ячеек памяти R_key и R_data в МОИ длиной 64 бита каждая, предназначенных для инициализации процесса выработки гаммы шифра при выработке сеансового ключа и непосредственном шифровании передаваемых по каналу связи данных соответственно, представляет собой предварительно сгенерированную псевдослучайную последовательность. Долговременная ключевая информация записывается в память МОИ перед началом эксплуатации системы. РГПЧ МОИ генерирует блоки данных длиной 64 бит по алгоритму, описанному в стан-

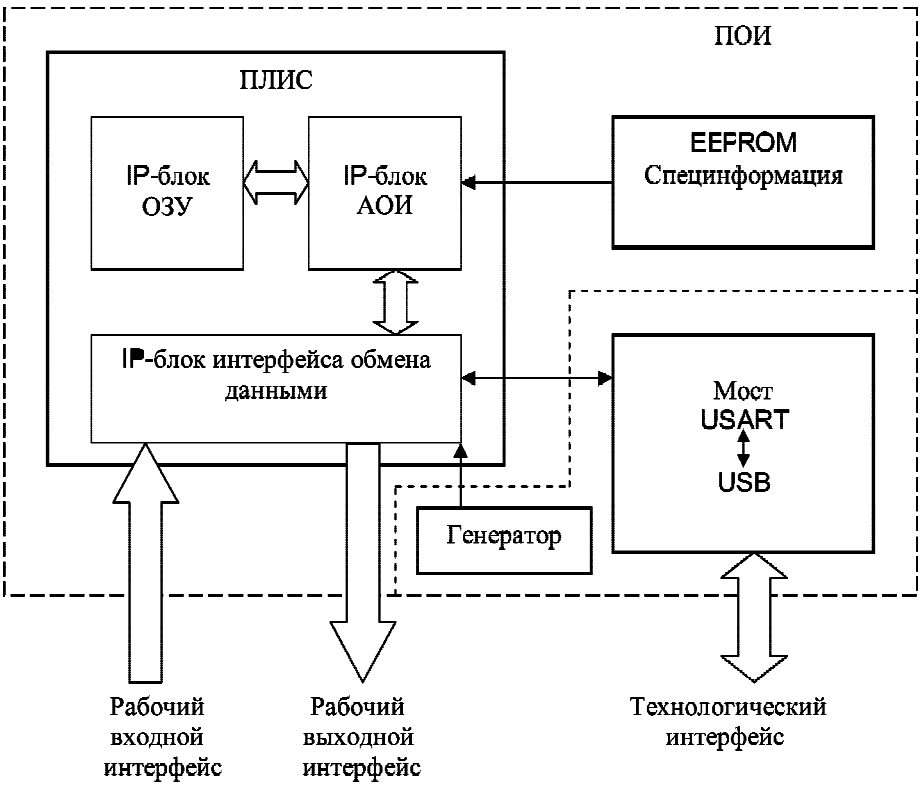

Рис. 2. Функциональная схема МОИ

дарте ГОСТ 28147–89, используется для генерации синхропосылок, хранимых в R_key и R_data, необходимых для спецобработки данных согласно алгоритму ГОСТ 28147-89. Логическая схема МОИ представлена на рис. 3 .

Процедура передачи данных с земли на борт (в обратном направлении передача осуществляется аналогично) осуществляется в следующей последовательности:

1. Кадр данных из ЦУП поступает на вход МОИ. Данные помещаются во входной буфер данных МОИ.

2. Выполняется генерация сеансового ключа (используемого только для зашифрования текущего кадра данных) путем выработки псевдослучайной гаммы по алгоритму ГОСТ 28147–89 в режиме гаммирования с обратной связью [2] при помощи текущего долговременного ключа и текущего набора таблиц замен из запоминающего устройства, при этом 64 инициализирующих бита берутся из R_key. Сгенерированная последовательность из 256 бит сохраняется в R_current для дальнейшего использования при спецобработке данных из входного буфера. Генерация сеансового ключа на данном шаге заключается в последовательном выполнении процессором спецобработки четырех циклов спецобработки данных по алгоритму ГОСТ 28147-89.

3. Для данных, находящихся во входном буфере, вычисляется имитовставка по алгоритму ГОСТ 28147–89 с использованием полученного на предыдущем шаге сеансового ключа из R_current и текущего набора таблиц замен, хранящегося в долговременной памяти МОИ. Младшие 32 бита полученной имитовставки сохраняются в R_imito.

4. Данные для передачи, находящиеся во входном буфере, подвергаются зашифрованию по алгоритму ГОСТ 28147–89 в режиме гаммирования с обратной связью с использованием сеансового ключа из R_current и текущего набора таблиц замен. Синхропосылка для шифрования берется из R_data. Данные на выходе процессора, выполняющего спецобработку, помещаются в выходной буфер МОИ.

5. Информационная часть кадра формируется следующим образом: первые 64 бит занимает содержимое R_key, затем – 64 бит из R_data, после чего следуют данные, полученные на предыдущем шаге из выходного буфера, и последние 32 бит занимает содержимое R_imito (рис. 4). Сформированная таким образом в выходном буфере последовательность передается в КИС и ППС, где к ней добавляется заголовок кадра, канальная синхропосылка, дополнительная служебная информация, после чего кадр транслируется на борт КА.

6. При помощи РГПЧ в МОИ на земле осуществляется генерация очередной 64-битовой последовательности для данных из R_key и R_data. Эти последовательности записываются в эти же R_key и R_data (таким образом, в эти регистры помещаются следующие за текущими числа из псевдослучайной последовательности, генерируемой РГПЧ). Они будут использоваться как инициализирующие при генерации сеансового ключа и непосредственно при зашифровании информации соответственно, для следующим за текущим кадра данных, поступившего в МОИ.

7. На борту переданный с земли кадр принимается, обрабатывается в ППС и КИС, после чего его информационная часть передается на вход МОИ. Первые 64 бита полученных данных помещаются в R_key, последующие 64 бит – в R_data, а последние 32 бита – в R_imito МОИ. Оставшиеся данные помещаются во входной буфер МОИ.

8. Выполняется генерация сеансового ключа и запись его в R_current аналогично п. 2. Идентичность сеансовых элементов специнформации на земле и на борту, необходимая для обратимости шифрования, обеспечивается, таким образом, путем передачи вместе с зашифрованными данными инициализирующего блока, использованного для генерации сеансового элемента специнформации (т. е. данных из R_key), и синхронной смены долговременных ключей и наборов таблиц замен в МОИ, установленных на земле и на борту КА.

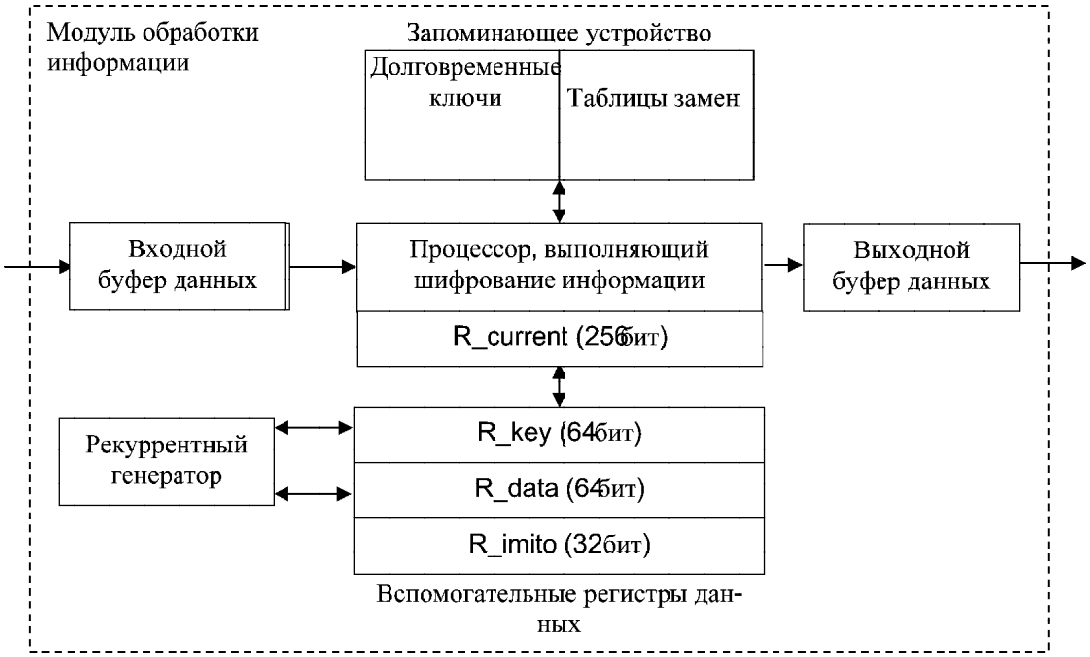

Рис. 3. Логическая схема МОИ

9. Данные из входного буфера подвергаются расшифрованию по алгоритму ГОСТ 28147–89 в режиме гаммирования с обратной связью процессором спецобработки с использованием сеансового ключа из R_current, и текущего набора таблиц замен из долговременного запоминающего устройства. Синхропосылка для расшифрования считывается из R_data. Расшифрованные данные помещаются в выходной буфер.

10. Для массива данных в выходном буфере выполняется вычисление имитовставки по алгоритму ГОСТ 28147–89 с использованием сеансового ключа из R_current и текущего набора таблиц замен, после чего полученное значение имитовставки сравнивается со значением в R_imito. При совпадении значений данные из выходного буфера передаются для обработки в БК КА, при расхождении данные в выходном буфере считаются ошибочно принятыми и на землю передается команда, сигнализирующая об искажении данных кадра.

Вышеизложенный протокол схематично представлен на рис. 5 и 6. Пунктирными соединительными линиями обозначены операции по перемещению данных без обработки, сплошными тонкими линиями – выработка оче-

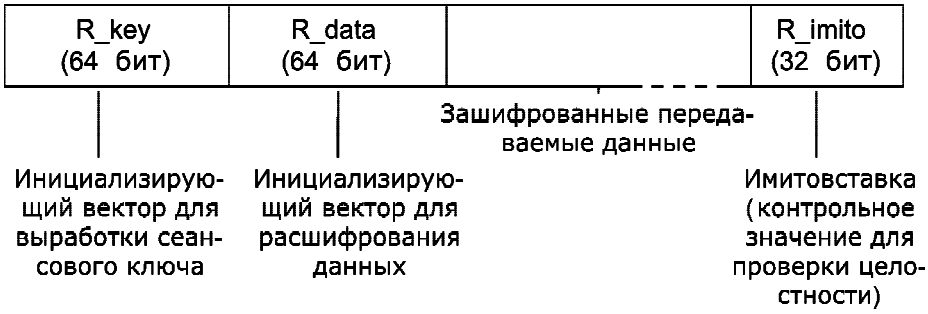

Рис. 4. Структура информационной части кадра

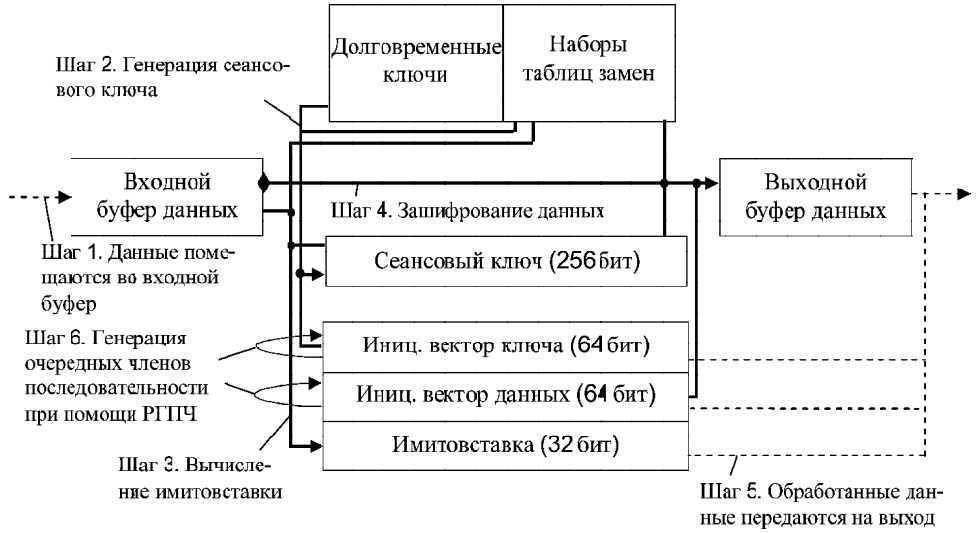

Рис. 5. Процедура зашифрования в МОИ передаваемых данных

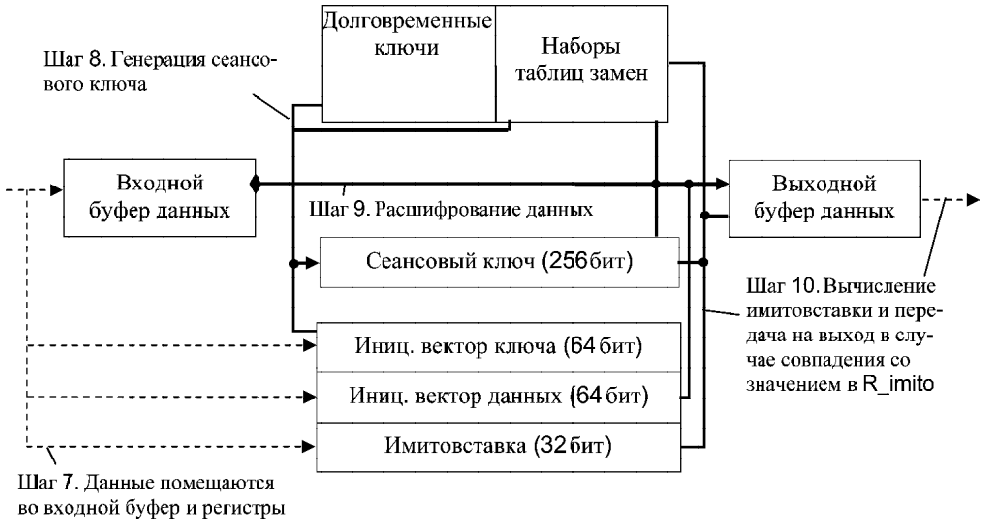

Рис. 6. Процедура расшифрования в МОИ принимаемых данных

редных членов последовательности чисел при помощи РГПЧ, сплошными жирными линиями – перемещение данных с их спецобработкой.

Таким образом, в соответствии с предоставленными исходными данными, проведенным анализом этих данных и выбранной аппаратной платформой реализации был разработан протокол прозрачного шифрования данных для организации сеансов передачи данных по защищенному каналу связи «земля–борт». Данный протокол определяет архитектуру построения МОИ, место генерации, тестирования и хранения, процедуры выбора и режимы смены ключевой информации при обработке передаваемых и принимаемых данных.

Библиографический список

1. Шаранок, А. С. Аппаратная реализация алгоритмов шифрования на элементной базе ПЛИС / А. С. Шаранок // Актуальные проблемы безопасности информационных технологий : сб. науч. ст. ; ред. О. Н. Жданов, В. В. Золотарев, А. В. Шахматов ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2008.

2. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : ИПК Изд-во стандартов, 1996.

3. Винокуров, А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы x86 [Электронный ресурс] / А. Винокуров. Электрон. дан. Режим доступа: http://re-tech.narod.ru/inf/crypto/gost.htm. Загл. с экрана.

4. Столингс, В. Криптография и защита сетей: принципы и практика / В. Столингс. 2-е изд. М. : Изд. дом «Вильямс», 2001.

5. Потехин, Д. С. Разработка систем цифровой обработки сигналов на базе ПЛИС / Д. С. Потехин, И. А. Тарасов // М. : Радио и связь, 2007.

K. M. Voloshchuk, T. A. Chalkin

TRANSPARENT ENCRYPTION PROTOCOL FOR DATA TRANSMITTED VIA «SURFACE-TO-BOARD» CHANNEL

The organization of the Transparent data encryption protocol designed for the data transmission via the secure «surface-to-board» channel is described in this paper. This protocol determines the place of key information generation, testing location, key information selection and change procedures while data-processing operation.

Keywords: transparent data encryption protocol, «surface-to-board» channel, data processing module.

УДК 004.056.53:519.873

Е. С. Семенкин, М. А. Стюгин

ЗАЩИТА ОТ ИССЛЕДОВАНИЯ И ЕЕ ПРИМЕНЕНИЕ В СИСТЕМАХ БЕЗОПАСНОСТИ

Рассматривается информационное взаимодействие нарушителя и защищаемой системы в виде стереотипных схем исследования, предлагается метод снижения эффективности атаки путем искусственного повышения разнообразия атакуемой системы, описывается задача автоматизации проектирования систем безопасности.

Ключевые слова: информационное взаимодействие с нарушителем, стереотипные схемы, снижение риска в системах безопасности.

С давних времен человечество пыталась упростить как свою жизнь, так и способы ее поддержания. Простота – признак гениальности, а порядок – залог успеха. Однако такой подход эффективен до тех пор, пока дело не доходит до серьезных конфликтов, где единственный способ преобладать – это сделать свой уникальный шаг к цели. В таком конфликте каждый исследует своего противника, и чем проще и стереотипнее этот противник, тем он беззащитнее от атак конкурента (нарушителя).

Информационный обмен. Любая активная деятельность сопровождается получением, передачей и анализом информации. Такой информационный обмен происходит всегда. Схематично его можно изобразить следующим образом (рис. 1).

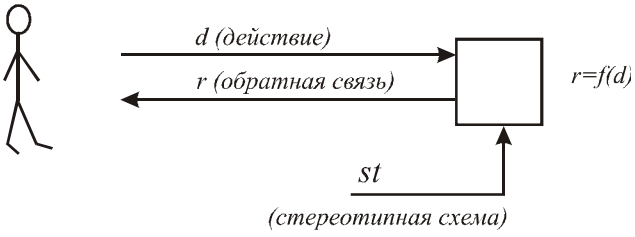

Рис. 1. Схема информационного обмена