АО «Концерн ГРАНИТ»

Россия, 119019, г. Москва, ул. Гоголевский бульвар, д. 31, стр. 2, эт. 2, пом.1
т. +7 495 642 97 42, ф. +7 499 558 15 29
office@granit-concern.ru, granit-concern.ru

Информация, необходимая для эксплуатации экземпляра программного обеспечения специального преобразования информации

Программное обеспечение СПИ

Акционерное общество «Концерн ГРАНИТ»
ОКПО 78089277, ОГРН 1055011347093, ИНН/КПП 5003056699/770401001
р/с 40702810738000014569 в ПАО «Сбербанк России»,
к/с 30101810400000000225, БИК 044525225

Содержание

Введение

Настоящий документ представляет собой сведения о назначении, условиях и порядке выполнения программного обеспечения СПИ.

Перед началом работы рекомендуется внимательно ознакомиться с данным руководством.

Программное обеспечение СПИ, предназначено для обеспечения маскирования и размаскирования данных согласно ГОСТ 34.12-2018.

1 Теоретические сведения

ГОСТ 34.12-2018 описывает два отечественных блочных симметричных шифра «Кузнечик» и «Магма» с длинами блока 128 и 64 бита соответственно и длиной ключа 256 бит, предназначенных для защиты конфиденциальности, целостности и аутентичности информации. Стандарт устанавливает алгоритмы базовых блочных шифров, применяемых в криптографических методах обработки и защиты информации в автоматизированных системах при передаче, хранении и обработки данных. Алгоритмы рассчитаны на программную и аппаратную реализацию и не накладывают ограничений на степень секретности защищенной информации.

ГОСТ 34.12-2018 применяется совместно с нормативными документами, регламентирующими режимы блочного шифрования, в которых задаются режимы простой замены, простой замены с зацеплением, гаммирования, гаммирования с обратной связью по выходу и по шифртексту, а также режимы выработки имитовставки.

В режиме простой замены каждый блок обрабатывается независимо, поэтому одинаковые блоки открытого теста дают одинаковые блоки шифртекста. Режим простой замены с зацеплением связывает каждый блок с предыдущим: перед шифрованием блок складывается с предыдущим шифртекстом, что устраняет повторяющие паттерны, но требует последовательной обработки.

Режим гаммирования превращает блочный шифр в потоковый: шифруется счетчик, получается гамма, которая накладывается на открытый текст, что позволяет шифровать данные произвольной длины. В режимах гаммирования с обратной связью по выходу и шифртексту следующая часть гаммы зависит от предыдущего результата, что усложняет анализ шифра и позволяет работать с произвольной длиной данных.

2 Выполнение программы

Структурная схема работы программного обеспечения специального преобразования информации приведена на рисунке 1. Микроконтроллер МІК32 «Амур» реализует формирование криптографической гаммы по алгоритму ГОСТ 34.12-2018 в режиме гаммирования по счетчику. Выполнение программы начинается с получения 64-битного значения счетчика и передачи его в модуль маскирования. В этом модуле значение счетчика обрабатывается в соответствии с блочным шифром «Магма» с заданным 256-битным ключом, в результате чего вырабатывается блок гаммы до 512 бит, который передается в МКУ для последующей обработки.

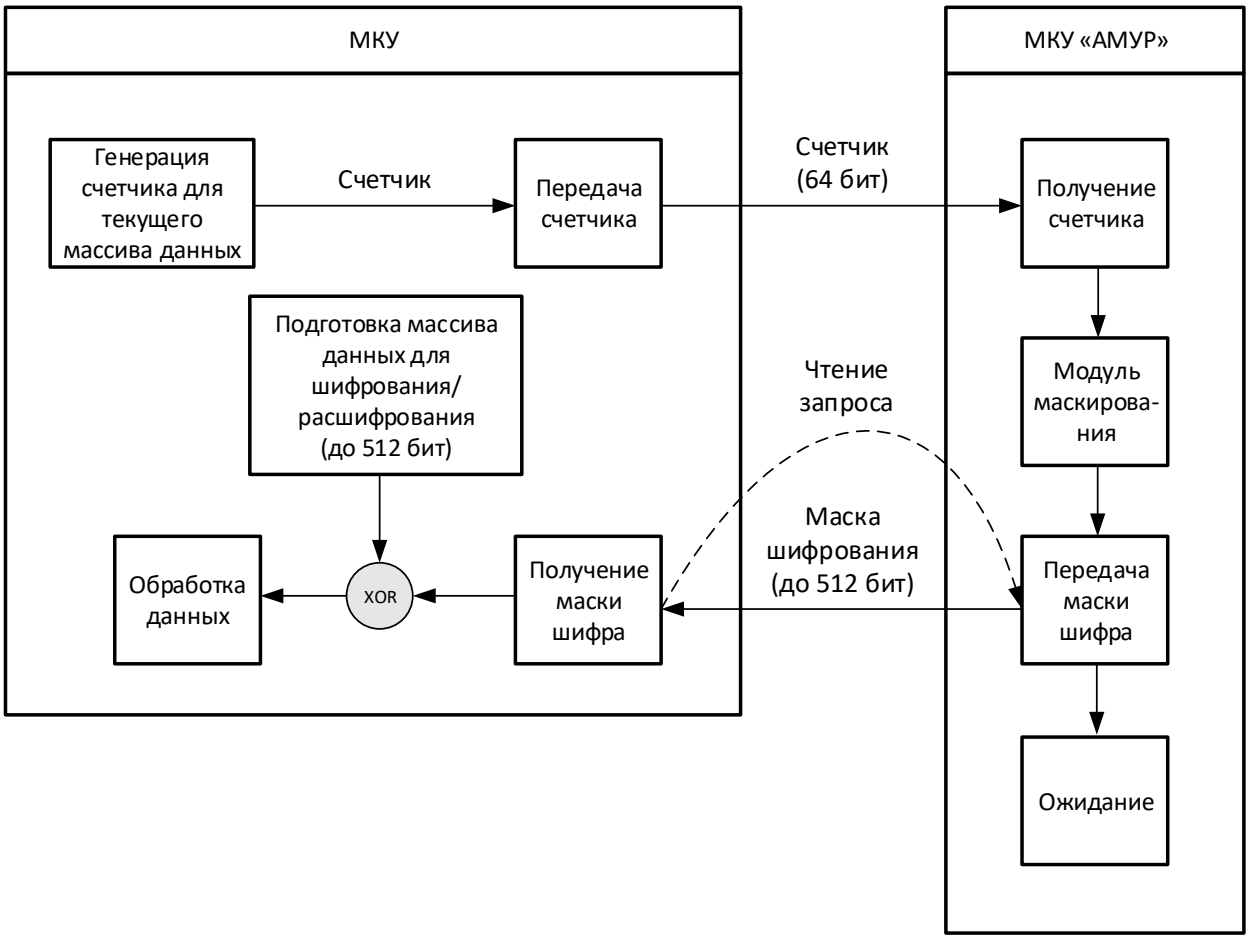

Рисунок 1

3 Проверка работоспособности

Проверку работоспособности программного обеспечения СПИ допустимо проводить на технологической плате типа «Отладочная плата START-MIK32-V1» или «DIP-MIK32-V4», которая подключается к ПЭВМ по виртуальному COM-порту через интерфейс UART. Для взаимодействия используют программное обеспечение «Тестирование СПИ» (Рисунок 2), способное устанавливать параметры COM-порта и скорость передачи данных, а также производить имитацию отправки команд.

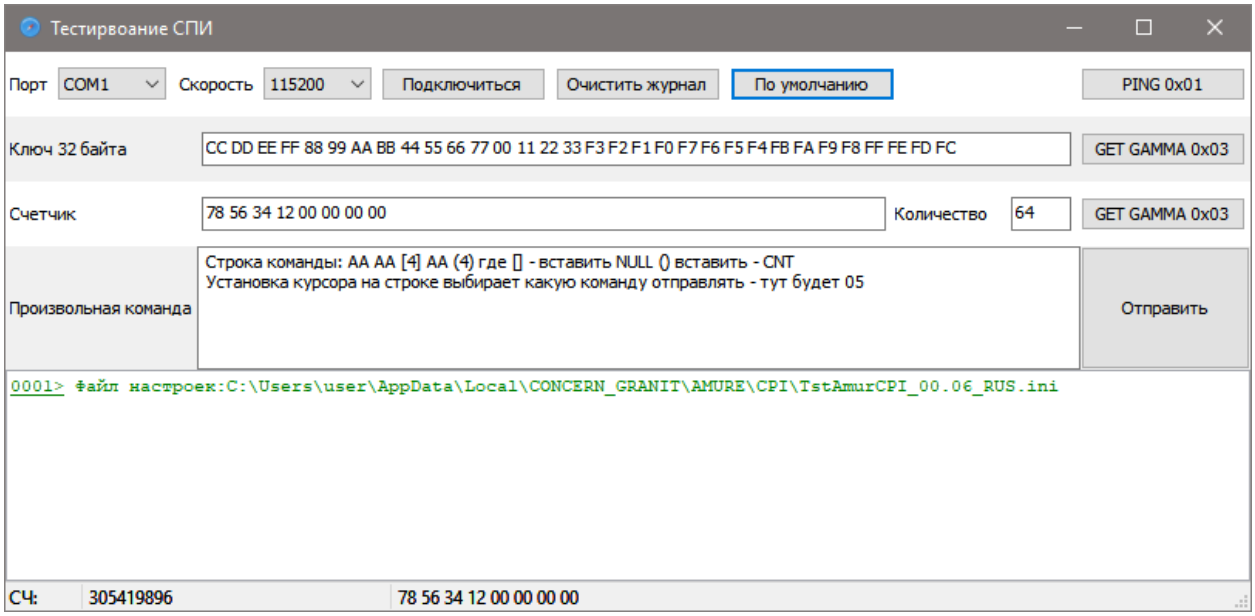

Рисунок 2

На время проверки работоспособности ПЭВМ выполняет функции МКУ: в программном обеспечении «Тестирование СПИ» пользователь заполняет поля «Ключ 32 байта», «Счетчик», «Количество» и по нажатию на соответствующие кнопки отправляет команды по виртуальному COM-порту на плату. Микроконтроллер MIK32 «Амур» на плате принимает эти данные, выполняет преобразования по алгоритму ГОСТ 34.12-2018 и возвращает результат по тому же интерфейсу UART. После чего пользователь может сразу увидеть полученные замаскированные или размаскированные данные в окне терминальной программы и оценить корректность работы контроллера.

3.1 Пример успешного выполнения команды пинг (0x01)

Формат пакета команды 0x01 приведен на рисунке 3. Данная команда позволяет произвести проверку наличия микроконтроллера MIK32 «Амур», а также запросить версию его программного обеспечения.

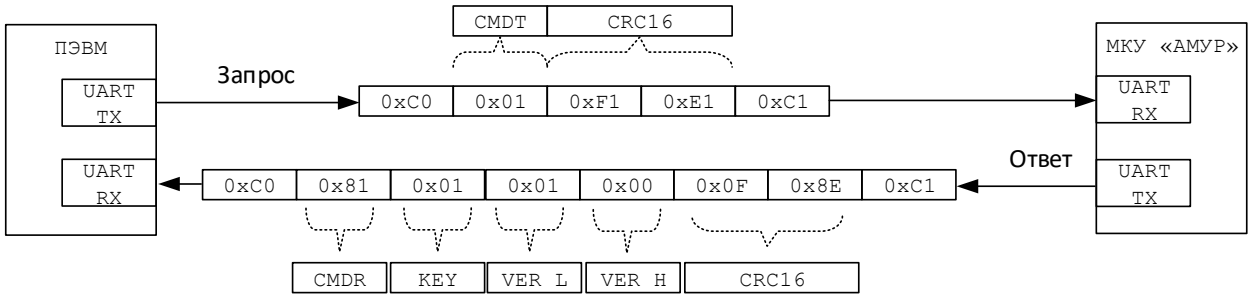

Рисунок 3

3.2 Пример успешной команды установки ключа (0x02)

Формат пакета команды 0x02 приведен на рисунке 4. Данная команда позволяет установить ключ маскирования размером 32 байт в микроконтроллер MIK32 «Амур». В качестве примера в поле «KEY» передается последовательность, взятая из ГОСТ 34.13-2018.

KEY = CCDDEEFF8899AABB4455667700112233F3F2F1F0F7F6F5F4FB FAF9F8FFFEFDFCh.

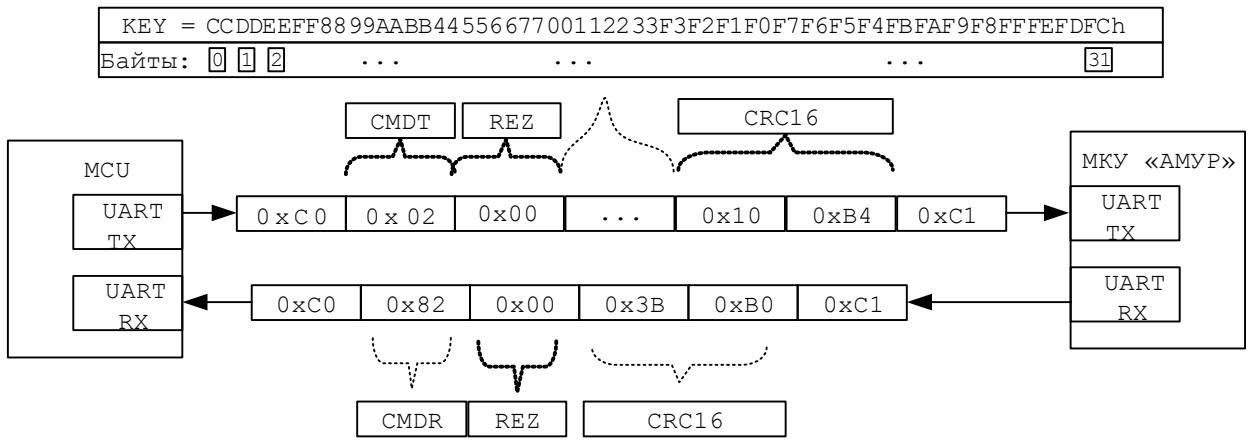

Рисунок 4

3.3 Пример успешной команды запроса гаммы (0x03)

Формат пакета команды 0x03 приведен на рисунке 5. Данная команда позволяет запросить гамму, сформированную микроконтроллером MIK32 «Амур». В примере приведен успешный запрос гаммы на счетчике CNT = 7856341200000000. Поле «GAMMA» содержит набор сформированных байт согласно алгоритму, «Магма» ГОСТ 34.12-2018.

Значение сформированной гаммы: 67E146DC65B3A4AB97CA71E549C 0F02EA67DF559A3D91A601BF69CDF6CDFE7BCh.

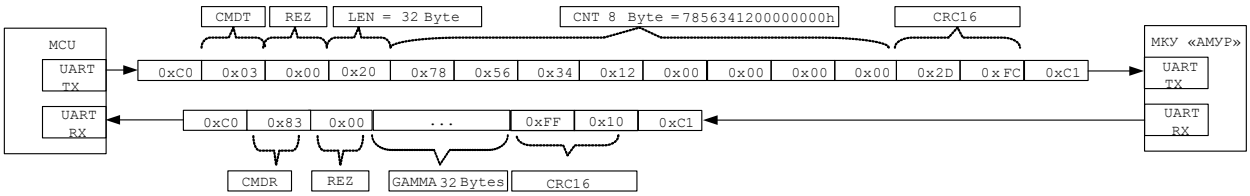

Рисунок 5