УДК 621.9.048.7

ШИФР «ANDROMEDA»

Щербина Т.С.

БГУИР, Минск, Республика Беларусь,radkevich.t.s@gmail.com

Прогресс подарил человечеству огромное множество достижений, но он же произвел и массу проблем. Разрешая одни проблемы, человеческий разум постоянно сталкивается с иными, уже новыми, и процесс этот бесконечен. Хотя, если уж быть точной, новые проблемы – это всего лишь немного измененная, где-то обновленная форма старых. Проблема, которая всегда была актуальной – проблема защиты информации. На разных этапах своего развития, эта проблема решалась человечеством согласно характерности, присущей для данной эпохи. Изобретение компьютера и последующее быстрое развитие информационных технологий во второй половине двадцатого века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества.

Сегодня, во времена стремительного развития технологий, наиболее остро встают проблемы информационной защиты. Повсеместное распространение разработки и использования автоматизированных систем обработки информации и управления выдвинуло проблему защиты информации от несанкционированного доступа на первый план. Основные проблемы защиты информации в компьютерных системах возникают из-за того, что информация не является жёстко связанной с носителем. Её можно легко и быстро скопировать и передать по каналам связи. Информационная система подвержена как внешним, так и внутренним угрозам со стороны нарушителей.

Основные проблемы защиты информации при работе в компьютерных сетях, можно условно разделить на три типа:

- перехват информации (нарушение конфиденциальности информации);
- модификация информации (искажение исходного сообщения или замена другой информацией);
- подмена авторства (кража информации и нарушение авторского права).

Сегодня защита компьютерных систем от несанкционированного доступа характеризуется возрастанием роли программных и криптографических механизмов по сравнению с аппаратными. Использование новых, стойких к существующим атакам и методам взлома алгоритмов поможет защитить информацию.

Andromeda – легко масштабируемый и легко реализуемый с точки зрения программного обеспечения шифр. Andromeda – поточный симметричный шифр с высокой производительностью. Он сочетает в себе такие «не сочетаемые» параметры как простота, но при этом стойкость к любым видам криптоанализа.

Генератор этого шифра sponcge – диффузный – когерентный. Шифр симметричный, с высокой производительностью.

В базовой реализации обычно состоит из пяти блоков:

- инициализатор шифра;
- байтовый весовой шифратор;
- байтовый весовой дешифратор (иногда, в случае модульного умножения, их объединяют);

− генератор-смеситель (компонент, который объединяет ГПСЧ с весовым дешифратором);

− деинициализатор (для повышения защиты ключа от его определения).

По своей структуре генератор напоминает генератор RC4, за исключением того, что Andromeda не имеет ключевого расписания, при инициализации генератора нужно использовать любые криптостойкие хеширующие методы и протоколы основанные на правиле 1567 (в режиме KDFx с использованием синтетической соли, для параметризации хеш-функции лучше использовать аппаратный ГСЧ или прораммные ГСЧ основанные, например, на осцилляции частот процессоров за счет теплового шума). Уникальность шифра в том, что можно без труда изменять выходной период генератора, а так же в наличии байтового весового шифратора и дешифратора.

Рассмотрим каждый блок шифра.

Инициализатор шифра – его задача любым способом инициализировать массивы Pool и SBox размером по 1500 б. Эти массивы должны быть заполнены случайными байтами, полученными в ходе хеширования случайных параметров стойким хешем в режиме KDFx ≥ 8000 (рекомендуемый режим). Размер массивов по 1500 байт является достаточным размером для обеспечения стойкости шифра.

Инициализатор шифра – инициализация SBox и Pool.

Генератор-смеситель – элемент, который определяет шифрующие ключи. Сложность алгоритма состоит в том, что каждый байт шифруется тремя ключами. Два из которых – ключи из Sbox и Pool, полученные при помощи алгоритмов смешивания элементов массивов, а третий – так называемый «синтетический ключ» – ключ, полученный рядом операций над SBox и Pool. Далее шифруемый символ, элемент по первому ключу из массива SBox, элемент по второму ключу из массива Pool и третий ключ отправляются на компонент смесителя.

Байтовый весовой шифратор – это компонент, принимающий три ключа и байт открытого текста для шифрования и при помощи любых комбинаций обратимых побитовых операций шифрует с помощью ключей исходный байт. Таких байтовых весовых шифраторов несколько, и сложность аключается в том, что по весу ключей определяется, каким шифратором будет зашифрован байт текста.

Байтовый весовой дешифратор работает по тому же принципу, что и байтовый шифратор, но использует, соответственно, обратные операции.

Деинициализатор – очищение инициализированных структур в памяти методом Гутмана.

Схема алгоритма «Andromeda» представлена на рисунках 1-4.

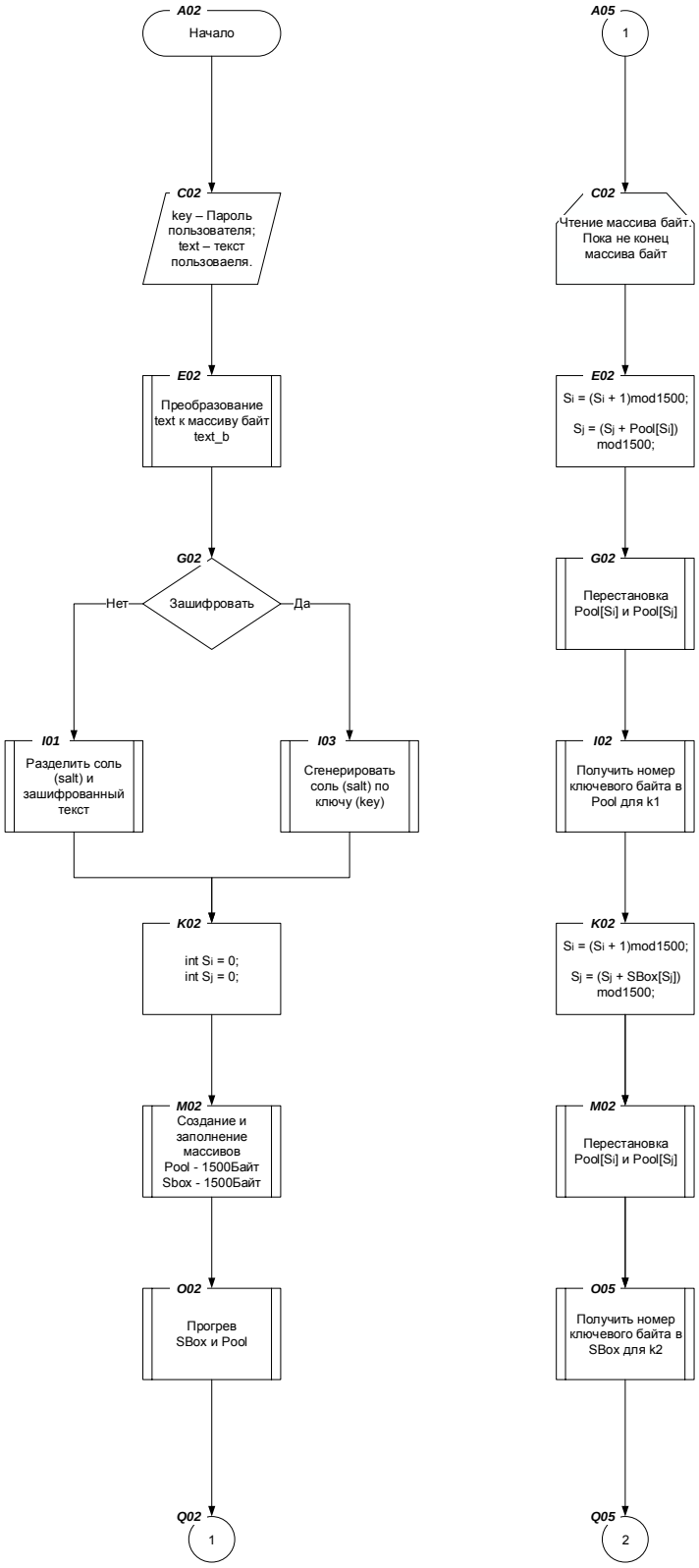

Рисунок 1 – Схема алгоритма «Andromeda»

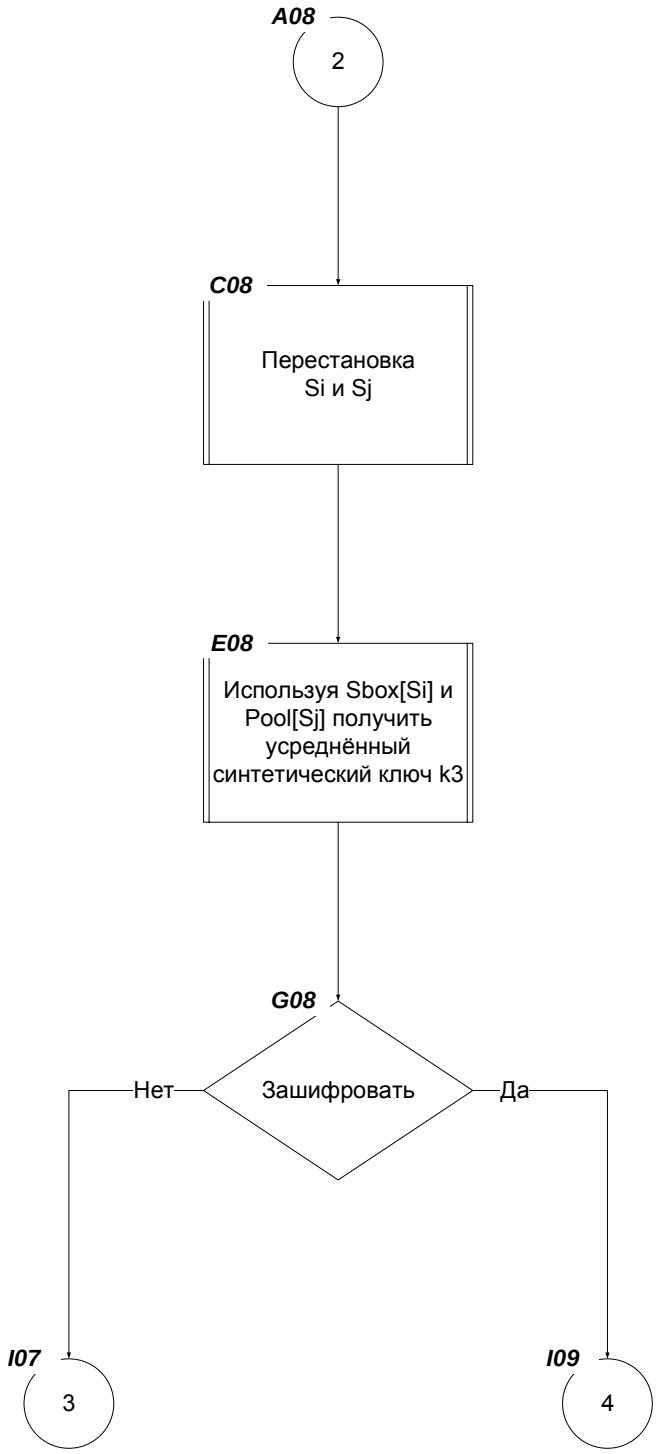

Рисунок 2 – Схема алгоритма «Andromeda»

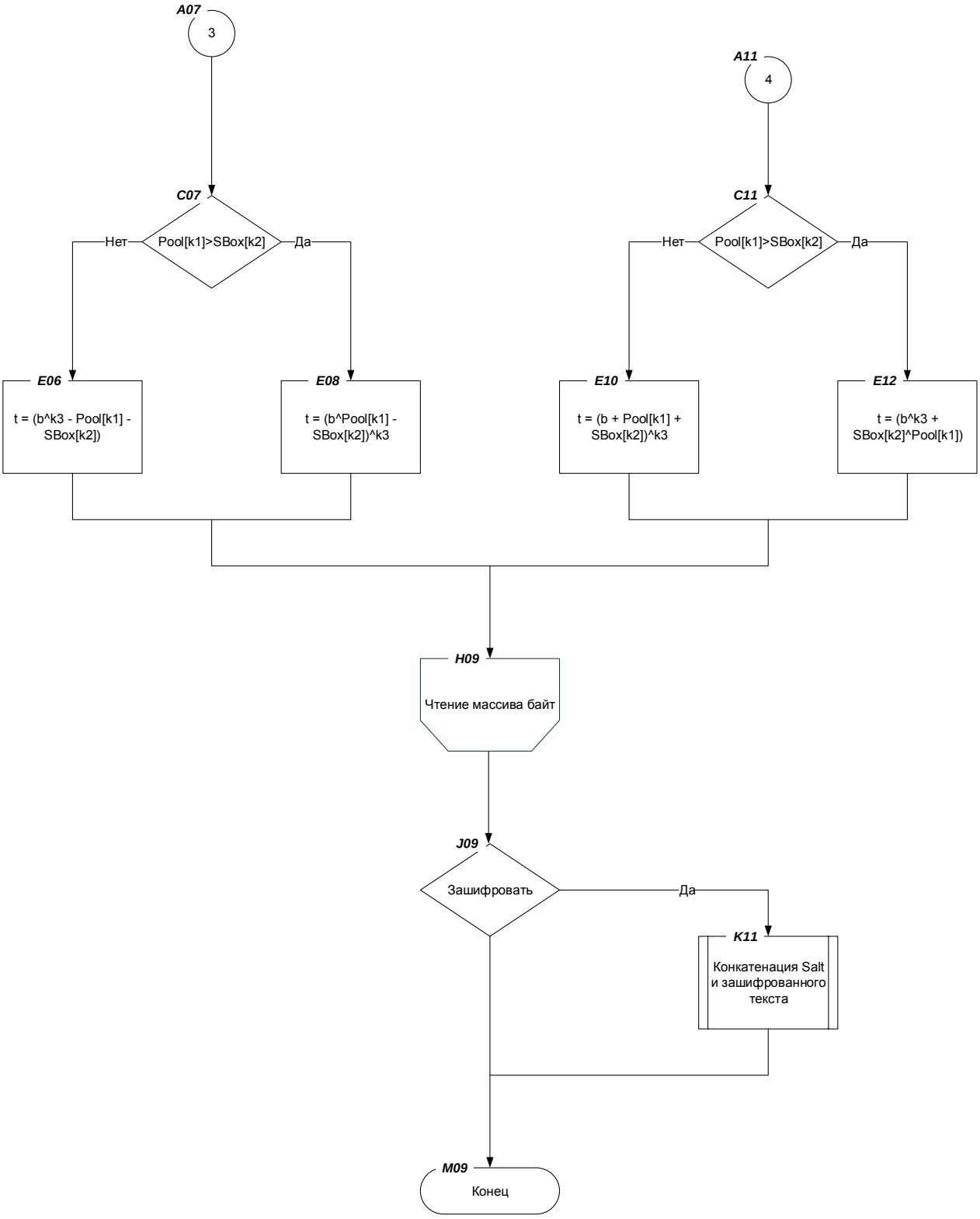

Рисунок 3 – Схема алгоритма «Andromeda»

Решение проблем защиты электронной информации базируется в основном на использовании криптографических методов. Притом современные методы криптографического преобразования сохраняют исходную производительность автоматизированной системы. Это немаловажно. Это является наиболее эффективным способом, обеспечивающим конфиденциальность данных, их целостность и подлинность.

Использование криптографических методов в совокупности с техническими и организационными мероприятиями обеспечивают надежную защиту от широкого спектра угроз.

Список литературы:

1. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер СПб: Питер, 2001

2. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

3 Голиков А.М. Основы информационной безопасности: учеб. пособие для практических и семинарских занятий. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 154 с.