DOI: 10.17117/na.2016.03.03.110

<http://ucom.ru/doc/na.2016.03.03.110.pdf>

Поступила (Received): 30.03.2016

Мангутов Д.В., Белехов А.Н. Алгоритм шифровки файлов на основе программного обеспечения Kerio Technologies

Mangutov D.V., Belekhov A.N.
Algorithm for file encryption based on Kerio Technologies software

Рассмотрены актуальные вопросы информационной безопасности. Предложен алгоритм программного обеспечения для шифрования и расшифровывания файлов на основе российского криптографического стандарта ГОСТ 28147-89 с использованием системы защиты Kerio Technologies

Ключевые слова: Kerio Technologies, криптопреобразование, информационная безопасность

Topical issues of information security were examined. Software Algorithm for to encrypt and decrypt files on the basis of the Russian cryptographic standards GOST 28147-89 using Kerio Technologies protection was offered

Key words: Kerio Technologies, cryptographic transformation, information security

Мангутов Дмитрий Вячеславович
Студент
Российский экономический университет им. Г.В. Плеханова
г. Москва, Стремянный пер., 36

Mangutov Dmitry Vyacheslavovich
Student
Russian university of economics named G.V. Plekhanov
Moscow, Stremyannyy ave., 36

Белехов Александр Николаевич
Кандидат технических наук, доцент
Российский экономический университет им. Г.В. Плеханова
г. Москва, Стремянный пер., 36

Belekhov Aleksandr Nikolaevich
Candidate of Technical Sciences, Associate Professor
Russian university of economics named G.V. Plekhanov
Moscow, Stremyannyy ave., 36

Вопросы информационной безопасности и физические методы защиты [1] играют сегодня огромную роль в сфере высоких технологий, где именно информация (особенно цифровая) становится одновременно «продуктом и сырьём» [2]. Огромный «мегаполис IT» построен на всемирных «реках» данных из разных точек планеты. Её производят, обрабатывают, продают и, к сожалению, зачастую воруют.

Транс альянс онлайн (ТАО) проанализировал более 1000 нарушений данных с 2014 года и пришли к выводу, что около 90% из них можно было бы легко предотвратить. ТАО изучили утечки данных с 2014 года, повлекшей за собой потерю личной информации (PII) и обнаружили, что эти нарушения могут быть отнесены к одной из четырех причин: 40% от внешних вторжений; 29% сотрудниками, случайно или злонамеренно; 18% от потерянных или украденных

устройств или документов; и 11% по социальной инженерии или мошенничества. Согласно ОТА, 90% этих данных нарушений можно было бы легко избежать путем укрепления внутреннего контроля. "Компании перегружены растущими рисками и угрозами, но слишком часто не в состоянии применить основы безопасности", сказал Крейг Спайзл, исполнительный директор и президент компании ОТА [3].

Государственная политика обеспечения информационной безопасности РФ определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов территорий в этой области, порядок закрепления их обязанностей и ответственности за защищенность интересов РФ в информационной сфере в рамках закрепленных за ними направлений деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере [4].

Множество существующих методов обеспечения информационной безопасности можно классифицировать по разным признакам, но только уместные комбинации этих признаков позволяют сетевому администратору обеспечить надлежащий уровень информационной безопасности [5].

В целом все методы можно разделить на два класса:

I. Правовые методы обеспечения информационной безопасности РФ, включающие разработку нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности. Наиболее важными направлениями этой деятельности являются: внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности РФ, устранения внутренних противоречий в федеральном законодательстве, а также противоречий, связанных с международными соглашениями, к которым присоединилась Россия, и противоречий между федеральными законодательными актами и законодательными актами субъектов РФ. Определению целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан будет способствовать законодательное разграничение полномочий в области обеспечения информационной безопасности РФ между федеральными органами государственной власти и органами государственной власти субъектов РФ в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности.

II. Организационно-технические методы обеспечения информационной безопасности РФ, включавшие разработку, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения. Сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации; совершенствование системы сертификации телекоммуникационного оборудова-

ния и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности; контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ; формирование системы мониторинга показателей и характеристик информационной безопасности страны в наиболее важных сферах жизни и деятельности общества и государства.

Автором статьи предлагается алгоритм программного обеспечения для шифрования и расшифровывания файлов на основе криптографического стандарта ГОСТ 28147-89 с использованием системы защиты Kerio Technologies. [6].

Основной шаг криптопреобразования моделируется следующими командными процедурами.

1. Определение исходных данных для основного шага криптопреобразования: N – преобразуемый 64-битовый блок данных, в ходе выполнения шага его младшая ($N1$) и старшая ($N2$) части обрабатываются как отдельные 32-битовые целые числа без знака. Таким образом, можно записать (основной шаг криптопреобразования) $N = (N1, N2)$.

2. Сложение младшей половины преобразуемого блока (основного шага криптопреобразования) по модулю 2^{32} с используемым на шаге элементом ключа с передачей результата на следующий шаг.

3. Проведение поблочной замены – 32-битное значение, полученное на предыдущем шаге, интерпретируется как массив из восьми 4-битовых блоков кода: $S = (S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7)$, с представлением заменены на новое значение каждого из восьми блоков, которое выбирается в следующем порядке – значение блока S_i заменяется на S_{i+1} (нумерация с нуля) i -ого узла замен (в i -ой строке таблицы замен нумерация начинается также с нуля). Таким образом, в качестве замены для значения блока выбирается элемент из таблицы замен с номером строки, равным номеру заменяемого блока, и номером столбца, равным значению заменяемого блока как 4-битового целого неотрицательного числа.

4. Назначение циклического сдвига на 11 бит влево – результат предыдущего шага сдвигается в сторону старших разрядов и передается на следующий шаг.

5. Выполнение побитового сложения для значения N (основного шага криптопреобразования) – полученное на шаге 3, побитно складывается по «модулю 2 со старшей половиной преобразуемого блока».

6. Обеспечение сдвига по цепочке на шаг вперед – младшая часть преобразуемого блока сдвигается на место старшей, а на ее место помещается результат выполнения предыдущего шага.

7. Возвращение полученного значения преобразуемого блока, как результата выполнения алгоритма основного шага криптопреобразования.

Базовые циклы являются алгоритмами для криптографических преобразований, то есть для шифрования, расшифрования и «учета» в контрольной комбинации одного блока данных.

Для каждого элемента данных выполняется основной шаг криптографического преобразования с элементами ключа, порядок базовых циклы построены из основных шагов криптографического преобразования.

Существует всего три базовых цикла, различающиеся порядком следования ключевых элементов, принятых в ГОСТ 28147-89 [7] циклов:

– зашифрования 32-З

(K0,K1,K2,K3,K4,K5,K6,K7,K0,K1,K2,K3,K4,K5,K6,K7,K7,K6,K5,K4,K3,K2,K1,K0).

– расшифрования 32-Р в виде

(K0,K1,K2,K3,K4,K5,K6,K7,K7,K6,K5,K4,K3,K2,K1,K0,K7,K6,K5,K4,K3,K2,K1,K0).

– выработки имитовставки 16-З:

(K0,K1,K2,K3,K4,K5,K6,K7,K0,K1,K2,K3,K4,K5,K6,K7).

Каждый из циклов имеет собственное буквенно-цифровое обозначение, соответствующее шаблону «n-X», где первый элемент обозначения (n), задает число повторений основного шага в цикле, а второй элемент обозначения (X), буква, задает порядок зашифрования («З») или расшифрования («Р») в использовании ключевых элементов.

Для циклов шифрования левая и правая половины блока меняются местами, для цикла выработки имитовставки – нет.

В данной статье были рассмотрены основные проблемы информационной безопасности и предложен алгоритм программного обеспечения на основе криптографического стандарта ГОСТ 28147-89, как части системы защиты «Kerio Technologies, путем криптографического преобразования данных, позволяющий шифровать и расшифровывать файлы, для обеспечения сохранности информации. Были указаны командные процедуры в обеспечение процесса оперативного криптопреобразования произвольных файлов различного назначения.

Список используемых источников:

1. Гришачев В.В., Халяпин Д.Б., Шевченко Н.А., Мерзликин В.Г. Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС // Специальная техника. 2009. № 2. С. 2-9.
2. Шаньгин В. Информационная безопасность и защита информации. ДМК Пресс, 2014. 702 с.
3. Геллер М. Tech Target 21 января 2015.
URL: <http://searchsecurity.techtarget.com/news/2240238606/Report-More-than-90-of-2014-data-breaches-could-have-been-prevented>
4. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации». 2006. Ред. от 13.07.2015.
5. Доктрина информационной безопасности Российской Федерации № ПР 1895. 2004.
6. Kerio Technologies. JSC Kerio Technologies. URL: <http://www.kerio.ru/>
7. Государственный общероссийский стандарт 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». М.: Стандарты, 1990.