УДК 504.064.36

А.М. Игнатьев[1], О.М. Семкив[1], А.Б. Куренко[2]

[1] *Университет гражданской защиты Украины, Харьков*
[2] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*

ОБЕСПЕЧЕНИЕ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ СООБЩЕНИЙ ПРИ МОНИТОРИНГЕ ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

Проведен анализ существующих методов защиты целостности и достоверности передаваемых сообщений. Показаны перспективы использования несимметричных криптосистем для передачи сообщений при сборе, обмене и хранении информации о состоянии потенциально опасных объектов. Представлен исследовательский прототип программы генерации электронной цифровой подписи, позволяющий использовать открытые каналы связи для передачи информации. Предлагаемый метод передачи сообщений исключает возможность проведения актов технического терроризма в базе данных Государственного реестра потенциально опасных объектов.

Ключевые слова: *электронная цифровая подпись, несимметричные криптосистемы, потенциально опасные объекты, исследовательский прототип.*

Введение

Постановка проблемы. С целью получения данных о текущем состоянии потенциально опасных объектов (ПОО) и актуализации информации, которая содержится в базе данных Государственного реестра ПОО, проводится мониторинг этих объектов в рамках заданий единой государственной системы предупреждения и реагирования на чрезвычайные ситуации техногенного и природного характера [1].

При этом для передачи информации используются системы компьютерной связи и существующие технические средства связи. Следует отметить, что в отличие от закрытых каналов связи, существующие компьютерные системы являются весьма уязвимыми с точки зрения достоверности передаваемых сообщений.

Благодаря открытости каналов передачи данных, а также доступности в оснащении современными образцами оконечной аппаратуры связи, становится возможным внедрение дезинформации и искажение передаваемых сообщений злоумышленниками, в том числе и с целью проведения актов технического терроризма [2]. При этом возможны значительные осложнения ситуаций в виду не объективного получения информации о действительном состоянии ПОО, а также проникновения программ-вирусов в компьютерную систему. Не снимается с повестки дня и возможность проведения информационно-психологических операций. В связи с тем, что вышеуказанные факторы подлежат учету при проведении мониторинга потенциально опасных объектов в условиях открытости большинства каналов передачи сообщений, весьма актуальной представляется задача исследования, разработки и внедрения современных методов обеспечения защиты передаваемой информации.

Анализ последних исследований и публикаций. В ряде работ, посвященных обеспечению защиты информации, как правило, рассматриваются симметричные криптографические системы и разнообразные методы контроля и защиты при помощи

технических средств [3 – 6]. Применение симметричных криптографических систем связано с генерацией, рассылкой и контролем ключевых данных, что требует создания и содержания дополнительной закрытой системы. Вместе с тем, для проникновения в компьютерные системы всѐ чаще используется некомпетентность и халатность обслуживающего персонала [6].

Эти недостатки отсутствуют в криптографических системах с открытым ключом (несимметричные криптосистемы). В таких системах для шифрования данных используется один ключ, а для расшифровки другой.

Первый ключ является открытым и может быть опубликован для шифрования своей информации любым пользователем сети.

Получатель зашифрованной информации для расшифровки данных использует второй ключ, являющийся секретным. При этом соблюдается условие: секретный ключ не может быть определѐн из опубликованного открытого ключа. Однако следует отметить тот факт, что алгоритмы несимметричных криптосистем требуют больших вычислительных ресурсов.

Сравнительная характеристика алгоритмов шифрования приведена в табл. 1.

Таким образом, в связи с огромным прогрессом в области вычислительной техники, значительным увеличением производительности компьютерных систем массового персонального производства, задача исследования целесообразности внедрения несимметричных криптосистем приобретает особую актуальность.

Таблица 1

Сравнительная характеристика алгоритмов шифрования

Характеристика алгоритма	DES, AES, ГОСТ 28147-89	RSA
Скорость шифрования	Высокая	Низкая
Используемая функция шифрования	Перестановка и подстановка	Возведение в степень
Длина ключа	56 бит	Более 500 бит
Наименее затратный криптоанализ (его сложность определяет стойкость алгоритма)	Перебор по всему ключевому простору	Разложение числа на простые множители
Время генерации ключа	Миллисекунды	Минуты
Тип ключа	Симметричный	Асимметричный

Постановка задачи и ее решение

Для проведения исследований алгоритм наиболее известной системы несимметричного шифрования RSA (название алгоритма взято из первых букв фамилий его авторов – Rivest, Shamir и Aldeman в английском варианте) был представлен в следующем виде:

1. Случайно выбираются два очень больших простых числа p и q.

2. Вычисляются два множителя $n = p \times q$ и $m = (p-1) \times (q-1)$.

3. Выбирается случайное целое число E, которое не имеет общих сомножителей с m.

4. Находится D, такое, что $DE = 1$ по модулю m.

5. Исходный текст X разбивается на блоки так, чтобы $0 < X < n$.

6. Для шифрования сообщения необходимо вычислить $C = X^E$ по модулю n.

7. Для дешифрования вычисляется $X = C^D$ по модулю n.

В системе, построенной на базе протокола RSA, зашифровать сообщение может любой, кто знает открытый ключ, а раскрыть только адресат, который обладает закрытым ключом. Другое свойство протокола RSA состоит в том, что если поменять местами числа E и D, то получится, что зашифровать можно закрытым ключом, а расшифровать открытым. Таким образом, зашифровать сообщение может отправитель, а расшифровать может любой получатель. На этом свойстве формируется так называемая «цифровая подпись» [6]. Она определяет авторство сообщения.

Вышеприведенное свойство алгоритма RSA было применено при разработке исследовательского прототипа программы генерации электронной цифровой подписи (ЭЦП). С целью контроля достоверности сообщений использовалось свойство свѐртки (зависимости целостности сообщения от ключа и сформированной электронной подписи). Для передачи сообщения, открытого ключа и ЭЦП используются обычные каналы связи (на первом этапе испытаний передача велась по локальной компьютерной сети).

Возможна передача «подписанного» сообщения и через компьютерную сеть Internet, как показано на рис. 1.

При проведении испытаний исследовательского прототипа программы генерации электронной цифровой подписи, в которых экспериментально определялась зависимость времени генерации ЭЦП от объѐма сообщения, было установлено, что при объѐме текста до 50 страниц интервал работы программы не превышает 8 секунд.

Эксперименты проводились при следующих параметрах, влияющих на производительность компьютерной системы: архитектура процессора – двухядерный Athlon, рабочая частота процессора – 1,8 ГГц, объём оперативной памяти – 1 Гбайт, операционная система – Windows XP.

При этом программный продукт разработан в среде объектно-ориентированного программирования Delphi 7.0, имеет удобный для пользователя интерфейс, представленный на рис. 2, и не требует длительного обучения.

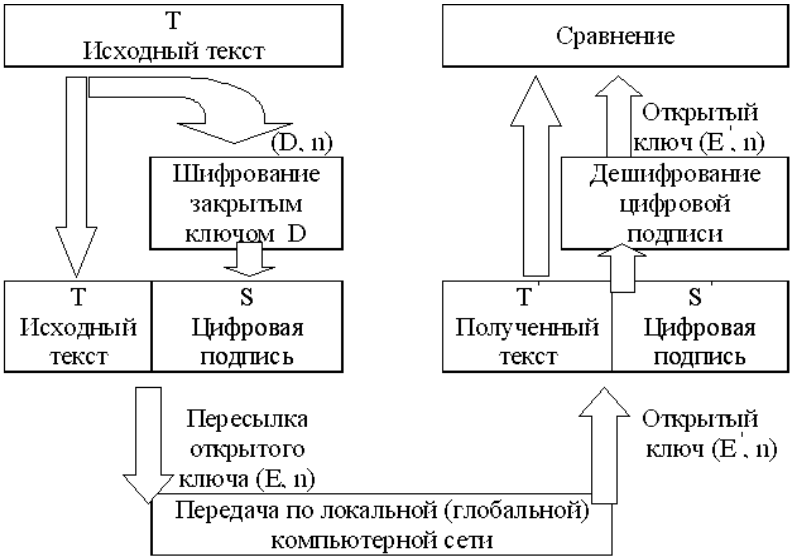

Рис. 1. Формирование электронной цифровой подписи
в соответствии с алгоритмом RSA

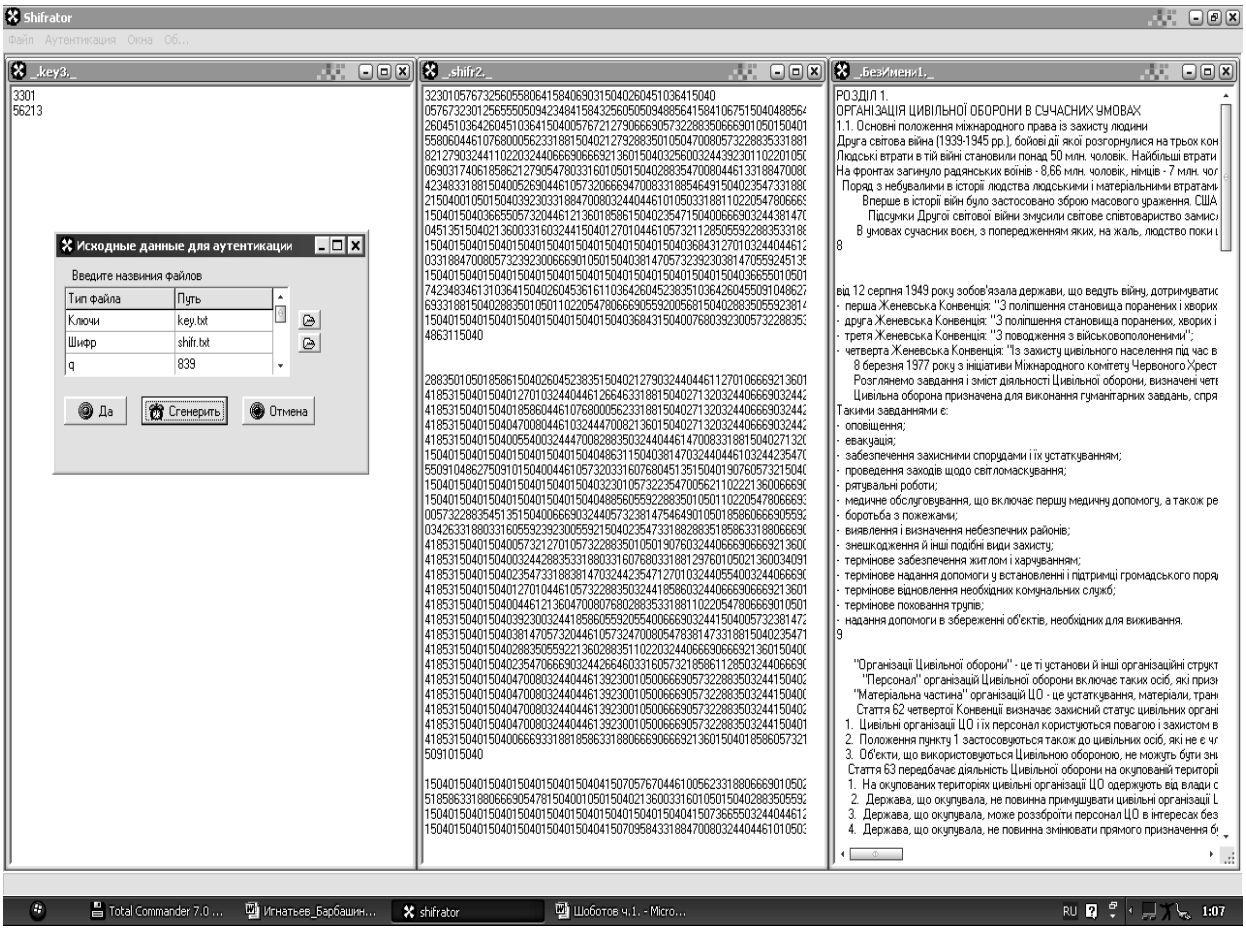

Рис. 2. Интерфейс исследовательского прототипа программы генерации ЭЦП

Выбор мотивировался тем, что указанная версия включает в себя простую и удобную диалоговую оболочку, позволяющую эффективно отлаживать программы на уровне исходных текстов и оптимизировать их, повышая производительность. К недостаткам исследовательского прототипа программы генерации ЭЦП можно отнести наличие при передаче сообщений ещѐ и самой ЭЦП.

Сама электронная цифровая подпись по объѐму несколько превышает передаваемое сообщение. Однако именно этот дополнительный файл позволяет подтвердить достоверность переданной информации.

Выводы

Рассмотрены возможности применения несимметричных криптосистем с целью решения актуальной задачи защиты информации при проведении мониторинга потенциально опасных объектов. Представлен исследовательский прототип программы генерации ЭЦП. Генерация ЭЦП осуществляется для каждого сообщения отдельно и позволяет решать задачи проверки целостности и подлинности сообщения, а также не позволяет вносить дезинформацию. Особенностью этой реализации является то, что все задачи защиты и сохранения целостности информации решены без применения аппаратуры шифрования. Генерация ключевых данных осуществляется посредством ПЭВМ, а использование современных несимметричных криптографических систем позволяет рассылать ключевые данные по открытым каналам связи.

Список литературы

1. Наказ МНС України від 06.11.2003р. №425 «Про затвердження Положення про моніторинг потенційно небезпечних об'єктів» // Офіційний вісник України, 09.01.2004. – 2003 р. – № 52, том 2. – С. 610. – ст. 2857.

2. Наказ МНС України та СБ України від 08.07.2008р. № 508/525 Інструкція про порядок взаємодії МНС та СБУ із запобігання виникненню та реагування на надзвичайні ситуації техногенного та природного характеру. Зареєстровано в Міністерстві юстиції України 30 липня 2008 року за № 703/15394. – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.gdo.kiev.ua.

3. Столингс В. Криптография и защита сетей / В. Столингс. – М.: Вильямс, 2001. – 669 с.

4. Иванов И.А. Криптографические методы защиты информации в компьютерных системах и сетях / И.А. Иванов. – М.: КУДИЦ – ОБРАЗ, 2001. – 368 с.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 797 с.

6. Соколов А.В.. Методы информационной защиты объектов и компьютерных сетей / А.В. Соколов, О.М. Степанюк. – М.: ООО «Фирма «Издательство АСТ», СПб: ООО «Издательство «Полигон», 2000. – 272 с.

Поступила в редколлегию 20.08.2009

Рецензент: д-р техн. наук, старший научный сотрудник Г.В. Худов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ ПРИ МОНІТОРИНГУ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ

О.М. Ігнатьєв, О.М. Семків, О.Б. Куренко

Проведено аналіз існуючих методів захисту цілісності та достовірності повідомлень, які передаються. Показані перспективи використання несиметричних криптосистем для передачі повідомлень при зборі, обміні та зберіганні інформації про стан потенційно небезпечних об'єктів. Представлений дослідницький прототип програми генерації електронного цифрового підпису, який дозволяє використовувати відкриті канали зв'язку для передачі інформації. Запропонований метод передачі повідомлень виключає можливість проведення актів технічного тероризму в базі даних Державного реєстру потенційно небезпечних об'єктів.

Ключові слова: *електронний цифровий підпис, несиметричні криптосистеми, потенційно небезпечні об'єкти, дослідницький прототип.*

PROVISION TO VALIDITY OF THE ISSUE OF THE MESSAGES WHEN MONITORING POTENTIALLY DANGEROUS OBJECT

A.M. Ignatev, O.M. Semkiv, A.B. Kurenko

The organized analysis existing methods of protection to wholeness and validity of the sent messages. They are shown prospects of the use asymmetrical cryptosystems for issue of the messages at collection, exchange and keeping to information on condition potentially dangerous object. Will presented exploratory prototype of the program to generations electronic digital signature, allowing use the opened channels a relationship for transmission of information. The proposed method of the transmission of the messages excludes the possibility of the undertaking the acts of the technical terrorism in database of the State roll potentially dangerous object.

Keywords: *electronic digital signature, asymmetrical cryptosystems, potentially dangerous objects, exploratory prototype.*