Легко видеть, что полученное время, равное сумме $eft(a_1) + eft(a_2) - eft(a_1)$ будет минимальным. Следовательно, в общем случае минимальное время будет равно max ($eft(a_1)$, $eft(a_2)$). Аналогично получим, что максимальное время выполнения действий будет равно max ($lft(a_1)$, $lft(a_2)$).

ПРИМЕНЕНИЕ ОЦЕНОК НА ОСНОВЕ ЭНТРОПИИ ДЛЯ СРАВНЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ

Сен Н.Д., Котляров В.П., Григорьев Я.Ю.

ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет», Комсомольск-на-Амуре, e-mail: naj198282@mail.ru

Объектом исследования являются методы криптографических преобразований данных. *Предмет исследования* – криптостойкость. Исходные данные представлены в виде цветного изображения в формате gif, 400×296 пикселей. Алгоритмы шифрования – гаммирование, DES, TripleDES, Rijndael; режимы шифрования – ECB, CBC, CFB. Поиск энтропии исходных и зашифрованных данных осуществляется по классической формуле Шеннона [2]. Выявлены два подхода к определению энтропии изображений (RGB):

– энтропия изображения находится как сумма энтропии каналов изображения;

– энтропия изображения вычисляется в зависимости от вхождений цветов в изображение.

В первом подходе [3] для расчета энтропии изображения H(X) необходимо определить энтропию каждого из каналов изображения. Пусть вектор C – канал изображения X, $C = \{R, G, B\}$. Тогда э*нтропия канала изображения* определяется по формуле Шеннона:

$$H(C) = \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i} \right),$$

где C – канал изображения X; p_i – вероятность, определяемая как частное от деления количества появлений i-го байта ($i = 0...255$) в канале изображения C к числу байт канала C изображения X. Так как энтропия независимых источников равна сумме энтропии источников, то энтропия всего изображения $H(X)$ определяется как сумма энтропии каналов изображения:

$$H(X) = \sum H(C),$$

где C – канал изображения X, $C = \{R, G, B\}$.

В соответствии со вторым подходом энтропия изображения вычисляется по формуле Шеннона, однако вероятности определяются иным образом:

$$H(X) = \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i} \right),$$

где X – изображение; p_i – вероятность, определяемая как частное от деления количества вхождений пикселя i-го цвета (RGB) к количеству пикселей изображения X.

Пусть $H_1(X)$ и $H_1(Y)$ – энтропии исходного и зашифрованного изображения, рассчитанные первым способом, а $H_2(X)$ и $H_2(Y)$ – вторым способом соответственно. Энтропия зашифрованного изображения, «зашумленного» ранее, рассчитанная первым и вторым способом – Hga1(Y) и Hga2(Y). Начальная энтропия $H_1(X) = 14{,}81$, $H_2(X) = 5{,}57$.

При использовании и первого, и второго способа расчета энтропии наблюдается схожая тенденция – шифрование в режиме ECB является наиболее «слабым», что подтверждается визуально. Наиболее «сильным» является шифрование DES, TripleDES, Rijndael в режиме CBC, при «зашумлении» исходных данных – Rijndael в режиме CBC. Энтропия Hga1(Y) и Hga2(Y) практически не меняется относительно $H_1(Y)$ и $H_2(Y)$, а в ряде случаев – значительно меньше. Таким образом, выполняемые преобразования над исходными данными существенно не добавляют вариации цвета изображения. Недостатком подхода является то, что энтропия не учитывает сложность формирования структуры данных и если изображение зашумлено, то оно всё равно формально обладает большим количеством информации [4]. Следовательно, оценивание на основе энтропии не является достаточным условием для принятия решений о стойкости криптопреобразований.

Список литературы

1. Вентцель Е.С. Теория вероятностей. – М., 2002.

2. Shannon, C. E A Mathematical Theory of Communication // Bell System Technical Journal, 1948.

3. Ковалев Д.С. Представление и сжатие данных // НГУ, спецкурс. – Режим доступа: http://nsu.videosoft.org/2010/tasks/task1/, свободный.

4. Бутенков С.А. энтропийный подход к оценке качества гранулирования многомерных данных // КИИ. – 2008.

О ПОРЯДКЕ, ПРАВИЛАХ И ОПЫТЕ СОСТАВЛЕНИЯ ТЕХНИЧЕСКИХ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУКЦИОНОВ В ЭЛЕКТРОННОЙ ФОРМЕ НА ОСНОВЕ ФЗ-94

Чудинов А.В., Трещёв И.А., Григорьева А.Л.

ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет», Комсомольск-на-Амуре, e-mail: naj198282@mail.ru

Люди не так ясно понимали механизмы контроля за процессом проведения аукционов. Но со временем, как и везде, в этой области многие придумали обходные пути, для того, чтобы закупать товары и услуги у предопределенного до аукциона поставщика. Придумывались хитрые технические задания, менялись цены в ходе вскрытия конвертов поставщиков, усложнялись условия осуществления конкурсов.

В итоге в большинстве случаев стороннему поставщику выиграть аукцион было практически невозможно.Открытый аукцион в электронной форме – это тот же самый аукцион, но только в виртуальном его исполнении, и участникам нет необходимости присутствовать на аукционе физически. Участникам не надо присылать заявки на бумажных носителях в адрес заказчика, нет необходимости, в случае победы в торгах, оформлять бумажные договоры и высылать их почтой.

Вся техническая информация для проведения аукциона, сам аукцион с предложением цен и конечные договора предоставляются в электронной форме. Это накладывает определенные требования на участников торгов, которые должны пройти обязательные процедуры по аккредитации. Организаторы же должны создать все условия для проведения электронных аукционов.Заказчикам, которые собираются объявить аукцион для государственных нужд и на государственные деньги, теперь необходимо сделать следующее:

1. Получить ЭЦП (электронную цифровую подпись) в уполномоченном удостоверяющем центре Федерального казначейства, по месту регистрации предприятия. Выдача ЭЦП производится на безвозмездной основе. Для этого нужно в центр регистрации предоставить определённый пакет документов.

2. Проверить ЭЦП на сайте электронной площадке. Зарегистрироваться на одном или нескольких из сайтов, электронных площадок.

3. Заключить договор с электронной площадкой на обслуживание. Договор заключается на безвозмездной основе (единожды).

4. Установить программное обеспечение для работы с электронной площадкой.

5. Разместить на электронной площадке техническое задание и извещение о проведении аукциона.

Электронная цифровая подпись (ЭЦП) – это реквизит электронного документа, получаемый посредством его кодирования с помощью закрытого ключа. Всегда можно проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Использование ЭЦП защищает документ от внесения изменений после того, как документ подписан.

Поставщикам для участия в аукционах необходимо сделать почти все то же самое, за малым исключением:

1. Необходимо получить ЭЦП в удостоверяющих центрах (УЦ) электронной площадки, для каждой из площадок они разные. Если ЭЦП уже есть, необходимо проверить ЭЦП на сайте электронной площадки. Получение ЭЦП для поставщиков является платной услугой.

2. Пройти процедуру авторизации ЭЦП (Крипто-Про 3.6.6497, LISSI 1.3.6,,ViPNetCSP 3.2 4).

3. Пройти процедуру аккредитации, предоставив определённый пакет документов.

4. Перечислить на счет оператора электронной площадки денежные средства для обеспечения заявки участия в аукционе.

5. Далее поставщик может участвовать в аукционе.

Технические задания (задания на поставку товаров, выполнение работ, оказание услуг) – ключевой раздел конкурсной документации и документации об аукционе, в котором должны быть предельно подробно определены стоящие перед исполнителем задачи, а также объемы и перечень товаров, работ, услуг, являющихся предметом конкурса или аукциона. Техническое задание должно содержать требования: к качеству, техническим характеристикам товара, работ, услуг; к их безопасности; функциональным характеристикам (потребительским свойствам) товара; к размерам, упаковке, отгрузке товара; к результатам работ и иные показатели, связанные с определением соответствия поставляемого товара, выполняемых работ, оказываемых услуг потребностям заказчика.

В конкурсной документации (документации об аукционе) должен быть приведен полный и конечный перечень товаров, работ, услуг, которые будет поставлять, выполнять или оказывать победитель торгов, так как на этапе исполнения контракта изменению могут подлежать только количественные и объемные показатели в пределах ограничений, накладываемых нормами Закона № 94-ФЗ. Хотелось бы отметить, что ТЗ должно соответствовать не только нормам закона № 94-ФЗ, но и антимонопольному законодательству. Иными словами не ограничивать конкуренцию, т.е. на рынке должно быть два или более товаров от разных производителей.

Список литературы

1. О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд :федер. закон от 21.07.2005 г. № 94-ФЗ // Собрание законодательства РФ. – 2011.

2. Гречка Э. Новые правила проведения государственных закупок // GBI-MAGAZINE.RU: Журнал ЖБИ и конструкции. 2010. – URL: http://www.gbi-magazine.ru/index.php/n3-2010-/245-2010-07-22-16-20-06 (дата обращения: 25.03.2012)