Кульков И.В. Методы выявления шифротекста. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 50-52.

УДК 004

МЕТОДЫ ВЫЯВЛЕНИЯ ШИФРТЕКСТА

И.В. Кульков

CIPHERTEXT DETECTION METHODS

I.V. Kulkov

Аннотация. В статье рассматриваются возможные методы определения, являются ли данные шифртекстом.

Ключевые слова: шифртекст, информационная безопасность.

Abstract. This article describes the methods that can be used to determine whether some data is ciphertext or not.

Keywords: ciphertext, security.

Для того чтобы определить, является ли заданная информационная последовательность результатом работы функции шифрования, может быть использован ряд методов, описанных далее.

Основываясь на основных общепринятых свойствах шифров, таких как рассеивание и перемешивание [1, 2], можно говорить о том, что шифртекст должен обладать высоким уровнем информационной энтропии. Зашифрованные данные должны обладать высоким уровнем энтропии [1], в то время как низкий уровень энтропии информации является показателем того, что данные таковыми не являются. Как известно, энтропия информации вычисляется по следующей формуле:

$$H = -\sum_{0}^{255} p_i * log_2\ p_i$$

.

Однако преобразование

$$H = log_2\ n - \frac{1}{n}\sum_{0}^{255} N_i\ log_2\ n_i = log_2\ n - \sum_{0}^{255} p_i * log_2\ n_i$$

, где $p_i = \frac{n_i}{n}$,

показывает зависимость энтропии информации от размера исследуемых данных и распределения значений байт в этих данных. Вместе с тем в данный метод не может быть использован для гарантированной однозначной идентификации шифртекста, так как высокая энтропия присуща и другим видам распространенных в современном мире данных, например, архивированным данным. Таким образом, метод информационной энтропии дает наилучшие результаты при совместном использовании с другими методами.

Универсальный тест Маурера [3] относится к пакету статистических тестов NIST, разработанных в Национальном институте стандартов и технологий для проверки качества псевдослучайной последовательности. В основе рассматриваемого метода лежит идея Зива для универсальных алгоритмов кодирования, согласно которой случайную последовательность с равномерным законом распределения невозможно заметно сжать без потери информации. Таким образом, значи-

тельно сжимаемая последовательность считается неслучайной. Тест Маурера опирается на вычислении сумм логарифмов от числа бит между повторными проявлениями шаблонов заданной длины L и сравнении этой суммы с ее распределением для последовательности идеально случайной. Однако данный тест также имеет некоторые ограничения – размер анализируемых последовательностей данных не должен быть меньше 400 килобайт, иначе есть вероятность получить некорректный результат.

Критерий независимости Хи-квадрат [4] позволяет определить наличие значимой взаимосвязи между двумя номинальными переменными. Для реализации теста принимаются нулевая и альтернативные гипотезы – две переменные являются независимыми или зависимыми соответственно. В условиях рассматриваемой задачи статистическое значение может быть рассчитано для потока байтов данных по формуле

$$X^2 = \sum \frac{(O-E)^2}{E},$$

где O – наблюдаемое и E – ожидаемое значения байта в файле.

В случае, если полученное значение X^2 меньше критического, то принимается нулевая гипотеза, т.е. можно предположить, что рассматриваемые данные являются шифортекстом, т.к. последующий символ не зависит от предыдущего.

Библиографический список

1. Шеннон К. Работы по теории информации и кибернетике. М.: Изд. иностр. лит., 2002.

2. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. – John Wiley & Sons, 2017.

3. Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования = The Art of Computer Programming. 3-е изд.. М.: Вильямс, 2000. Т. 2. Получисленные алгоритмы. 832 с. ISBN 5-8459-0081-6.

4. William G. Cochran. The Annals of Mathematical Statistics Vol. 23, No. 3 (Sep., 1952), pp. 315-345

Кульков Иван Васильевич
ООО «Открытые решения»,
г. Пенза, Россия
E-mail: ivan.kulkov@osinit.com

Kulkov I.V.
LLC «Otkrytye resheniya»,
Penza, Russia