Сокрытие данных в контейнере с шумом с полосой частот маскируемых данных

Смирнова Н.В, Смирнов В.В, Кировоградский национальный технический университет, swckntu@rambler.ru

The method for data protection by hiding the data in to container which containing the noise spectrum of lying in the useful signal (data) frequency band is submitted

ВСТУПЛЕНИЕ

В настоящее время имеется проблема защиты информации в корпоративных информационных системах от несанкционированного доступа, как со стороны пользователей, так и со стороны злоумышленников. Статистика фактов несанкционированного доступа к информации показывает, что большинство современных информационных систем достаточно уязвимо с точки зрения безопасности. Имеющиеся на сегодняшний день средства защиты данных в той или иной мере решают эту проблему, но не всегда являются приемлемыми в каждом конкретном случае, например, по причине технической несовместимости с уже используемыми средствами.

РЕАЛИЗАЦИЯ МЕТОДА СОКРЫТИЯ ДАННЫХ

Для решения задачи ограничения доступа к информации в базе данных системы тестирования знаний студентов была разработана библиотека API, позволяющая использовать функции защиты данных при создании любых программ работы с данными. В основе библиотеки API лежат элементы методов защиты данных: стеганографии, одноразового блокнота, рандомизированного динамического XOR. Основным методом является метод сокрытия зашифрованных данных в контейнере (записи базы данных) со спектром шумов, совпадающим со спектром полезного сигнала (данных). При этом спектр сигнала (данных) приведен к рандомизированному в ограниченном интервале IR спектру шумов контейнера L (рис.1).

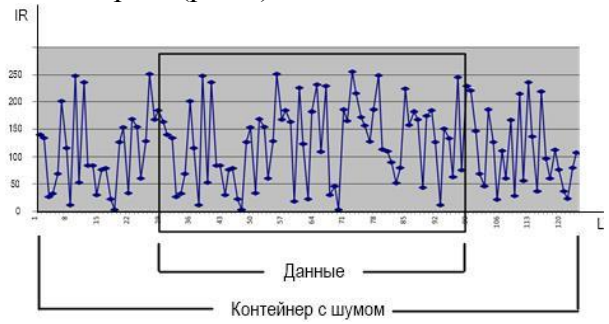

Рисунок 1 – Блок данных в контейнере

Местоположение зашифрованного блока данных в контейнере зависит от параметров рандомизирующей функции. Начальный ключ в цепочке зашифрованных ключей также является зашифрованным, а его расположение в контейнере зависит от ряда дополнительных параметров. Основной особенностью в данной реализации метода сокрытия данных является уникальность всех параметров рандомизированного динамического XOR как в границах записи, так и во всем массиве данных.

ВЫВОДЫ

Достоинством метода является его простота, достаточная эффективность, высокое быстродействие. К недостаткам следует отнести увеличение объема хранимой информации до 10-20%.

ЛИТЕРАТУРА

[1] Schiller J. I. "Secure Distributed Computing" Scientific American, v. 271, n.5 / J. I. Schiller. - Nov 1994. - P. 72-76.

[2] Schneier B."One-Way Hash Functions," Dr. Dobb's journal, v. 16, n. 9 / B. Schneier - Sep 1991. - P. 148-151.