УДК 003.26

В. О. Берников, асп. (БГТУ, г. Минск)

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ ОЦЕНКИ СТЕГАНОГРАФИЧЕСКОЙ СТОЙКОСТИ МНОГОКЛЮЧЕВОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСИТЕМЫ

Как известно, авторское право является важной составной частью универсальной системы прав человека, авторские полномочия – одно из важнейших гарантов интеллектуального творчества, самоутверждения, достоинства и заработка каждого человека. Цифровые технологии позволяют на качественно новом, более высоком уровне решать проблему авторских прав, которая в РБ относится к числу приоритетных.

Задача повышения стеганографической стойкости документов-контейнеров текстового или иного типа приобретает все большую актуальность в связи с возрастающей ролью правовых аспектов создания, размещения и использования электронного контента.

Одно из эффективных средств решения задачи повышения стеганографической стойкости документов-контейнеров текстового типа – применение эффективных методов стеганографии. При этом необходимо обеспечить требуемый уровень защищенности стеганографической системы перед несанкционированным использованием осажденной в контейнер информации. Использование различных методов стеганографии, а также криптографии, помехоустойчивого кодирования или иных методов преобразования исходных данных обеспечивает эффективное решение сформулированной задачи и может опираться на известную многоключевую модель информационной системы. Математический аппарат для описания и анализа стеганографической стойкости описываемых систем разработан слабо [1].

Разработано программное средство для оценки стеганостойкости многоключевой информационной системы. Одним из важнейших ключей многоключевой модели информационной системы является стеганографический метод для осаждения и извлечения информации. Реализованы следующие методы: на основе использования параметра апроша (изменение межбуквенного интервала), на основе цвета, на основе изменения шрифта, на основе изменения начертаний текста, а также разработан стеганографический метод на основе изменений атрибутов текста для электронных документов форматов DOC и DOCX. Предусмотрено предварительное шифрование информации на основе симметричных (алгоритмы AES и TwoFish) и асимметричных (RSA и Эль-Гамаль) криптосистем. Имеется возможность дополнительно кодировать стегосообщения на основе использования циклических ко-

дов, классического и модифицированного кодов Хемминга. Реализованы методы хеширования секретной информации на основе алгоритмов SHA512 и MD5 для проверки целостности осажденных сообщений в стеганоконтейнер. Дополнительно может быть использован ключ для псевдорандомизации секретных бит по всему электронному документу. Если данный ключ не выбран, то секретная информации будет осаждена в начало документа.

Соответствующее программное средство имеет следующие функциональные возможности:

– выбор документа, в котором будет скрываться информация;

– задание дополнительных параметров осаждения информации (предварительное криптопреобразование, кодирование, хеширование и псевдорандомизация секретных бит по всему электронному документу);

– выбор дополнительной подсветки символов в тексте, в которых осаждена информация;

– ввод сообщения, которое необходимо скрыть;

– скрытие самой секретной информации;

– просмотр электронного документа-контейнера, в котором скрыта информация;

– извлечение секретной информации;

– просмотр времени сокрытия и извлечения сообщения [2-4].

Описанное программное обеспечение реализовано на основе модели информационной системы, которая подразумевает применение практически неограниченного числа ключей. Разработанное средство используется также в учебном процессе при изучении студентами дисциплин «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации».

ЛИТЕРАТУРА

1. Берников В.О. Математическое моделирование стеганографической стойкости многоключевой системы / В.О. Берников, П.П. Урбанович // Информационные технологии: материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 г. / отв. за изд. И.В. Войтов; УО БГТУ. – Минск: БГТУ, 2019. – С. 31–33.

2. Берников В.О. Разработка стеганографических методов на основе многоключевой модели информационной системы // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях. – Гомель: ГГУ им. Ф. Скорины. – 2018. – С. 192–193.

3. Берников В.О. Сравнительный анализ криптостойкости симметричных алгоритмов шифрования // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – Минск: БГТУ, 2020. – № 1 (230). – С. 69–73.

4. Берников В. О. Метод на основе атрибутов текста в многоключевой стеганографической системе // Информационные технологии в образовании, науке и производстве: VII Международная научно-техническая интернет-конференция, 16-17 ноября 2019 г. (в печати).

УДК 004.89

А. В. Олеферович, асп.; В.В. Смелов, доц., канд. техн. наук
(БГТУ, г. Минск)

МЕТОД АВТОРИЗАЦИИ НА ОСНОВЕ РАЗЛОЖЕНИЯ ЧИСЕЛ НА ПРОСТЫЕ СОМНОЖИТЕЛИ

Построение системы информационной безопасности начинается с выявления (идентификации) субъектов и объектов информационной безопасности. В информационных системах под субъектами подразумеваются активные компоненты (пользователи, программные средства), а под объектами – пассивные компоненты системы (аппаратное обеспечение, информационные ресурсы, каналы связи, программные коды) [1].

В общем случае формальное описание системы S авторизации произвольной информационной системы может быть описано в виде тройки:

$$S = < R, U, A >,$$

где $R=\{r_1, r_2, r_3, \ldots, r_N\}$ – конечное множество объектов (ресурсов) информационной системы, доступ к которым регулируется системой авторизации S; $U=\{u_1, u_2, u_3, \ldots, u_L\}$ – конечное множество субъектов информационной системы, доступ которых к объектам R регулируется системой авторизации S; $A \subset U \times R$ – бинарное отношение, определенное на декартовом произведении $U \times R$ и такое, что если $<u,r> \in A$, то субъекту $u \in U$ разрешен доступ (привилегия) к объекту $r \in R$, бинарное отношение A может быть представлено в виде графа $G_A=<U \cup R, A>$, где $U \cup R$ – множество вершин графа; A – множество дуг. По всей видимости, построение бинарного отношения A над множеством $U \times R$ можно свести к построению характеристической функции

$$H(u,r)=\begin{cases}1, & <u,r> \in A \\ 0, & <u,r> \notin A\end{cases},$$