

различных ситуациях, в том числе при сетевых атаках.

Форма сформированных фазовых портретов позволяет судить о конкретной ситуации, наблюдаемой в сети.

Разработанная аналитическая модель позволяет изучить особенности функционирования сети как сложной динамической системы.

#### Выводы.

Разработанная аналитическая модель динамической системы, представленная векторными уравнениями, описывает процедуру формирования динамических переменных, отражающих состояние исследуемой сети. Она позволяет аналитически описать поведение системы при различных ситуациях, в том числе при сетевых атаках.

УДК 004.056.55

## МЕТОД СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В ГИБРИДНЫЙ ЗВУКОВОЙ КОНТЕЙНЕР

В статье предлагается алгоритм стеганографического преобразования информации, позволяющий осуществлять не только защиту конфиденциальных сведений, но и выявлять попытки несанкционированного доступа к внедренному в аудиоконтейнер сообщению. Вследствие того, что на сегодняшний день вопрос информационной безопасности представляет особую значимость практически во всех сферах деятельности человека, актуальность темы представленного в статье материала имеет первостепенное значение.

Стеганографический метод, аудиоконтейнер, преобразование информации, выявление попыток несанкционированного доступа.

Description of the steganographics method for modification different kinds of information is suggested in the article. It is new audio steganographics method for protection of confidential data of organizations and detection of any security attack at the audio container. The method described in this article means input binary stream for creation melodic container. Any message of the different type or format is interpreted as audio container.

Steganographics method, audio container, modification of the information, detection of security attack.

#### Введение.

Конкуренция в условиях рыночных отношений является одним из основных стимулов развития экономики предприятий. Она порождает необходимость защиты конфиденциальной информации от обнаружения ее носителей, т. е. применения в практике предприятий стеганографических методов. Возникает прагматичный вопрос: каким образом можно обеспечить скрытую передачу конфиденциальных сведений, и тем самым защитить авторские права правообладателей? Ответ на этот вопрос известен: применять методы защиты конфиденциальной информации на основе форматных и неформатных способов ее внедрения в специальные контейнеры.

Определенный научный интерес представляет процесс маскировки сигналов, содержащих конфиденциальные сведения, на основе применения аудиоинформации в интересах сокрытия данных. Сравнительный анализ современных аудиоформатов

Значения динамических переменных отображаются на двумерной плоскости в виде фазового портрета. Форма сформированного фазового портрета отображает возможные ситуации, происходящие в сети.

#### Литература

1. Блэкьер, О. Анализ нелинейных систем / О. Блэкьер. – М., 1969.
2. Бутковский, А. Г. Фазовые портреты управляемых динамических систем / А. Г. Бутковский. – М., 1985.
3. Кривулин, Н. К. Вычисление показателя Ляпунова обобщенных линейных систем с показательным распределением элементов переходной матрицы / Н. К. Кривулин // Вестник Санкт-Петербургского государственного университета. Сер. 1. – 2009. – Вып. 2. – С. 37–47.
4. Романко, В. К. Разностные уравнения / В. К. Романко. – М., 2012.

*Д. Е. Стародубцев, В. В. Плащенко*  
Череповецкий государственный университет

показал, что формат MIDI имеет ряд следующих преимуществ [1, с. 85]:

- возможность воспроизведения всеми цифровыми устройствами;
- многоканальное хранение аудиоинформации, обеспечивающее многоуровневое сокрытие данных с возможностью закладок дезинформации;
- простая аппаратная и программная реализация чтения, записи и редактирования скрытой информации.

#### Основная часть.

*Постановка задачи.* В формате MIDI требуется разработка метода сокрытия информации, позволяющего по сравнению с существующими аналогами обеспечить пропускную способность формируемого контейнера выше по сравнению с пропускной способностью подбираемых готовых контейнеров существующими методами в заданном формате.

**Методика решения.** В такой постановке задачи исследования предлагается метод, суть которого заключается в преобразовании исходного сообщения в аудиоконтейнер путем интерпретации двоичного потока сообщения в виде мелодической последовательности.

Представленный на рис. 1 алгоритм реализует процедуру интерпретации двоичного потока сообщения как некоторого мелодического контейнера, хранящегося в формате MIDI-файла. Вводимый пользователем ключ содержит в себе следующую информацию:

- матрицу инцидентности сети кодирования ( $T$ );
- вероятности отношений между состояниями сети кодирования ( $P_m$ );
- число состояний сети, используемое в одном раунде кодирования ( $n$ );

– длительность каждого состояния сети в одном раунде кодирования ( $d_n$ ).

Сообщение представляется в виде двоичного потока. Далее на основании данных ключа формируется сеть кодирования. Также с использованием информации ключа и некоторого сжимающего префиксного кода строится таблица вероятностей мелодических последовательностей, применяемых для интерпретации исходного потока сообщения на каждом раунде кодирования. Далее непосредственно осуществляется преобразование сообщения в мелодический контейнер путем сопоставления двоичных кодов и мелодических последовательностей на основании ранее построенной таблицы. После завершения процесса преобразования сообщения полученный мелодический контейнер сохраняется в файле

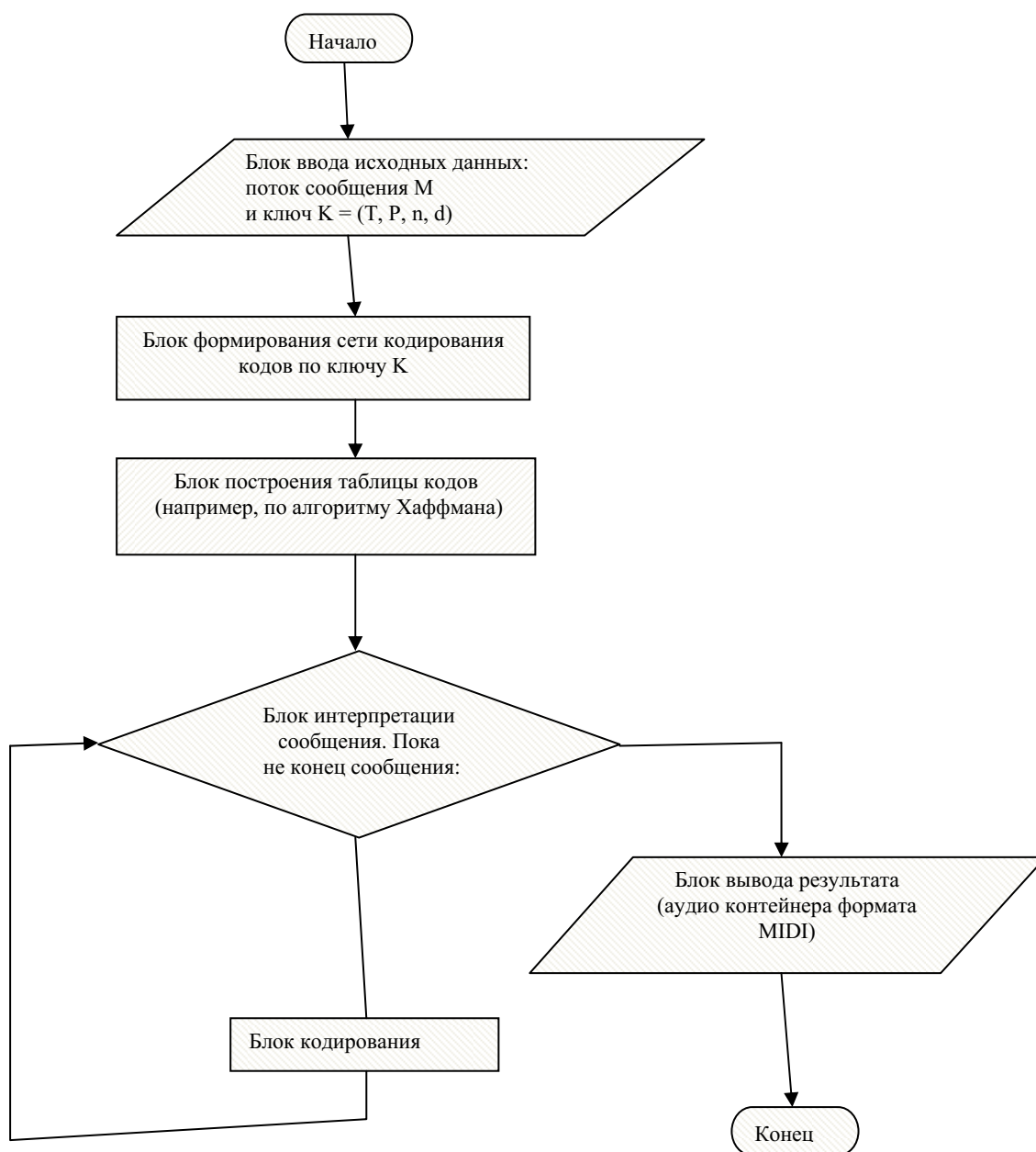


Рис. 1. Блок-схема алгоритма преобразования сообщения в аудиоконтейнер

формата MIDI. Стоит отметить, что при формировании сети кодирования недостаточно использование только лишь переходных вероятностей, определяемых ключом кодирования. Требуется вычисление стационарных вероятностей всех состояний сети кодирования. Под стационарной понимается вероятность обращения к оценке состояния в некоторый момент времени, которая определяется по следующему алгоритму:

1. Определение полной вероятности по соотношению:

$$P_1 + P_2 + P_3 + \dots + P_m = 1.$$

2. Определение стационарных вероятностей состояний сети по соотношению:

$$p_i = P_1 p_1 + P_2 p_2 + P_3 p_3 + \dots + P_m p_m,$$

где  $n$  – число состояний сети, определяемое ключом;  $m$  – число отношений, определяемое ключом;  $P_j = [1, m]$  – вероятности переходов в состояние  $n$ , определяемые ключом;  $P_i = [1, n]$  – стационарные вероятности состояний сети.

На рис. 2 представлена диаграмма пропускной способности наиболее значимых методов сокрытия информации в файлах формата MIDI. Указанная диаграмма построена на данных, полученных при сокрытии одного и того же сообщения в одинаковом контейнере тремя различными методами и его преобразованием в мелодический контейнер предлагаемым выше методом. Рис. 2 наглядно демонстрирует, что пропускная способность рассматриваемого метода (на рис. 2 столбец с пунктирным контуром) выше на 18 % по сравнению с тремя существующими методами сокрытия в формате MIDI.

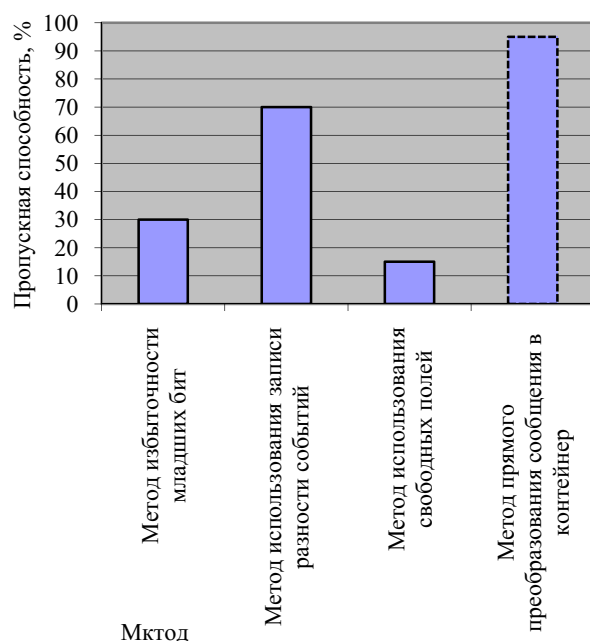


Рис. 2. Диаграмма пропускной способности методов сокрытия информации в MIDI-контейнере

Согласно классификации методов внедрения информации [2, с. 53] предлагаемый алгоритм реализует гибридный метод, суть которого заключается в преобразовании исходного сообщения в контейнер путем иной интерпретации двоичного потока сообщения. Под иной интерпретацией следует понимать совпадение неизменных блоков двоичного потока сообщения с блоками мелодического контейнера.

### Выводы.

Таким образом, предлагаемый метод по сравнению с существующими способами сокрытия информации в аудиоконтейнере формата MIDI позволяет:

- рассматривать формируемый контейнер и скрываемое сообщение как единое неделимое целое;
  - обеспечить устойчивость контейнера к статистическим стегоатакам;
  - предоставить возможность формирования многоканального контейнера;
  - увеличить пропускную способность контейнера более чем на 18 % благодаря применению сжимающего префиксного кодирования в процессе формирования контейнера;
  - создать контейнер необходимой информационной емкости, так как контейнер строится непосредственно из самого сообщения.
- В рамках предложенного метода дальнейшими направлениями исследования являются:
- определение стойкости формируемого контейнера к семантическим стегоатакам;
  - применение нейронных сетей с целью построения более естественных для восприятия человеком мелодических контейнеров;
  - определение стойкости формируемого контейнера к разрушению при передаче скрытой информации и разработке мер по ее повышению;
  - выявление альтернативных способов реализации алгоритма сокрытия с целью повышения пропускной способности формируемого контейнера.

### Литература

1. Аленин, А. А. Исследование методов обнаружения вложений в звуковых файлах формата WAV / А. А. Аленин, А. П. Алексеев // Безопасность информационных технологий, 2011. – С. 51–56.
2. Алексеев, А. П. Методы внедрения информации в звуковые файлы формата MIDI / А. П. Алексеев, А. А. Аленин // Инфокоммуникационные технологии. – 2011. – Т. 9. – С. 84–89.
3. Anderson, R., editor. Proc. Int. Workshop on Information Hiding: Lecture Notes in Computer Science / R. Anderson. – Springer-Verlag, Cambridge. 1996.
4. Anderson, R. Stretching the Limits of Steganography / R. Anderson // Information Hiding, Springer Lecture Notes in Computer Science. – 1996. – Vol. 1174. – P. 39–48.
5. Cox, J. Watermarking as communications with side information / J. Cox, M. Miller, A. McKellips // Proceedings of the IEEE. – 1999. – Vol. 87. – №7. – P. 1127–1141.
6. Fridrich, J. Steganalysis of LSB encoding in color images / J. Fridrich, R. Du, M. Long // ICME, 2000.
7. Marvel, L. Image Steganography for hidden communication. PhD Thesis / L. Marvel. – Univ. of Delaware, 1999.

8. Matsui, K. Digital signature on a facsimile document by recursive MH coding / K. Matsui, K. Tanaka and Y. Nakamura // Symposium On Cryptography and Information Security, 1989.

9. Osborne, C. A Digital Watermark / C. Osborne, R. van Schyndel, A. Tirkel // IEEE Intern. Conf. on Image Processing. – 1994. – P. 86–90.

10. Ramkumar, M. Data Hiding in Multimedia. PhD Thesis / M. Ramkumar. – New Jersey Institute of Technology, 1999.

11. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York / B. Schneier. – John Wiley and Sons, 1996.

12. Simmons, G. The History of Subliminal Channels / G. Simmons // IEEE Journal on Selected Areas of Communications. – 1998. – Vol. 16. – № 4. – P. 452–461.

13. Simmons, G. The prisoner's problem and the subliminal channel / G. Simmons // Proc. Workshop on Communications Security (Crypto'83). – 1984. – P. 51–67.

14. Voloshynovskiy, S. Attack Modelling: Towards a Second Generation Watermark Benchmark / [S. Voloshynovskiy et al.] // Preprint. University of Geneva, 2001.

УДК 621.395

**В. Л. Тамп, Н. В. Тамп**

*Череповецкое высшее военное инженерное училище радиоэлектроники,*

**А. А. Кузьмин**

*Череповецкий государственный университет*

## ИМИТАЦИОННАЯ МОДЕЛЬ ПОТОКОВ ЗАПРОСОВ НА ПЕРЕДАЧУ КАДРОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

В статье приводится описание и алгоритм имитационной модели, позволяющей формировать потоки запросов на передачу кадров в информационно-вычислительную сеть (ИВС). Предложенная модель позволяет проводить исследования ИВС для различных ситуаций, возникающих в процессе сетевых атак. Показано, что ее использование позволяет осуществлять имитацию как стандартных, так и аномальных ситуаций, возникающих в ИВС. Модель предназначена для исследования возможных путей повышения информационной безопасности вычислительных сетей.

Интенсивность, экспоненциальный закон, поток запросов, ИВС, информационная безопасность.

The article provides the algorithm and simulation model that allows to generate streams of requests for the frame transfer to the IT system. The suggested model allows the study information and computing networks, for different situations that arise during network attacks. It is shown that its use can simulate both standard and abnormal situations arising in IT system. The model is intended to explore possible ways to improve the information security of computer networks.

Intensity, exponential law, the flow of requests, information networks, information security.

### Введение.

Мониторинг информационно-вычислительных сетей показывает, что участились сетевые атаки типа «отказ в обслуживании» (*Denial of service – DoS*) различных модификаций. Существующие алгоритмы, реализованные в современных анализаторах протоколов, не обеспечивают оперативное обнаружение ряда модификаций DoS-атак. В связи с этим возникает необходимость поиска новых подходов для своевременного обнаружения атак на центральный сетевой сервер.

Известно, что разные сетевые атаки вызывают различия аномального поведения ИВС [1]. Исследование этих различий, на наш взгляд, способствует улучшению распознавания типа атаки алгоритмами анализаторов протоколов, т. е. повышают информационную безопасность сети.

Для исследования ситуаций, возникающих при сетевой атаке, предлагается имитационная модель, предназначенная формировать потоки запросов на передачу кадров в ИВС.

Известно, что алгоритмы имитационного моделирования сетевого трафика могут использовать следующие подходы [1], [4]:

– классические модели потоков, применяемые в теории массового обслуживания (экспоненциальный и пуассоновский законы распределения);

– модулированные случайные процессы (гауссов закон распределения);

– потоки с учетом статистического самоподобия сетевого трафика (фрактальные модели);

– последовательности по образцу реального трафика.

Имитационную модель сетевого трафика предлагается строить, используя параметры реального трафика.

Проводились исследования реального потока кадров, для чего фиксировались моменты времени приема каждого кадра. Объем выборки составлял 2000 значений. Гистограмма распределения длительностей между моментами начала передачи соседних кадров показана на рис. 1. Видно (а также доказывается аналитически), что полученная гистограмма аппроксимируется экспоненциальным законом распределения.