взаимодействия с окружающими их элементами и внешней средой. Это способствует постоянному расширению области применения RFID-систем и появлению новых взглядов на развитие и способы использования информационных устройств.

Актуальной является проблема обеспечения защиты информации при радиочастотной идентификации. Как и другие информационные системы, RFID-системы уязвимы и могут подвергаться атакам на различных этапах их использования. В работе проводится обзор и описание наиболее существенных для RFID-систем атак, к которым относятся: перехват, атака “человек посередине“, использование имитационных радиопомех, отказ в обслуживании, слежение, клонирование метки, вирусные атаки, SQL-инъекции, атака раскрытия секрета, атака обезличивания метки, атака обезличивания считывателя.

В данной работе рассматриваются особенности атак: клонирование метки, обезличивания метки и обезличивания считывателя и методы защиты информации при таких атаках. Для защиты информации в таких RFID- системах, характеризующихся малыми вычислительными ресурсами и энергопотреблением, предпочтение отдается сверхлегковзвешенным (ultra-lightweight) криптографическим методам.

Разработано программное обеспечение и проанализированы возможности реализации выше названных атак при использовании протокола аутентификации ULRAS. При этом нами предложено в качестве синхронизированного ключа использовать числа, генерируемые хаотическими отображениями. Применены три хаотических отображения: логистическое, косой тент, кусочно-линейное. Получены количественные параметры и приведена графическая информация, позволяющие сделать вывод, что вероятности рассмотренных атак практически не превышают значения 0,5, что свидетельствует об эффективности предложенных хаотических отображений.

Полученные результаты подтверждают целесообразность использования хаотической динамики для решения вопросов защиты информации при радиочастотной идентификации объектов.

## ПЕРЕДАЧА ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ФОРМИРУЕМЫХ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

**Сидоренко А. В., Шакинко И. В.**

*Белорусский государственный университет, Минск, Беларусь,*
*e-mail: sidorenkoA@yandex.ru*

Вследствие стремительного развития телекоммуникационных технологий, веб-приложений и интернета, передача цифровых изображений по каналам связи осуществляется в различных графических форматах.

Одним из наиболее распространенных графических форматов при передаче изображений является формат JPEG. При использовании этого формата информация об изображении хранится в виде набора коэффициентов дискретного косинусного преобразования (ДКП) [1].

Возникает необходимость в обеспечении защиты передаваемой в виде изображений информации в каналах связи. Поставленная задача решается путем добавления к цифровым изображениям особых меток, получивших название «цифровые водяные знаки» (ЦВЗ) [2]. Однако при использовании такого подхода необходимо учитывать специфические особенности соответствующего графического формата.

В данной работе рассматривается формирование цифровых водяных знаков на основе дискретных хаотических отображений для изображений, передаваемых в формате JPEG.

Особенностью предлагаемого алгоритма является возможность восстановления исходного ЦВЗ даже при модификации передаваемого изображения. Следует отметить, что успешное проведение процедуры восстановления не требует передачи по каналу связи значений параметров, используемых при формировании цифровых водяных знаков.

В работе приводятся результаты тестирования предлагаемого алгоритма формирования цифровых водяных знаков. Полученные результаты свидетельствуют о том, что рассматриваемый алгоритм позволяет не только установить факт присутствия ЦВЗ в изображении, передаваемом в формате JPEG, но и выявить те области изображения, которые подверглись модификации в канале связи.

Таким образом, разработанный алгоритм формирования ЦВЗ на основе дискретных хаотических отображений может быть применен для защиты цифровых изображений в формате JPEG при их использовании в современных веб-технологиях.

**Библиографические ссылки**

1. Cheddad, A. Digital image steganography: survey and analysis of current methods / A. Cheddad [et al] // Signal processing. – 2010. – Vol 90. – Iss. 3. – P. 727 - 752.

2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М. : Солон-Пресс, 2002 . – 265 с.

# ПРОБЛЕМЫ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ БЛОКЧЕЙН

**Шульга В. С.**

*ЭПАМ СИСТЕМЗ, Минск, Беларусь*

В 2008 году Satoshi Nakamoto опубликовал концепт электронной валюты, основанной на peer-to-peer технологии взаимодействия узлов. Через два месяца был сгененирован genesis блок в цепочке криптовалюты Bitcoin. Еще через два года, в 2011 году появится один из самых известных альтернативных инструментов на базе блокчейна – Litecoin. В 2015 году Виталий Бутерин стартовал проект Etherium что привело к экспоненциальному росту количества инструментов на базе технологии блокчейн.

Среднерыночный курс конверсии биткойна к доллару США в первые три года развития технологии составлял меньше 1 USD/BTC. Стоимость биткойна росла, со 100 USD/BTC в 2013 году до 17900 в декабре 2017-го.

С ростом стоимости биткойна росли в цене и альтернативные криптовалюты. Количество токенов на конце 2017 года составляла 1500 и продолжает расти до сих пор. За ростом стоимости биткойна росло количество упоминаний о криптовалюте в медиа. В 2017 году количество релевантных упоминаний достигло пика не только в англоязычном сегменте, но и в ресурсах, расположенных в зоне by и ru.

На базе технологии блокчейн появилось большое количество приложений, компаний и технологий. По заявлению авторов новых криптовалют, сопутствующих инструментов и деривативов каждый из новых элементов решает задачу, которую до этого никто не решал. В докладе будут рассмотрены следующие вопросы:

- Популярные тренды в медиа
  - Зарубежные медиа
  - Отечественные медиа
- Заявленные возможности криптовалют, смарт-контрактов, токенов и деривативов