

## **ОБЕСПЕЧЕНИЕ АДАПТИВНОГО УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ ДАННЫМИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ БЕСПРОВОДНОЙ СВЯЗИ МАЛОГО РАДИУСА ДЕЙСТВИЯ**

Л.Л. Утин, М.А. Сабаериан

В последние годы наблюдается устойчивая тенденция развития технологий беспроводной связи малого радиуса действия (NFC).

Технологии ближней бесконтактной связи являются одним из альтернативных решений передачи данных с мобильного телефона к приемному устройству. NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092. Эта технология может применяться:

- для обмена файлами между телефонами (отдельно либо в сочетании с каналом Bluetooth);
- эмуляции смарт-карт;
- в качестве средства оплаты за проезд в общественном транспорте;
- для открытия электронных замков в квартиру или машину;
- в качестве удостоверения личности, страховой карты и т.д.

Достоинствами данной технологии является низкое время установления связи (менее 0,1 с (для сравнения в технологии Bluetooth данный параметр равен 6 с)), сложность перехвата электромагнитного излучения злоумышленником из-за малого радиуса действия (менее 20 см), простота реализации и ряд других.

Следует отметить, что не смотря на достоинства данной технологии ей присущи определенные недостатки, которые предлагаются к обсуждению на конференции. Кроме этого предлагается к обсуждению подход по адаптивному управлению передачей данных при использовании технологий NFC.

## **ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ОПТИКО-ЭЛЕКТРОННЫХ СИСТЕМ СОПРОВОЖДЕНИЯ ОПТИЧЕСКИ НАБЛЮДАЕМЫХ ОБЪЕКТОВ В УСЛОВИЯХ ИЗМЕНЯЮЩЕЙСЯ ФОНОВО- ЦЕЛЕВОЙ ОБСТАНОВКИ**

Д.С. Шарак, Е.И. Хижняк

Интеллектуальные системы обработки и анализа видеоинформации интенсивно применяются в различных областях человеческой деятельности. Одной из задач, которые обычно интересуют потребителей оптико-электронных систем, является задача сопровождения движущихся объектов.

Необходимость разработки методов сопровождения объектов, ориентированных на системы реального времени, объясняется двумя причинами. Во-первых, исторически наибольшее развитие получили методы обработки отдельно взятых изображений, в то время как решение задач оценки параметров и сопровождения движущихся объектов, очевидно, требует анализа последовательности кадров. Во-вторых, задача измерения координат и скоростей движения объектов является традиционной для активной радио- и оптической локации, где объекты чаще всего являются точечными или малоразмерными и наблюдаются на относительно ровном фоне.

Поэтому разработка эффективных алгоритмов обработки видеопоследовательностей, ориентированных на использование в многоканальных оптико-электронных системах сопровождения объектов, является актуальной научно-исследовательской задачей.

В рамках данных исследований на кафедре Автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь» было разработано специализированное программное обеспечение, позволяющее осуществлять оценку эффективности работы алгоритмов сопровождения оптически наблюдаемых объектов.

Данное программное обеспечение включает в себя:

- модель типового корреляционного алгоритма сопровождения оптически наблюдаемых объектов;
- имитационные модели алгоритмов комплексирования цифровых видеопоследовательностей различного спектрального диапазона.

Одновременно с этим разработана имитационная модель корреляционного алгоритма сопровождения оптически наблюдаемых объектов с комплексированием первичной видеоинформации. Данный алгоритм отличается построением дополнительных корреляционных поверхностей для комплексированных изображений ИК и ТВ диапазона.

Для сравнения качества работы на вход алгоритмов сопровождения оптически наблюдаемых объектов подавались синтезированные и экспериментальные видеопоследовательности ТВ и ИК

диапазонов. Показателем качества работы алгоритмов было определено количество срывов сопровождения на 1000 кадров видеопоследовательности. Срывом сопровождения считалось отсутствие перемещения строки сопровождения в направлении движения объекта интереса в течении более 2 с.

Проведенный анализ показал существенное улучшение работы корреляционного алгоритма с комплексированием первичной видеоинформации по сравнению с типовым алгоритмом (от 33 до 83%). Результаты проведенных исследований планируется применить в автомате сопровождения системы «Адунок».

## **ПРОВЕРКА КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ В ДИАПАЗОНЕ РАБОЧИХ ТЕМПЕРАТУР**

А.М. Ярук, Н.Г. Киевец, А.В. Босак, Э.В. Машкович

В соответствии со стандартом информационных технологий и безопасности [1] одним из наиболее важных требований по генерации случайных чисел является использование физических генераторов для получения криптографических ключей. Одним из устройств, содержащих физические генераторы случайных чисел (ГСЧ), является электронная пластиковая карта (ЭПК). Интерес к применению ЭПК в криптографических системах вызван их дополнительными преимуществами: ЭПК защищены от посторонних атак и используют стандартные команды.

Так как в основе функционирования ГСЧ ЭПК лежит физический процесс, в их работе возможны сбои и отказы, возникающие в том числе под воздействием температуры окружающей среды. Для проверки качества работы генераторов ЭПК требуется статистическое тестирование их выходных последовательностей.

Для ЭПК стандартом [2] определен диапазон рабочих температур от 0 °С до 50 °С. В докладе приводятся результаты тестирования случайных последовательностей, полученных из ЭПК при температурах 0 °С, 20 °С и 50 °С. Для проверки статистических свойств последовательностей применены системы тестов FIPS 140-2 и NIST. Полученные результаты могут быть использованы при выборе ЭПК для генерации криптографических ключей.

### **Литература**

1. Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации: СТБ 34.101.27-2011. Введ. 01.03.12. Минск: Госстандарт, 2012. – 33 с.

2. Карточки идентификационные. Карточки с интегральными схемами контактные. Часть 1: СТБ 1211.1-2000 (ИСО/МЭК 7816-1:1998). – Введ. 01.07.2000. – Мн.: Госстандарт, 2000. – 4 с.