*«Приоритетные направления развития науки, технологий и техники», Нидерланды (Амстердам), 20–26 октября 2016 г.*

*Технические науки*

## ЭФФЕКТИВНОСТЬ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ CRC (32,16)

Котенко В.В., Перминов А.Е., Поляков А.И.

*Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru*

Проводилась экспериментальная оценка эффективности комплексного решения задачи защиты информации с позиций виртуализации процесса помехоустойчивого кодирования [1]в части кодирования видеоинформации помехоустойчивым кодом CRC (32,16). Оценка эффективности криптографической защиты осуществлялось путем применения апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования CRC (32,16) и базового криптографического алгоритма aes256-cbc стандарта шифрования США. Пакет NIST STS включает в себя 16 статистических тестов. Базовый алгоритм:

1) выдвигается нулевая гипотеза $H_0$ – предположение о том, что данная последовательность случайна;

2) по S вычисляется статистика теста c(S);

3) с использованием специальной функции и статистики теста вычисляется значение вероятности P = f(c(S)), P∈[0,1];

4) значение P сравнивается с уровнем a, a∈[0,001, 0,01]. Если P ≥ a, то гипотеза $H_0$ принимается. В противном случае принимается альтернативная гипотеза. Результаты криптографической оценки эффективности защиты видеоинформации приведены в таблице.

Результаты криптографической оценки эффективности защиты видеоинформации

| Алгоритм защиты | Кол-во тестов, в которых тестирование прошли более 99% последовательностей | Кол-во тестов, в которых тестирование прошли более 96% последовательностей |
|---|---|---|
| Виртуальное помехоустойчивое кодирование CRC (32,16) | 134(70%) – 148(78%) | 187(98%) – 189(100%) |
| Шифрование с помощью алгоритма aes256-cbc | 128(67%) – 147(77%) | 184(97%) – 189(100%) |

Анализ полученных результатов показывает, что реализуемая разработанным комплексом оптимальная виртуализации информационных потоков помехоустойчивого кодирования CRC (32,16) обеспечивает эффективность криптографической защиты видеоинформации, сравнимую с эффективностью современных стандартов криптографической защиты.

**Список литературы**

1. Котенко В.В. Теория виртуализации и защита телекоммуникаций: монография – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.

2. Котенко В.В. Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости / Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 140-147.

3. Котенко В.В., Котенко С.В. Идентификационный анализ криптографических алгоритмов с позиций виртуализации идентификаторов / Известия ЮФУ. Технические науки. – 2015. – № 8 (169). – С. 32-46.

4. Котенко В.В., Кертиев А.Р. Модель алгоритма шифрования с виртуализацией оценок / Международный журнал экспериментального образования. – 2015. – № 8-3. – С. 411-412.

5. Котенко В.В. Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости / Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 140-147.

6. Котенко В.В., Котенко С.В., Румянцев К.Е., Горбенко Ю.И. Стратегия защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей. Прикладная радиоэлектроника. – 2013. – Т. 12. № 3. – С. 308.

7. Котенко С.В., Котенко В.В. Методика идентификационного анализа процессов помехоустойчивого кодирования при кодировании для непрерывных каналов / Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 151-157.

8. Котенко С.В., Першин И.М., Котенко В.В. Особенности идентификационного анализа на основе информационной виртуализации изображений местоположения объектов в ГИС. Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 212-219.

9. Котенко В.В. Информационное квантование / Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 97-99.

10. Котенко В.В. Информационная оценка качества связи / Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 50-55.

11. Котенко В.В. Теоремы кодирования для дискретных каналов при передаче информации непрерывных источников / Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 184-187.

## РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ПЛАНИРОВАНИЯ И УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ И ИХ РЕЗУЛЬТАТАМИ

Назаренко М.А., Кашкин Е.В., Маркова И.А., Селиванов В.И., Макарова И.В.

*ФГБОУ ВО «Московский технологический университет», Москва, e-mail: nazarenko_maxim_anatolievich@mail.ru*

На сегодняшний день производству, которое отвечает высокому темпу развития экономики,