СРАВНИТЕЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ АУДИОИНФОРМАЦИИ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ CRC (32,16)

Котенко В.В., Кушвара Д.А., Поляков А.И.

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

Проводилась сравнительная оценка эффективности комплексного решения задачи защиты информации с позиций виртуализации процесса помехоустойчивого кодирования [1] в части кодирования аудиоинформации 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, которые разработаны для проверки гипотезы о случайности двоичных последовательностей произвольной длины. Основным принципом тестирования является проверка нулевой гипотезы H_0, заключающейся в том, что тестируемая последовательность является случайной. Все тесты направлены на выявление различных дефектов случайности. Решение о том, будет ли последовательность случайной или нет, принимается по совокупности результатов всех тестов. Результаты криптографической оценки эффективности защиты аудиоинформации приведены в таблице.

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

Результаты криптографической оценки эффективности защиты аудиоинформации

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)	135(71%) – 153(80%)	188(99%) – 189(100%)
Шифрование с помощью алгоритма aes256-cbc	129(68%) – 151(79%)	187(98%) – 189(100%)

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.