

Анализ полученных результатов показывает, что реализуемая разработанным комплексом оптимальная виртуализации информационных потоков помехоустойчивого кодирования REED-SOLOMON обеспечивает эффективность криптографической защиты аудиоинформации, 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., Котенко В.В., Румянцев К.Е., Горбенко Ю.И. Оптимизация процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Прикладная радиоэлектроника. – 2013. – Т. 12. № 3. – С. 265.
3. Котенко В.В. Основы виртуального шифрования. Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 68-75.
4. Котенко В.В. Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа. Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 96.
5. Котенко В.В., Левендян И.Б. Компьютерная технология формирования виртуального образа личности при решении задач аутентификации. Информационная безопасность регионов. – 2005. – С. 112.
6. Котенко В.В., Румянцев К.Е., Левендян И.Б., Котенко Д.В. Количественная оценка качества образовательных систем с позиций виртуализации процессов творчества и познания. Успехи современного естествознания. – 2004. – № 11. – С. 81-82.
7. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации. Информационное противодействие угрозам терроризма. – 2004. – № 2. – С. 36-42.
8. Котенко В.В. Принципы кодирования для канала с позиций виртуального представления выборочных пространств ансамблей сообщений и кодовых комбинаций. Информационное противодействие угрозам терроризма. – 2004. – № 3. – С. 65.
9. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Компьютерная технология виртуального шифрования. Современные наукоемкие технологии. – 2004. – № 2. – С. 42.
10. Котенко В.В., Поликарпов С.В. Формирование исходной проекции виртуального выборочного пространства ансамбля ключа / Известия ЮФУ. Технические науки. 2003. № 4.
11. Котенко В.В. Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Известия ЮФУ. Технические науки. – 2007. – Т. 76. – № 1. – С. 26-37.

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ REED-SOLOMON

Котенко В.В., Луданов А.Д., Писарев И.А.

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 REED-SOLOMON. Оценка эффективности криптографической защиты осуществлялась путем применения

апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования REED-SOLOMON 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 S случайна;
- 2) по S вычисляется статистика теста $c(S)$;
- 3) с использованием специальной функции и статистики теста вычисляется значение вероятности $P = f(c(S))$, $P \in [0, 1]$;
- 4) значение P сравнивается с уровнем α , $\alpha \in [0,001, 0,01]$. Если $P \geq \alpha$, 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 прошло более 99% последовательностей	Кол-во тестов, в которых тестирование прошло более 96% последовательностей
Виртуальное помехоустойчивое кодирование REED-SOLOMON	132(69%) – 151(79%)	183(96%) – 188(99%)
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 REED-SOLOMON 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., Котенко В.В., Румянцев К.Е., Горбенко Ю.И. Оптимизация процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Прикладная радиоэлектроника. – 2013. – Т. 12. № 3. – С. 265.
3. Котенко В.В. Основы виртуального шифрования. Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 68-75.
4. Котенко В.В. Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа. Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 96.
5. Котенко В.В., Левендян И.Б. Компьютерная технология формирования виртуального образа личности при решении задач аутентификации. Информационная безопасность регионов. – 2005. – С. 112.

6. Котенко В.В., Румянцев К.Е., Левендян И.Б., Котенко Д.В. Количественная оценка качества образовательных систем с позиции виртуализации процессов творчества и познания. Успехи современного естествознания. – 2004. – № 11. – С. 81-82.

7. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации Информационное противодействие угрозам терроризма. – 2004. – № 2. – С. 36-42.

8. Котенко В.В. Принципы кодирования для канала с позиций виртуального представления выборочных пространств ансамблей сообщений и кодовых комбинаций. Информационное противодействие угрозам терроризма. – 2004. – № 3. – С. 65.

9. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Компьютерная технология виртуального шифрования. Современные наукоемкие технологии. – 2004. – № 2. – С. 42.

10. Котенко В.В., Поликарпов С.В. Формирование исходной проекции виртуального выборочного пространства ансамбля ключа / Известия ЮФУ. Технические науки. 2003. № 4.

11. Котенко В.В. Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Известия ЮФУ. Технические науки. – 2007. – Т. 76. – № 1. – С. 26-37.

ЭФФЕКТИВНОСТЬ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДИСКРЕТНЫХ ИСТОЧНИКОВ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ REED-SOLOMON

Котенко В.В., Пашенко А.В., Анистратенко Р.И.

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

Исследовалась эффективность комплексного решения задачи защиты информации с позиций виртуализации процесса помехоустойчивого кодирования [1] в части кодирования дискретной информации помехоустойчивым кодом REED-SOLOMON. Оценка эффективности криптографической защиты осуществлялась путем применения апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования REED-SOLOMON 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. Все тесты направлены на выявление различных дефектов случайности. Решение о том, будет ли заданная последовательность нулей и единиц случайной или нет, принимается по совокупности результатов всех тестов. Результаты криптографической оценки эффективности защиты дискретной информации приведены в таблице.

Анализ полученных результатов показывает, что реализуемая разработанным комплексом оптимальная виртуализации информационных потоков помехоустойчивого кодирования REED-SOLOMON обеспечивает эффективность криптографической защиты дискретной информации, сравнимую с эффективностью современных стандартов криптографической защиты.

Результаты криптографической оценки эффективности защиты дискретной информации

Алгоритм защиты	Кол-во тестов, в которых тестирование прошло более 99% последовательностей	Кол-во тестов, в которых тестирование прошло более 96% последовательностей
Виртуальное помехоустойчивое кодирование REED-SOLOMON	135(71%) – 153(80%)	187(98%) – 189(100%)
Шифрование с помощью алгоритма aes256-cbc	131(69%) – 152(80%)	186(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., Кертеев 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.

ЭФФЕКТИВНОСТЬ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДИСКРЕТНЫХ ИСТОЧНИКОВ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ CRC (32,16)

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

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

Исследовалась эффективность комплексного решения задачи защиты информации с по-