

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., Левендя 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., Левендя 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., Левендя 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 HAMMING (15, 11)

Котенко В.В., Плясовских С.Д., Улещенко Д.С.

*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 HAMMING (15, 11). Оценка эффективности криптографической защиты осуществлялась путем применения апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования HAMMING (15, 11) 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.

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 HAMMING (15, 11)	129(68%) – 147(77%)	183(96%) – 185(97%)
Шифрование с помощью алгоритма aes256-cbc	131(69%) – 152(80%)	186(98%) – 189(100%)

Анализ полученных результатов показывает, что реализуемая разработанным комплексом оптимальная виртуализации информационных потоков помехоустойчивого кодирования HAMMING (15, 11) обеспечивает эффективность криптографической защиты дискретной информации, 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., Левендя 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., Левендя 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., Левендя 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.