требует значительных затрат, как умственных, так и материальных. На самом деле это не так. С помощью квалифицированных консультантов реализация системы статистического управления процессами может быть осуществлена в сжатые сроки с оптимальными вложениями.

Для этого нужно выполнить всего два базовых условия – оснастить производство современными средствами измерения, позволяющими реализовать надежное получение и передачу данных процесса, и реализовать саму систему управления. Это можно сделать на примере, одного их мировых лидеров в области разработки программных средств для реализации статистического управления производством – фирмы Q-DAS (Германия).

На первом уровне осуществляется сбор данных с помощью различных средств измерения, пригодных для измерения рассматриваемых величин и создающих значения параметров процесса в достаточном объеме и с достаточным уровнем достоверности. Для связи средств измерения с системами оценки параметров процесса и для получения данных в нужном формате применяются специализированные программные продукты (procella My.SPC и O-QIS). Отметим, что созданные фирмой Q-DAS форматы данных поддерживаются практически всеми поставщиками измерительных систем.

На втором уровне полученные данные подвергаются первичной оценке с помощью этих же программных продуктов. Результатом оценки являются параметры (показатели) процесса – ход процесса, гистограммы, контрольные карты, индексы воспроизводимости и пригодности и т.д. Эти результаты оценки могут быть представлены в различной форме в зависимости от получателя этих результатов.

На третьем этапе данные передаются в центральную базу данных.

На четвертом этапе при необходимости производится более глубокий анализ полученных данных. С помощью программного продукта solara.MP реализуется анализ пригодности средств измерения. Программный продукт qs-STAT предназначен для получения практически любых статистических оценок процесса, а программный продукт destra позволяет с применением статистических методов (например, регрессионного и вариационного анализа) оптимизировать изучаемый процесс.

На пятом уровне происходит составление отчетов по проведенным оценкам. Формы и наполнение отчетов можно изменять в зависимости от адресата получения отчета.

Наконец, шестой уровень обеспечивает архивацию полученных данных для дальнейшего хранения и проведения долгосрочного анализа.

Данные результаты получены в рамках прикладного научного исследования проводимого при финансовой поддержке Министерства образования РФ в рамках соглашения № 14.574.21.0127 от 28 ноября 2014 г. Уникальный идентификатор проекта RFMEFI57414X0127.

СРАВНИТЕЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ АУДИОИНФОРМАЦИИ ПРИ ВИРТУАЛЬНОМ ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ REED-SOLOMON

Котенко В.В., Коршунов В.А., Котенко С.В.

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 REED-SOLOMON. Оценка эффективности криптографической защиты осуществлялось 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. 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.

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 REED-SOLOMON	124(65%) – 147(77%)	186(98%) – 189(100%)
Шифрование с помощью алгоритма aes256-cbc	129(68%) – 151(79%)	187(98%) – 189(100%)

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 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.

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 осуществлялось 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 a, $a \in [0{,}001, 0{,}01]$. Если $P \geq a$, 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 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.