анализ эффективности криптографической защиты информации при виртуализации помехоустойчивого кодирования HAMMING (15, 11). Проводилось компьютерное моделирование и исследование алгоритма кодирования и алгоритма декодирования кода HAMMING (15, 11), при оптимизации информационного потока относительно условия виртуализации [1, 2, 3, 4, 5].

Оценка эффективности криптографической защиты информации осуществлялась из следующих соображений. При кодировании модуль виртуализации информационного потока (МВП) искажает кодовые комбинации и при декодировании их восстанавливает. Таким образом, для пользователей, у которых нет МВП, декодирование будет осуществляться со значительными ошибками. С позиций защиты информации эти пользователи рассматриваются как несанкционированные. При этом, чем выше будет вероятность ошибки декодирования, тем выше будет эффективность защиты. Значения вероятности ошибки декодирования без МВП для кода HAMMING (15, 11) при различных значениях задержек приведены в таблице 1. Анализ приведенных значений показывает, что виртуализация информационных потоков при кодировании кодом HAMMING (15, 11) приводит к средней вероятности ошибки декодирования, равной 0,999505. При этом минимальное значение вероятности ошибки декодирования составляет 0,999456, а максимальное – 0,998553. Полученные результаты показывают о высокой эффективности защиты информации.

Список литературы

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

2. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. – 369 с.

3. Котенко В.В. Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177–183.

4. Котенко В.В. Виртуализация процесса защиты дискретной информации // Актуальные вопросы науки: Материалы II Международной научно-практической конференции.- М.: Изд-во Спутник, 2011. – С. 36–40.

5. 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.

6. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации. // Вопросы защиты информации. – 2002. – № 2. – С. 47–51.

7. Котенко В.В., Румянцев К.Е., Поликарпов С.В. Новый подход к оценке эффективности способов шифрования с позиций теории информации // Вопросы защиты информации. – 2004. – № 1. – С. 16–22.

8. Котенко В.В., Румянцев К.Е., Юханов Ю.В., Евсеев А.С. Технологии виртуализации процессов защиты информации в компьютерных сетях // Вестник компьютерных и информационных технологий: Науч.-практ. журн., Москва. – 2007. – № 9 (39). – С. 46–56.

9. Котенко В.В. Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Сборник трудов IX Международной научно-практической конференции «Информационная безопасность». – Таганрог: – 2007. – С. 68–73.

10. Котенко В.В., Румянцев К.Е., Поликарпов С.В. Способ шифрования двоичной информации // Патент на изобретение № 2260916 РФ. Опубликовано: 20.09.2005 Бюл. № 26. С. 1–31.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ВИРТУАЛИЗАЦИИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ REED SOLOMON

Котенко В.В., Румянцев К.Е., Кудинов А.К., Писарев И.А.

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

Процесс виртуализации помехоустойчивого кодирования REED SOLOMON определяется [1] алгоритмом виртуализации кодирования (1) и алгоритмом виртуализации декодирования (2), относительно заданного условия виртуализации:

$$y_i^* = y_i + \Phi_{i\text{-}l}\left(\left(\Phi_{i\text{-}r}^{-1}\left(y_{i\text{-}r}^*\right) - \right.\right.$$

$$\left.\left. - \Phi_{i\text{-}n}^{-1}\left(y_{i\text{-}n}\right)\right) + \left(x_{i\text{-}p}^* - x_{i\text{-}j}\right)\right) \quad (1)$$

$$x_i = \Phi_i^{-1}\left(y_i^* - \Phi_{i\text{-}l}\left(\left(\Phi_{i\text{-}r}^{-1}\left(y_{i\text{-}r}^*\right) - \right.\right.\right.$$

$$\left.\left.\left. - \Phi_{i\text{-}n}^{-1}\left(y_{i\text{-}n}\right)\right) + \left(x_{i\text{-}p}^* - x_{i\text{-}j}\right)\right)\right) \quad (2)$$

Приведенные алгоритмы образуют модуль виртуализации информационного потока (МВП). При кодировании МВП искажает кодовые комбинации и при декодировании их восстанавливает. Для пользователей, у которых нет МВП, декодирование будет осуществляться со значительными ошибками. С позиций защиты информации эти пользователи рассматриваются как несанкционированные. Тогда, чем выше вероятность ошибки декодирования, тем выше будет эффективность защиты.

Значения вероятности ошибки декодирования без МВП для кода REED SOLOMON при различных значениях задержек, следующих из (1) и (2), приведены в таблице.

Вероятности ошибки декодирования кода REED SOLOMON без МВП

Линия задержки с фиксацией	1	2	3	4	5
Средняя вероятность	0,99994698	0,99994697	0,99995989	0,99995989	0,99995986

Приведенные значения показывают, что эффективность криптографической защиты при виртуализации процесса кодирования REED SOLOMON практически не зависит от выбора значений задержек. Если значения задержек трактовать как исходный ключ, то этот результат свидетельствует о потенциальной стойкости защиты. Это подкрепляется высокими значениями вероятности ошибки декодирования. Полученные результаты определяют актуальность дальнейших исследований.

Список литературы

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

2. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. –369 с.

3. Котенко В.В. Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177–183.

4. Котенко В.В. Виртуализация процесса защиты дискретной информации // Актуальные вопросы науки: Материалы II Международной научно-практической конференции. – М.: Изд-во Спутник, 2011. – С. 36–40.

5. 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.

6. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации. // Вопросы защиты информации. – 2002. – № 2. – С. 47–51.

7. Котенко В.В., Румянцев К.Е., Поликарпов С.В. Новый подход к оценке эффективности способов шифрования с позиций теории информации // Вопросы защиты информации. – 2004. – № 1. – С. 16–22.

8. Котенко В.В., Румянцев К.Е., Юханов Ю.В., Евсеев А.С. Технологии виртуализации процессов защиты информации в компьютерных сетях // Вестник компьютерных и информационных технологий: Науч.-практ. журн., Москва. – 2007. – № 9 (39). – С. 46–56.

9. Котенко В.В. Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Сборник трудов IX Международной научно-практической конференции «Информационная безопасность». – Таганрог: – 2007. – С. 68–73.

10. Котенко В.В., Румянцев К.Е., Поликарпов С.В. Способ шифрования двоичной информации // Патент на изобретение № 2260916 РФ. Опубликовано: 20.09.2005 Бюл. № 26. С. 1–31.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ CRC (32,16) ПРИ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ

Котенко В.В., Румянцев К.Е., Плясовских С.Д., Анистратенко Р.И.

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

Ставилась задача экспериментального исследования эффективности защиты информации при виртуализации [1] процесса помехоустойчивого кодирования CRC (32,16). Проводилось компьютерное моделирование и исследование алгоритма кодирования (1) и алгоритма декодирования (2) кода CRC (32, 16), при оптимизации информационного потока относительно заданного условия виртуализации:

$$y_i^* = y_i + \Phi_{i\text{-}l}\left(\left(\Phi_{i\text{-}r}^{-1}\left(y_{i\text{-}r}^*\right) - \Phi_{i\text{-}n}^{-1}\left(y_{i\text{-}n}\right)\right) + \left(x^*_{i\text{-}p} - x_{i\text{-}j}\right)\right) \quad (1)$$

$$x_i = \Phi_i^{-1}\left(y_i^* - \Phi_{i\text{-}l}\left(\left(\Phi_{i\text{-}r}^{-1}\left(y_{i\text{-}r}^*\right) - \Phi_{i\text{-}n}^{-1}\left(y_{i\text{-}n}\right)\right) + \left(x^*_{i\text{-}p} - x_{i\text{-}j}\right)\right)\right) \quad (2)$$

Приведенные алгоритмы реализуются в модуле виртуализации информационного потока (МВП). При кодировании МВП искажает кодовые комбинации и при декодировании их восстанавливает. Таким образом, для пользователей, у которых нет МВП, декодирование будет осуществляться со значительными ошибками. С позиций защиты информации эти пользователи рассматриваются как несанкционированные. Тогда, чем выше вероятность ошибки декодирования, тем выше будет эффективность защиты.

Значения вероятности ошибки декодирования без МВП для кода CRC (32, 16) при различных значениях задержек, следующих из (1) и (2), приведены в таблице.

Вероятности ошибки декодирования кода CRC (32, 16) без МВП

Линия задержки с фиксацией	1	2	3	4	5
Средняя вероятность	0,99995761	0,94995741	0,99997314	0,99997317	0,99997319

Анализ приведенных значений показывает, что эффективность криптографической защиты при виртуализации процесса кодирования CRC (32, 16) практически не зависит от выбора значений задержек. Если значения задержек трактовать как исходный ключ, то этот результат свидетельствует о потенциальной стойкости защиты. Это подкрепляется высокими значениями вероятности ошибки декодирования. Полученные результаты определяют актуальность дальнейших исследований.

Список литературы

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

2. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. – 369 с.