Технические науки

ОСОБЕННОСТИ МЕТОДИКИ ИДЕНТИФИКАЦИОННОГО АНАЛИЗА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОСНОВЕ ИНФОРМАЦИОННОЙ ВИРТУАЛИЗАЦИИ ВИДЕОИДЕНТИФИКАТОРОВ

Котенко В.В., Румянцев К.Е.,
Гапонов О.С., Евко П.П.

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

В настоящее время складывается ситуация, когда решение задачи повышения эффективности защиты объектов информатизации может быть достигнуто только путем многоуровневого комплексного применения значительного числа обнаружителей несанкционированного доступа (НСД) различных видов. То есть повышение надежности обнаружения НСД достигается путем увеличения числа различных видов обнаружителей НСД и увеличения количества уровней их комплексного применения. Возможность решения этой проблемы открывает подход, основанный на информационной виртуализации идентификаторов [1]. Методика реализации этого подхода в рамках решения задачи защиты объекта информатизации от НСД включает следующие этапы. Первый этап состоит в инъективном отображении ансамбля измеренных значений параметра видеоидентификатора в ансамбль соответствующих значений количества информации. Второй этап состоит в инъективном отображении ансамбля количества информации, соответствующего измеренным значениям параметра, в ансамбль оценок количества информации. Третий этап состоит в формировании информационных спектров параметров видеоидентификатора и определении составляющих виртуального информационного образа видеоидентификатора. Четвертый этап состоит в формировании текущего виртуального информационного образа видеоидентификатора путем унификации его составляющих. Пятый этап состоит в определении коэффициента идентичности текущего виртуального информационного образа и эталонного виртуального информационного образа, соответствующего отсутствию НСД. Определение коэффициента идентичности осуществляется путем вычисления коэффициента корреляции трехмерных изображений текущего и эталонного виртуального информационного образа. Равенство коэффициента идентичности единице будет свидетельствовать об отсутствии НСД. Любое отличие коэффициента идентичности от единицы фиксируется как наличие несанкционированного объекта.

Экспериментальные исследования варианта реализации методики показали значительное расширение возможностей защиты объектов информатизации при незначительных экономических затратах. Обеспечивается гарантированное обнаружение несанкционированный объект размером 1 мм на расстоянии 10 м. При этом, рамках области гарантированного обнаружения наблюдается изменение коэффициента идентичности в зависимости от расстояния до несанкционированного объекта и размера объекта.

Особенностью методики является отрывающаяся возможность идентификации не только самого факта НСД, но и объекта, совершающего несанкционированный доступ. Реализация этой возможности осуществляется путем задании базы данных виртуальных информационных образов объектов, способных реализовать НСД.

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.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ВИРТУАЛИЗАЦИИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ CRC (64, 32)

Котенко В.В., Миргородский С.В.,
Анистратенко Р.И., Ермолаев А.Ю.

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

Экспериментально исследовалась эффективность защиты информации в процессе виртуализации помехоустойчивого кодирования CRC (64.32). В этих целях проводилось компьютерное моделирование алгоритма кодирования (1) и алгоритма декодирования (2) кода CRC (64.32), при оптимизации информационного потока относительно условия виртуализации [1].

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

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

Вероятности ошибки декодирования кода CRC (64.32) без МВП

Линия задержки с фиксацией	1	2	3	4	5
Средняя вероятность	0,99996399	0,99996399	0,99997902	0,99997902	0,99997906

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 CRC (64.32) при различных значениях задержек, следующих из (1) и (2), приведены в таблице.

Приведенные значения показывают, что эффективность криптографической защиты при виртуализации процесса кодирования CRC (64.32) 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.

ЭФФЕКТИВНОСТЬ КРИПРОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ HAMMING (21, 16) ПРИ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ

Котенко В.В., Миргородский С.В.,
Писарев И.А., Кертиев А.Р.

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

Исследовалось комплексное решение задачи защиты информации с позиций виртуализации процесса помехоустойчивого кодирования [1]. Решение задачи осуществлялось путем применения подхода на основе оптимальной виртуализации информационных потоков в процессе кодирования HAMMING (21, 16). Проводилось компьютерное моделирование и исследование алгоритма кодирования (1) и алгоритма декодирования (2) кода HAMMING (21, 16), при оптимизации информационного потока относительно заданного условия виртуализации [1, 2, 3, 4, 5].

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

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

Виртуализация реализуется включением модуля виртуализации информационного потока, осуществляющего декодирование кодограмм исходного и виртуального информа-