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

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

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-

ционных потоков, кодирование результатов декодирования, задержки во времени кодограмм и сообщений. Это обеспечивает оптимизацию исходных преобразований кодирования и декодирования в части открывающихся возможностей комплексного обеспечения шифрования, аутентификации, имитозащиты и помехоустойчивости. Оценка эффективности защиты информации осуществлялась из следующих соображений. Включение МВП при кодировании 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. Анализ вероятности ошибки декодирования без МВП для кода HAMMING (21, 16) при различных значения задержек, что виртуализация информационных потоков при кодировании кодом HAMMING (21, 16) приводит к средней вероятности ошибки декодирования, равной 0,995329. При этом минимальное значение вероятности ошибки декодирования составляет 0,995228, а максимальное – 0,995397. Полученные результаты показывают возможность обеспечения криптографической 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.

«Внедрение новых образовательных технологий и принципов организации учебного процесса», Индонезия (о. Бали), 13–20 декабря 2015 г.

Педагогические науки

МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОЛИЯЗЫЧНОГО ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «БИОГЕОЦЕНОЛОГИЯ»

Жумабекова Б.К., Рамазанова А.С.

Павлодарский государственный педагогический институт, Павлодар, e-mail: bibigul_kz@bk.ru

По инициативе Главы государства Н.Назарбаева в стране реализуется уникальный проект – триединства языков: государственного казахского, русского и английского. С этой целью ведется большая научно-методическая работа. Выявляются факторы и основания актуализации полиязычного образования [1], формируется понятийно-терминологический фонд для теоретико-методологической концептуализации полиязычного образования [2], определяются теоретические основы полиязычного образования [3, 4], создаются учебники, учебные пособия и другое методологическое обеспечение полиязычного образования [5, 6, 7], разрабатываются проекты по научно-методическому сопровождению полиязычного образования как педагогической инновации [8], предпринимаются попытки совершенствования нормативно-правовой базы полиязычного образования [9].

С целью создания условий для полиязычного обучения на специальности 5В011300 «Биология» нами разработано учебное пособие по дисциплине «Biogeocenology» на английском языке. Основой для данной разработки послужило учебное пособие «Биогеоценология» (сост. Б.К. Жумабекова) [10]. Цель этой разработки – ознакомление студентов с основными понятиями, концепциями и проблемами биогеоценологии на английском языке, формирование у студентов системы научных знаний и создание условий для изучения материала на английском языке.

Учебное пособие разработано в рамках полиязычного образования и содержит курс лекций по биогеоценологии, контрольные вопросы