17. *Pljonkin A., Rumyantsev K.* Single-photon synchronization mode of quantum key distribution system, *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*. India, New Delhi, 2016, pp. 531-534. DOI: 10.1109/ICCTICT.2016.7514637.
18. Clavis. Plug & play quantum cryptography, *id 3000. Specifications. id Quantique SA*, Ver. 2.1. January 2005, 2 p.
19. Vectis. id 5000. Specifications, *id Quantique SA*, Ver. 1.2, April 2005, 2 p.
20. QPN 5505. User's manual, *MagiQ Technologies, Inc*., November 2004, 62 p. Available at: www.magiqtech.com.
21. *Kang Y. et al.* InGaAs-on-Si single photon avalanche photodetectors, *Appl. Phys. Lett*., 2004, Vol. 85, No. 10, pp. 1668-1670.
22. Single photon detection modules with high timing resolution and low dark count rate. Visible single-photon counters. 2016. Specifications as of January 2016. Available at: www.idquantique.com.

Статью рекомендовал к опубликованию к.т.н., доцент Е.А. Ищукова.

Румянцев Константин Евгеньевич − Южный федеральный университет; e-mail: rke2004@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Плёнкин Антон Павлович – e-mail: pljonkin@mail.ru; тел.: 89054592158; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; ассистент.

Rumyantsev Konstantin Evgen'evich – Southern Federal University; e-mail: rke2004@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Pljonkin Anton Pavlovich – e-mail: pljonkin@mail.ru; phone: +79054592158; the department of information security of telecommunication systems; cand. of eng. sc.; assistant.

УДК 621.39 DOI 10.18522/2311-3103-2016-9-1526

В.В. Котенко

ЭФФЕКТИВНОСТЬ ВИРТУАЛЬНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Проведен анализ стратегических моделей передачи и защиты информации с позиций теории виртуализации. Проведенный анализ показал возможность усовершенствования известных решений путём обеспечения криптографической эффективности кодирования на основе виртуализации информационных потоков. Отличительной особенностью виртуализации помехоустойчивого кодирования является реализованная возможность комплексного решения задач помехоустойчивости, криптографической защиты и имитостойкости. Это при сравнительно низких экономических затратах позволит существенно расширить возможности телекоммуникационных систем в части защиты информации. Виртуализация реализуется включением на выходе преобразования кодирования и на входе преобразования декодирования модуля виртуализации информационного потока, осуществляющего декодирование кодограмм исходного и виртуального информационных потоков, кодирование результатов декодирования и задержки во времени кодограмм и сообщений. Это обеспечивает оптимизацию исходных преобразований кодирования и декодирования. В работе экспериментально обоснована эффективность комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования. Экспериментально исследовались эффективность криптографической защиты, обеспечиваемая виртуальными помехоустойчивыми кодами и влияние виртуализации на эффективность исходного помехоустойчивого кода. Оценка эффективности криптографической защиты осуществлялось путем применения апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования и базового криптографического алгоритма aes256-cbc. Полученные результаты показывают, что виртуальное помехоустойчивое кодирование обеспечивает эф-

фективность криптографической защиты, сравнимую с эффективностью современных стандартов криптографической защиты, при значительно более низкой сложности практической реализации. В условиях хорошего качества связи при вероятности ошибки в канале телекоммуникации 10^{-4} виртуализация процесса помехоустойчивого кодирования не оказывает влияние на исходные свойства помехоустойчивых кодов. В условиях плохого качества связи при вероятности ошибки в канале телекоммуникации 10^{-2}–10^{-3} виртуализация процесса помехоустойчивого кодирования может оказывать влияние на исходные свойства помехоустойчивых кодов. В целом полученные результаты экспериментальных исследований показывают, что виртуализация процесса помехоустойчивого кодирования с позиций подхода, предложенного автором, открывает дополнительную возможность защиты информации в части обеспечения информационной безопасности.

Защита информации; кодирование; помехоустойчивость; шифрование; виртуализация; оптимизация; информационный поток; информационная безопасность.

V.V. Kotenko

EFFICIENCY OF VIRTUAL NOISEPROOF CODING

The analysis of strategic models of information transfer and security from the point of view of the theory of virtualization is carried out. The carried-out analysis showed a possibility of enhancement of the known decisions by ensuring cryptographic efficiency of coding on the basis of virtualization of information flows. Distinctive feature of virtualization of noiseproof coding is the realized possibility of the complex solution of tasks of noise stability, cryptographic protection and mimic resistance. In case of rather low economic costs it will permit to significantly expand the capabilities of telecommunication systems regarding information security. Virtualization is implemented by turning on at the output of coding transformation and the input of decoding transformation the module of information flow virtualization which performs decoding of patterns of initial and virtual information flows, coding of decoding results and time lags in patterns and messages. It provides an optimization of initial transformations of coding and decoding. The efficiency of the complex solution of tasks of information security from the point of view of virtualization of processes of noiseproof coding is experimentally proved herein. The efficiency of cryptographic protection provided with virtual noiseproof codes and influence of virtualization on efficiency of source noiseproof code have been experimentally studied. An efficiency evaluation of cryptographic protection has been performed by application of the approved complex of the NIST STS tests during experimental check of computer model of the virtual coding complex and the aes256-cbc basic cryptographic algorithm. The received results show that the virtual noiseproof coding provides the efficiency of cryptographic protection comparable with the efficiency of modern standards of cryptographic protection, in case of much lower complexity of practical implementation. In the conditions of high quality communication in case of probability of error in the channel of telecommunication 10^{-4} the virtualization of process of noiseproof coding does not impact on initial properties of noiseproof codes. In the conditions of bad communication quality in case of probability of error in the channel of telecommunication 10^{-2}–10^{-3} the virtualization of process of noiseproof coding can impact on initial properties of noiseproof codes. In general, the received results of pilot studies show that the virtualization of the noiseproof coding process in the light of the approach proposed herein provides additional capabilities of information security.

Information security; coding; noiseproof feature; encoding; virtualization; optimization; dataflow; information safety.

Введение. Комплексное решения задач помехоустойчивости и информационной безопасности в телекоммуникациях с позиций известных подходов представляется невозможным ввиду антагонизма стратегических целей преобразования информации: обеспечение информационной безопасности требует уменьшения избыточности, обеспечение помехоустойчивости – увеличения избыточности. Возможность решения проблемы открывает подход с позиций теории виртуализации, предложенный в [1–7]. Целью исследования является разработка и обоснование стратегии комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования.

1. Теоретическое обоснование. Согласно [1] передачу информации от источника к получателю можно представить в виде информационного потока, изначально представляющего поток сообщений $\mathbf{I[X]}$, форма которого в ходе передачи подвергается изменениям путем ответвления или добавления новых информационных потоков. При этом виртуализация предполагает оптимизацию этих потоков относительно установленного значения Q путем задания условий виртуализации. Применительно к помехоустойчивому кодированию совокупность условий виртуализации определяется как:

Условие 1. Форма информационного потока оптимальна при $I\left[X^*;Y^*\right] = Q$.

Условие 2. Средняя условная взаимная информация $\mathbf{I[X/Y]}$ однозначно характеризует прямое преобразование кодирования Φ элементов ансамбля X в элементы ансамбля Y.

Условие 3. Средняя условная взаимная информация $\mathbf{I[Y/X]}$ однозначно характеризует обратное преобразование кодирования Φ^{-1} элементов ансамбля Y в элементы ансамбля X.

Условие 4. Сумма условных взаимных информаций $I[Y/X]+I[X/Y]$ характеризует прямое преобразование кодирования Φ от обратного преобразования кодирования Φ^{-1}.

Тогда виртуализация, определяемая условием 1, состоит в инъективном отображении совместного ансамбля XY в совместный виртуальный ансамбль X^*Y^*:

$$vir(I[X;Y]) : XY \to X^*Y^*, \tag{1}$$

где общий вид процесса виртуализации характеризуется как

$$I\left[X;Y\right]+\Psi\left[I;I^*\right]=I\left[X^*;Y^*\right]. \tag{2}$$

Из (2) следует, что выполнение условия 1 требует изменения характеристики преобразования формы информационного потока на величину $\Psi\left[I;I^*\right]$, определяемую как *функционал виртуализации* [9]. Функционал $\Psi\left[I;I^*\right]$ – это числовая функция, заданная на векторном пространстве, образованном $I[X;Y]$ и $I[X^*;Y^*]$ над выборочным пространством совместного ансамбля XYX^*Y^*. Функционал берёт в качестве аргумента элемент этого векторного пространства (вектор) и возвращает в качестве результата скаляр. С позиций математики самый простой функционал – это проекция.

Функционал виртуализации, обеспечивающий оптимизацию информационного потока относительно условия 1, определяется как

$$\Psi\left[I;I^*\right]= Q - I\left[X\right]+I\left[X/Y\right]= Q - I\left[Y\right]+I\left[Y/X\right]. \tag{3}$$

Функционал виртуализации в (3) на основании теорем 1.2.4–1.2.9 в [1] формирует проекцию на область абсолютно оптимальных решений, заданную условием виртуализации 1. Задача оптимизации информационных потоков сводится к оптимизации формы представления информационного потока $\mathbf{I[Y]}$ на выходе преобразования кодирования, т.е. к определению $\mathbf{I[Y*]}$. Форма представления информационного потока $\mathbf{I[Y*]}$ может быть получена путем преобразования выражения, выведенного из (3)

$$I\left[Y\right] - I\left[Y/X\right] + Q - I\left[X\right]+I\left[X/Y\right] = I\left[Y^*\right] - I\left[Y^*/X^*\right], \tag{4}$$

к виду

$$I\left[Y^{*}\right] = I[Y]+\left(\left(I\left[Y^{*}/X^{*}\right]-I[Y/X]\right)+\left(Q-I[X]\right)\right)+I[X/Y]. \quad (5)$$

Необходимо отметить, что выражения (4) и (5) представляют формы информационных потоков, что не допускает возможность произвольного сокращения одинаковых и производных от них элементов левой и правой части равенств. Допустимость этих утверждений убедительно подкрепляется результатами экспериментальных исследований [10–19, 21–30].

Выражение (5) отражает общий вид решения задачи оптимизации формы преобразования информационного потока относительно условия 1. С этих позиций $I[Y^{*}]$ можно рассматривать как проекцию логической формы представления информационного потока [2, 21, 23] на выходе преобразования кодирования на область абсолютно оптимальных решений, заданную условием 1. Переход от (5) к материальной форме представления информационных потоков обеспечивается условиями виртуализации 2–4. Применение этих условий позволяет получить алгоритм виртуального кодирования

$$y^{*}_{i} = y_{i} + \Phi_{i\text{-}l}\left(\left(\Phi^{-1}_{i\text{-}r}\left(y^{*}_{i\text{-}r}\right)-\Phi^{-1}_{i\text{-}n}\left(y_{i\text{-}n}\right)\right)+\left(x^{*}_{i\text{-}p}-x_{i\text{-}j}\right)\right). \quad (6)$$

и алгоритм виртуального декодирования

$$x_{i} = \Phi^{-1}_{i}\left(y^{*}_{i}-\Phi_{i\text{-}l}\left(\left(\Phi^{-1}_{i\text{-}r}\left(y^{*}_{i\text{-}r}\right)-\Phi^{-1}_{i\text{-}n}\left(y_{i\text{-}n}\right)\right)+\left(x^{*}_{i\text{-}p}-x_{i\text{-}j}\right)\right)\right). \quad \textbf{(7)}$$

Анализ алгоритмов показывает, что виртуализация реализуется включением на выходе преобразования кодирования и на входе преобразования декодирования модуля виртуализации информационного потока (МВП), осуществляющего декодирование кодограмм исходного и виртуального информационных потоков, кодирование результатов декодирования и задержки во времени кодограмм и сообщений. Это обеспечивает оптимизацию исходных преобразований кодирования и декодирования, характеризуемую следующими дополнительно открывающимися возможностями. Во-первых, включение дополнительного преобразования кодирования обеспечивает возможность повышения помехоустойчивости. Применительно к цифровой идеологии современных телекоммуникаций, позволяющей реализовывать операции сложения и вычитания посредством операции сложения по модулю 2, повышение помехоустойчивости в данном случае может достигаться при неизменной исходной длине кодовых комбинаций (кодограмм). Образно говоря, осуществляется кодирование в кодировании, при этом сдвиг кодовых комбинаций повторного кодирования во времени можно трактовать как их повторную передачу. Во-вторых, появляется возможность идентификации и аутентификации источника информации. В качестве идентификатора источника при этом выступает последовательность значений задержек $lrnpj$, устанавливаемых в модуле временных задержек (ВЗ). Соответствие значений $lrnpj$ в модуле виртуализации преобразования декодирования значениям $lrnpj$, установленным в модуле виртуализации преобразования кодирования, будет свидетельствовать об истинности идентификатора источника. Образно говоря, в информационный поток вводятся индивидуальные признаки источника, и осуществляется определение их истинности при декодировании. В-третьих, сложение исходных кодограмм с кодограммами повторного кодирования можно интерпретировать как преобразование защиты информации. С этих позиций кодограммы повторного кодирования выступают в роли ключевой последовательности. При этом включение разности исходных и виртуальных сообщений в формирование этой ключевой последовательности будет обеспечивать решение задачи имитозащиты [20, 22, 25, 26].

Экспериментальная оценка эффективности полученных решений проводилась на основе компьютерного моделирования полученных алгоритмов в виде программного комплекса (рис. 1). Экспериментально исследовались: 1) эффективность криптографической защиты, обеспечиваемая виртуальным помехоустойчивым кодом; 2) влияние виртуализации на эффективность исходного помехоустойчивого кода.

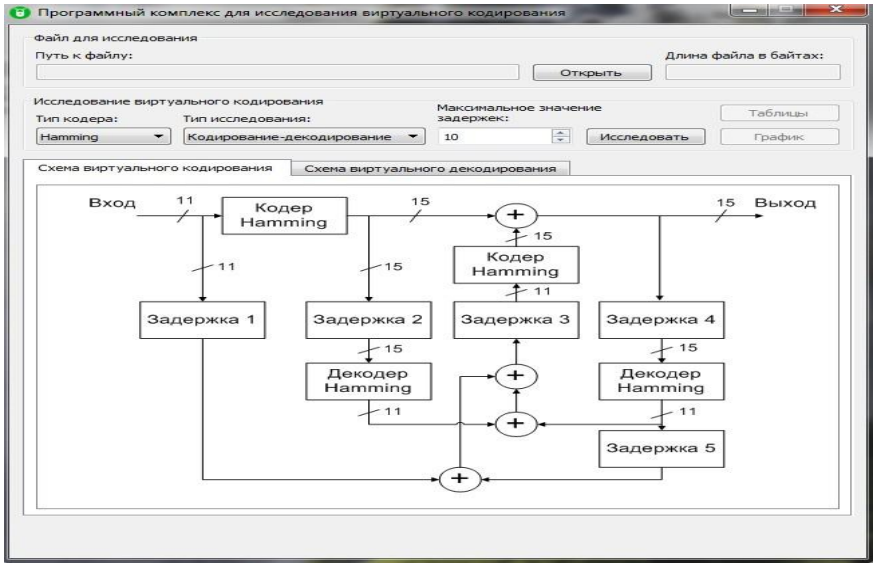


Рис. 1. Интерфейс программного комплекса исследования виртуального помехоустойчивого кодирования

2. Экспериментальное исследование эффективности криптографической защиты. Основным средством используемым настоящее время для оценки эффективности криптографических алгоритмов является комплекс тестов NIST STS.

С использованием пакета NIST STS проводилось тестирование в трех режимах виртуализации:

1. Виртуальное помехоустойчивое кодирование HAMMING (15, 11).
2. Виртуальное помехоустойчивое кодирование CRC32, полином: $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$
3. Виртуальное помехоустойчивое кодирование REED-SOLOMON.

Тестирование осуществлялось на различных форматах файлов:

1) текстовые данные (txt);

2) аудио данные (mp3) видео данные (mp4).

С целью сравнительного анализа на идентичных файлах проведено тестирование стандарта шифрования США AES (алгоритма aes256-cbc).

Для осуществления тестирования выбраны следующие параметры: длина тестируемой последовательности $n=10^6$ бит; количество тестируемых последовательностей m=100; объем тестируемой выборки $N=10^8$ бит; уровень значимости $a = 0.01$; количество тестов $q = 189$.

Таким образом, статистический портрет генератора содержит 18900 значений вероятности *P*.

В идеальном случае при $m = 100$ и $a = 0.01$ может быть отвергнута только одна последовательность из ста, т. е. коэффициент прохождения каждого теста должен составлять 99 %. Но это слишком жесткое правило. Поэтому применяется правило на основе доверительного интервала для r_j. Нижняя граница в этом случае составит значение $r_{min} = 0.96015$.

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 информации приведены в табл. 1.

Таблица 1

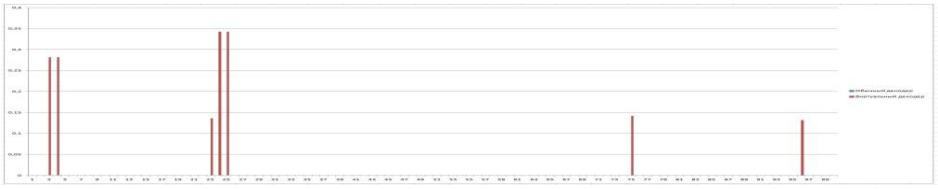
Результаты криптографической оценки эффективности защиты информации

Виртуальное помехоустойчивое кодирование, алгоритм защиты		Кол-во тестов, в которых тестирование прошли более 99% последовательностей	Кол-во тестов, в которых тестирование прошли более 96% последовательностей
HAMMING (15,11)	txt	129(68%) – 147(77%)	183(96%) – 185(97%)
HAMMING (15,11)	mp3	124(65%) – 150(79%)	182(96%) – 185(97%)
HAMMING (15,11)	mp4	122(64%)–151(79%)	183(96%) – 185(97%)
CRC32	txt	129(68%) – 151(79%)	185(97%) – 189(100%)
CRC32	mp3	135(71%) – 153(80%)	188(99%) – 189(100%)
CRC32	mp4	134(70%) – 148(78%)	187(98%) – 189(100%)
REED-SOLOMON	txt	135(71%) – 153(80%)	187(98%) – 189(100%)
REED-SOLOMON	mp3	124(65%) – 147(77%)	186(98%) – 189(100%)
REED –SOLOMON	mp4	132(69%) – 151(79%)	183(96%) – 188(99%)
Алгоритм aes256-cbc	txt	131(69%) – 152(80%)	186(98%) – 189(100%)
Алгоритм aes256-cbc	mp3	129(68%) – 151(79%)	187(98%) – 189(100%)
Алгоритм aes256-cbc	mp4	128(67%) – 147(77%)	184(97%) – 189(100%)

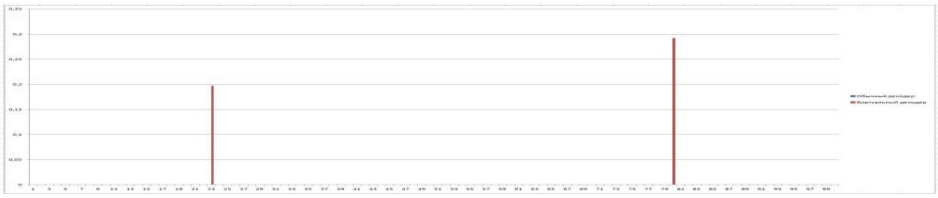
Анализ полученных результатов показывает, что виртуальное помехоустойчивое кодирование обеспечивает эффективность криптографической защиты, сравнимую с эффективностью современных стандартов криптографической защиты.

3. Экспериментальное исследование влияния виртуализации на эффективность исходного помехоустойчивого кода. Исследовалось влияние виртуализации на свойства исходных помехоустойчивых кодов. Для этого определялась вероятность ошибки декодирования при включении модуля виртуализации в условия изменения линий задержки для вероятностей ошибки в канале телекоммуникации 10^{-2}, 10^{-3},10^{-4}.

Графики вероятности ошибки декодирования для помехоустойчивых кодов HAMMING (15,11), CRC32, REED-SOLOMON приведены на рис. 2–4.

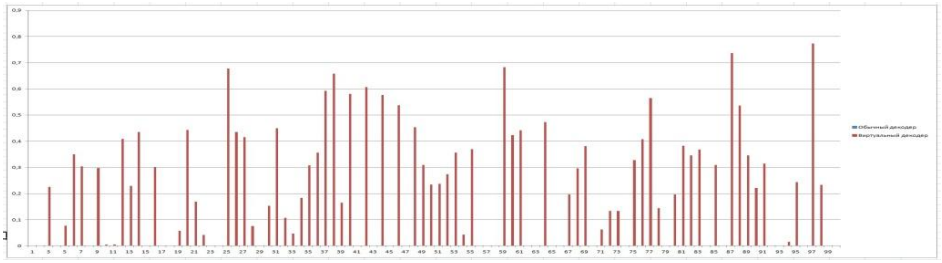


а

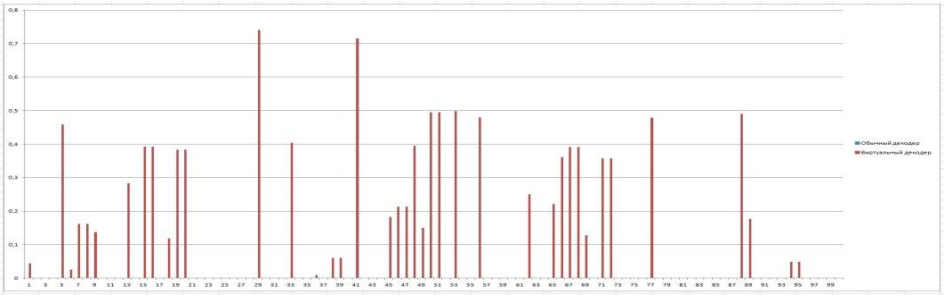


б

Рис. 2. График вероятности ошибки декодирования кода HAMMING (15,11) в условия изменения линий задержки для вероятности ошибки в канале телекоммуникации: а – 10^{-2}; б – 10^{-3}

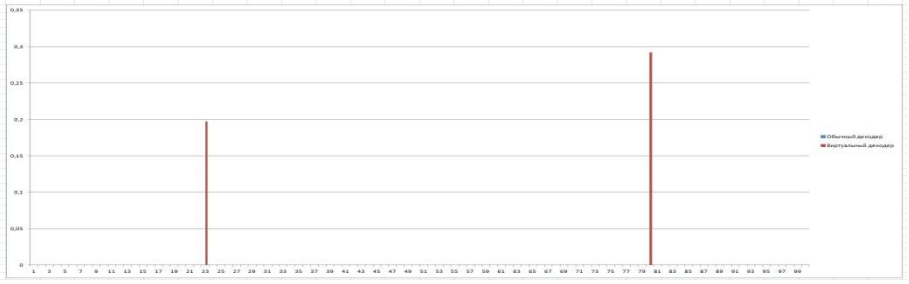


а

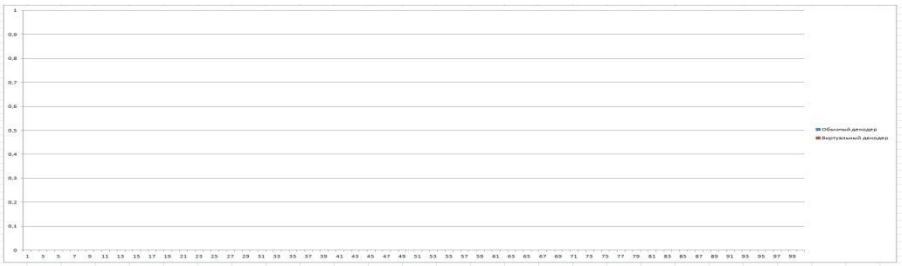


б

Рис. 3. График вероятности ошибки декодирования кода CRC32 в условия изменения линий задержки для вероятности ошибки в канале телекоммуникации: а – 10^{-2}; б – 10^{-3}



а



б

Рис. 4. График вероятности ошибки декодирования кода REED-SOLOMON в условия изменения линий задержки для вероятности ошибки в канале телекоммуникации: а – 10^{-2}; б – 10^{-3}

Из результатов проведенных исследований следует:

1. В условиях хорошего качества связи при вероятности ошибки в канале телекоммуникации 10^{-4} виртуализация процесса помехоустойчивого кодирования не оказывает влияние на исходные свойства помехоустойчивых кодов.
2. В условиях плохого качества связи при вероятности ошибки в канале телекоммуникации 10^{-2}–10^{-3} виртуализация процесса помехоустойчивого кодирования оказывает влияние на исходные свойства помехоустойчивых кодов. Для кодов CRC это влияние может быть значительным, для кодов HAMMING – менее значительным, а для кодов REED SOLOMON – практически незначительным.
3. В условиях хорошего качества связи комплекс виртуального криптографического кодирования целесообразно использовать в режимах CRC.
4. В условиях плохого качества связи комплекс виртуального криптографического кодирования целесообразно использовать в режиме REED SOLOMON.

Заключение. Отличительной особенностью виртуализации помехоустойчивого кодирования является реализованная возможность комплексного решения задач помехоустойчивого кодирования, криптографической защиты и имитостойкости. Это при сравнительно низких экономических затратах позволит существенно расширить возможности телекоммуникационных систем в части защиты информации.

В работе экспериментально обоснована эффективность комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования. Полученные результаты показывают, что виртуальное помехоустойчивое кодирование обеспечивает эффективность криптографической защиты, сравнимую с эффективностью современных стандартов криптографической защиты.

В целом полученные результаты экспериментальных исследований показывают, что виртуализация процесса помехоустойчивого кодирования с позиций подхода, предложенного в [1], открывает дополнительную возможность защиты информации в части обеспечения информационной безопасности. Это определяет целесообразность дальнейших исследований в данном направлении.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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.* Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 140-147.
4. *Котенко В.В., Котенко С.В.* Идентификационный анализ криптографических алгоритмов с позиций виртуализации идентификаторов // Известия ЮФУ. Технические науки. – 2015. – № 8 (169). – С. 32-46.
5. *Котенко В.В., Кертиев А.Р.* Модель алгоритма шифрования с виртуализацией оценок // Международный журнал экспериментального образования. – 2015. – № 8-3. – С. 411-412.
6. *Котенко В.В.* Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа // Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 96-105.
7. *Котенко В.В., Котенко С.В., Румянцев К.Е., Горбенко Ю.И.* Стратегия защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей // Прикладная радиоэлектроника. – 2013. – Т. 12, № 3. – С. 308.
8. *Котенко С.В., Котенко В.В.* Методика идентификационного анализа процессов помехоустойчивого кодирования при кодировании для непрерывных каналов // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 151-157.
9. *Котенко С.В., Першин И.М., Котенко В.В.* Особенности идентификационного анализа на основе информационной виртуализации изображений местоположения объектов в ГИС // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 212-219.
10. *Котенко В.В.* Информационное квантование // Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 97-99.
11. *Котенко В.В.* Информационная оценка качества связи // Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 50-55.
12. *Котенко В.В.* Теоремы кодирования для дискретных каналов при передаче информации непрерывных источников // Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 184-187.
13. *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.
14. *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.
15. *Котенко В.В.* Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Известия ЮФУ. Технические науки. – 2007. – № 1 (76). – С. 26-37.
16. *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.
17. *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.
18. *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. – 2007. – № 9 (39). – С. 46-56.

19. *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.
20. Пат. на изобретение № 2260916 РФ. Способ шифрования двоичной информации / Котенко В.В., Румянцев К.Е., Поликарпов С.В. Опубликовано: 20.09.2005, Бюл. № 26. – С. 1-3.
21. *Котенко В.В.* Оценка информационного образа исследуемого объекта с позиций теории виртуального познания // Известия ТРТУ. – 2006. – № 4 (48). – С. 42-48.
22. *Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б.* Компьютерная технология виртуального шифрования // Современные наукоемкие технологии. – 2004. – № 2. – С. 42.
23. *Kotenko V.V.* Information resources protection in position of information protection process virtualization with absolute uncertainty of the source // Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015. – Kirov, 2015. – P. 73-90.
24. *Kotenko S.V. Kotenko V.V. Rumyantsev K.E.* Evaluation of auricular-diagnostic identification topology effectiveness // Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015. – Kirov, 2015. – P. 91-107.
25. *Khovanskova V., Khovanskov S.* Multiagent systems: security concepts // Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015. – Kirov, 2015. – P. 167-175.
26. *Хованскоов С.А., Норкин О.Р., Парфенова, С.С. Хованскова В.С.* Алгоритмическое обеспечение распределенных вычислений с использованием иерархической вычислительной структуры // Информатизация и связь. – 2014. – № 2 (156). – С. 71-75.
27. *Котенко В.В., Котенко С.В., Ермолаев А.Ю., Крутаков Ю.Б.* Принципы идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 328-332.
28. *Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б.* Шифрование на основе многомерного представления виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97.
29. *Котенко В.В., Румянцев К.Е., Котенко С.В.* Методология идентификационного анализа инфокоммуникационных систем: монография. – Ростов-на-Дону: Изд-во ЮФУ, 2014. – 226 с.

REFERENCES

1. *Kotenko V.V.* Teoriya virtualizatsii i zashchita telekommunikatsiy: monografiya [The theory of virtualization and protection of telecommunications: monograph]. Taganrog: Izd-vo TTI YuFU, 2011, 244 p.
2. *Kotenko V.V., Rumyantsev K.E.* Teoriya informatsii i zashchita telekommunikatsiy: monografiya [Theory of Information and Protection of telecommunications: monograph]. Rostov-on-Don: Izd-vo YuFU, 2009, 369 p.
3. *Kotenko V.V.* Virtualizatsiya protsessa zashchity nepreryvnoy informatsii otnositel'no usloviy teoreticheskoy nedeshifruemosti [Virtualization continuous data protection process with respect to the theoretical conditions nedeshifruemosti], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2013, No. 20, pp. 140-147.
4. *Kotenko V.V., Kotenko S.V.* Identifikatsionnyy analiz kriptograficheskikh algoritmov s pozitsiy virtualizatsii identifikatorov [Identification analysis of cryptographic algorithms from the point of virtualization IDs], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 8 (169), pp. 32-46.
5. *Kotenko V.V., Kertiev A.R.* Model' algoritma shifrovaniya s virtualizatsiey otsenok [Model of cryptoalgorithm with the virtualization of estimations], *Mezhdunarodnyy zhurnal eksperimental'nogo obrazovaniya* [The International magazine of experimental education], 2015, No. 8-3, pp. 411-412.

6. *Kotenko V.V.* Virtualizatsiya zashchity diskretnoy informatsii otnositel'no usloviy neproduktivnosti analiza klyucha [Virtualization protect digital information on the conditions unproductive analysis key], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2011, No. 17, pp. 96-105.
7. *Kotenko V.V., Kotenko S.V., Rumyantsev K.E., Gorbenko Yu.I.* Strategiya zashchity nepreryvnoy informatsii s pozitsiy virtualizatsii ansamblya klyuchey na formal'nye otnosheniya ansambley [Continuous data protection strategy with a key position in the band virtualization formal relations ensembles], *Prikladnaya radioelektronika* [Applied electronics], 2013, Vol. 12, No. 3, pp. 308.
8. *Kotenko S.V., Kotenko V.V.* Metodika identifikatsionnogo analiza protsessov pomekhoustoychivogo kodirovaniya pri kodirovanii dlya nepreryvnykh kanalov [Methods of identification analysis of error-correcting coding in encoding processes for continuous channel], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2013, No. 20, pp. 151-157.
9. *Kotenko S.V., Pershin I.M., Kotenko V.V.* Osobennosti identifikatsionnogo analiza na osnove informatsionnoy virtualizatsii izobrazheniy mestopolozheniya ob"ektov v GIS [Features of identification analysis on the basis of information in the GIS objects virtualization location images], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 212-219.
10. *Kotenko V.V.* Informatsionnoe kvantovanie [Information quantization], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2007, No. 9, pp. 97-99.
11. *Kotenko V.V.* Informatsionnaya otsenka kachestva svyazi [Information evaluation of the quality of communication], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2007, No. 9, pp. 50-55.
12. *Kotenko V.V.* Teoremy kodirovaniya dlya diskretnykh kanalov pri peredache informatsii nepreryvnykh istochnikov [Coding theorem for discrete channel with continuous transfer of information sources], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter the threats of terrorism], 2007, No. 9, pp. 184-187.
13. *Kotenko V.V.* Teoreticheskoe obosnovanie virtual'nykh otsenok v zashchishchennykh telekommunikatsiyakh [The theoretical justification of virtual assessments of protected telecommunications], *Materialy XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [XI International scientific-practical conference "Information Security"]. Part 1. Taganrog: Izd-vo TTI YuFU, 2010, pp. 177-183.
14. *Kotenko V.V.* Virtualizatsiya protsessa zashchity diskretnoy informatsii [Virtualization is the process of protecting digital information], *Aktual'nye voprosy nauki: Materialy II Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Actual questions of science: Proceedings of the II International Scientific and Practical conference]. Moscow: Izd-vo Sputnik, 2011, pp. 36-40.
15. *Kotenko V.V.* Strategiya primeneniya teorii virtualizatsii informatsionnykh potokov pri reshenii zadach informatsionnoy bezopasnosti [The strategy of applying the theory of the virtualization of information flows for solving information security], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2007, No. 1 (76), pp. 26-37.
16. *Kotenko V.V., Polikarpov S.V.* Strategiya formirovaniya virtual'nykh vyborochnykh prostranstv ansambley klyucha pri reshenii zadach zashchity informatsii [The strategy of forming virtual sample spaces ensembles key in solving the problems of information security], *Voprosy zashchity informatsii* [Problems of information security], 2002, No. 2, pp. 47-51.
17. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V.* Novyy podkhod k otsenke effektivnosti sposobov shifrovaniya s pozitsiy teorii informatsii [A new approach to assessing the effectiveness of encryption methods from the standpoint of information theory], *Voprosy zashchity informatsii* [Questions of information security], 2004, No. 1, pp. 16-22.
18. *Kotenko V.V., Rumyantsev K.E., Yukhanov Yu.V., Evseev A.S.* Tekhnologii virtualizatsii protsessov zashchity informatsii v komp'yuternykh setyakh [Virtualization technologies of information security processes in computer networks], *Vestnik komp'yuternykh i informatsionnykh tekhnologiy* [Herald of computer and information technologies], 2007, No. 9 (39), pp. 46-56.

19. *Kotenko V.V.* Strategiya primeneniya teorii virtualizatsii informatsionnykh potokov pri reshenii zadach informatsionnoy bezopasnosti [The strategy of applying the theory of the virtualization of information flows for solving information security], *Sbornik trudov IX Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceedings of the IX International scientific-practical conference "Information Security"]. Taganrog, 2007, pp. 68-73.
20. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V.* Sposob shifrovaniya dvoichnoy informatsii [A method of encrypting binary data]. Patent for the invention No. 2260916 Russian Federation. Published: 20.09.2005, Bull. No. 26, pp. 1-3.
21. *Kotenko V.V.* Otsenka informatsionnogo obraza issleduemogo ob"ekta s pozitsiy teorii virtual'nogo poznaniya [Evaluation of the information of the image of the object from the point of virtual knowledge theory*], Izvestiya TRTU* [Izvestiya TSURE], 2006, No. 4 (48), pp. 42-48.
22. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V., Levendyan I.B.* Komp'yuternaya tekhnologiya virtual'nogo shifrovaniya [Virtual Computer encryption technology], *Sovremennye naukoemkie tekhnologii* [Modern high technologies], 2004, No. 2, pp. 42.
23. *Kotenko V.V.* Information resources protection in position of information protection process virtualization with absolute uncertainty of the source, *Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015*. Kirov, 2015, pp. 73-90.
24. *Kotenko S.V. Kotenko V.V. Rumyantsev K.E.* Evaluation of auricular-diagnostic identification topology effectiveness, *Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015*. Kirov, 2015, pp. 91-107.
25. *Khovanskova V., Khovanskov S.* Multiagent systems: security concepts, *Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27–28 March 2015*. Kirov, 2015, pp. 167-175.
26. *Khovanskov S.A., Norkin O.R., Parfenova, S.S. Khovanskova V.S.* Algoritmicheskoe obespechenie raspredelennykh vychisleniy s ispol'zovaniem ierarkhicheskoy vychislitel'noy struktury [Algorithmic support distributed computing using hierarchical computing structure], *Informatizatsiya i svyaz'* [Informatization and Communication], 2014, No. 2 (156), pp. 71-75.
27. *Kotenko V.V., Kotenko S.V., Ermolaev A.Yu., Krutakov Yu.B.* Printsipy identifikatsi-onnogo analiza kriptograficheskikh algoritmov s pozitsiy informatsionnykh identifikatorov protsessa shifrovaniya [Principles of identification analysis of cryptographic algorithms from the position information of the encryption process identifiers], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter terrorism threats], 2014, No. 23, pp. 328-332.
28. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V., Levendyan I.B.* Shifrovanie na osnove mnogomernogo predstavleniya virtual'nykh vyborochnykh prostranstv ansambley klyucha [Encryption is based on a multi-dimensional representation of a virtual sample spaces key ensembles], *Fundamental'nye issledovaniya* [Basic research], 2004, No. 5, pp. 97.
29. *Kotenko V.V., Rumyantsev K.E., Kotenko S.V.* Metodologiya identifikatsionnogo analiza infokommunikatsionnykh sistem: monografiya [Methodology of identification analysis of communication systems: monograph]. Rostov-on-Don: Izd-vo YuFU, 2014, 226 p.

Статью рекомендовал к опубликованию к.т.н., доцент Е.С. Абрамов.

Котенко Владимир Владимирович – Южный федеральный университет; e-mail: virtsecurity@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634315507; кафедра ИБТКС; доцент.

Kotenko Vladimir Vladimirovich – Southern Federal University; e-mail: virtsecurity@mail.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634315507; the department IBTKS; assistant professor.