

17. *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.
18. *Kotenko V.V., Kotenko S.V., Ermolaev A.Yu., Krutakov Yu.B.* Printsipy identifikatsionnogo 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.
19. *Kotenko V.V., Pershin I.M., Kotenko S.V.* Osobennosti identifikatsionnogo analiza na osnove informatsionnoy virtualizatsii izobrazheniy mestopolozheniya ob"ektov v GIS [Features of the analysis based on the identification information of virtualization image the location of objects in the GIS], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 212-219.
20. *Kotenko V.V., Polikarpov S.V.* Metodika sinteza algoritmov opredeleniya virtual'noy otsenki [Methodology of synthesis of algorithms of determination of virtual estimation], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counter Terrorism Threats], 2003, No. 1, pp. 54-58.

Статью рекомендовал к опубликованию д.т.н. И.И. Сныткин.

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

**Котенко Станислав Владимирович** – e-mail: virtsecurity@mail.ru; кафедра ИБТКС; аспирант.

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

**Kotenko Stanislav Vladimirovich** – e-mail: virtsecurity@mail.ru; the department IBTKS; post-graduate student.

УДК 621.39

**В.В. Котенко, М.Ю. Лукин, С.В. Миргородский**

### **СТРАТЕГИЯ КОМПЛЕКСНОГО РЕШЕНИЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ПРОЦЕССОВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ\***

*Предлагается оригинальное решение проблемы комплексного решения задач обеспечения информационной безопасности и помехоустойчивости. С позиций известных подходов решение этой проблемы не представляется возможным ввиду антагонизма стратегических целей преобразования информации при обеспечении информационной безопасности и обеспечении помехоустойчивости. Возможность решения проблемы открывает подход с позиций теории виртуализации. Целью исследования является разработка стратегии комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования. На основе теоретического обоснования условий виртуализации осуществляется синтез алгоритмов и моделей кодирования, оптимизирующего комплексное решение задач обеспечения информационной безопасности и помехоустойчивости относительно условия виртуализации. Виртуализация реализуется включением модуля виртуализации информационного потока, осуществляющего декодирование кодограмм исходного и виртуального информационных потоков, кодирование результатов декодирования, задержки во времени кодограмм и сообщений. Это обеспечивает оптимизацию исходных преобразований кодирования и декодирования в части*

\* Работа выполнена на основе гос. задания Минобрнауки РФ № 213.01-11/2014-9.

*открывающихся возможностей комплексного обеспечения шифрования, аутентификации, имитозащиты и помехоустойчивости. Компьютерная реализация предложенных алгоритмов и моделей в виде программного комплекса позволила произвести экспериментальный анализ предложенного подхода.*

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

V.V. Kotenko, M.J. Lukin, S.V. Mirgorodsky

## STRATEGY OF DECISION OF TASKS OF DEFENCE OF INFORMATION FROM POSITIONS OF VIRTUALIZATION OF PROCESSES OF ANTIJAMMING ENCRYPTION

*Original solution of problem of complex decision of tasks of providing of informative safety and antijammingness is offered. From positions of well-known approaches the decision of this problem is not possible because of antagonism of strategic aims of transformation of information at providing of informative safety and providing of antijammingness. Possibility of decision of problem opens approach from positions of theory of virtualization. A research aim is development of strategy of complex decision of tasks of defence of information from positions of virtualization of processes of antijamming encryption. On the basis of theoretical ground of terms of virtualization the synthesis of algorithms and models of encryption optimizing the complex decision of tasks of providing of informative safety and antijammingness in relation to the condition of virtualization comes true. A virtualization will be realized by including of the module of virtualization of dataflow, carrying out decoding of codegrams initial and virtual dataflows, encryption of results of decoding, delays in time of codegrams and reports. It provides optimization of initial transformations of encryption and decoding in part of the opened possibilities of the complex providing of encipherement, authentication, imitozashchity and antijammingness. Computer realization of offer algorithms and models as a programmatic complex allowed to make an experimental analysis offered approach.*

*Defense of information; encryption; antijammingness; encipherement; virtualization; optimization; dataflow; informative safety.*

**Введение.** Традиционно решение задач защиты информации в телекоммуникациях принято разделять на два основных направления: 1) защита от несанкционированного доступа (обеспечение информационной безопасности); 2) защита от помех (обеспечение помехоустойчивости). Задачи первого направления решаются в процессе кодирования источников, задачи второго направления – в процессе кодирования для каналов. Комплексное решения задач отмеченных направлений с позиций известных подходов невозможно ввиду антагонизма стратегических целей преобразования информации: обеспечение информационной безопасности требует уменьшения избыточности, обеспечение помехоустойчивости – увеличения избыточности. Возможность решения проблемы открывает предложенный Котенко В.В. подход с позиций теории виртуализации [1]. Целью исследования является разработка и обоснование стратегии комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования.

**1. Теоретическое обоснование подхода.** Передачу информации от источника к получателю можно представить в виде информационного потока, изначально представляющего поток сообщений. Согласно принятой общей модели передачи информации [1], форма этого потока в ходе передачи подвергается изменениям. Эти изменения вызываются предусмотренными преобразованиями кодирования источника или кодирования для канала. В общем виде форма информационного потока на выходе источника информации характеризуется средним количеством информации  $I[X]$  ансамбля сообщений источника, который в зависимости от вида источника может быть дискретным или непрерывным. В ходе преобразова-

ния кодирования  $\Phi$  ансамбль источника преобразуется к форме ансамбля кодограмм  $Y$ . Таким образом, процесс изменения формы информационного потока характеризуется выражением

$$I[X;Y] = I[X] - I[X/Y], \quad (1)$$

где  $I[X/Y]$  однозначно характеризует преобразование  $\Phi$ , описываемое как инъективное отображение элементов ансамбля  $X$  в элементы ансамбля  $Y$ :

$$\Phi: X \rightarrow Y. \quad (2)$$

Преобразование (1.64) считается прямым преобразованием. Тогда преобразование элементов ансамбля кодограмм в элементы ансамбля сообщений определяется как обратное преобразование:

$$\Phi^{-1}: Y \rightarrow X.$$

Учитывая свойство симметричности средней взаимной информации в (1), обратное преобразование  $\Phi^{-1}$  однозначно характеризуется средней условной информацией  $I[Y/X]$ .

Пусть ставится задача оптимизации изменения формы информационного потока относительно некоторого известного условия

$$I[X^*;Y^*] = Q. \quad (3)$$

С позиций теории виртуализации условие (3) определяет условие виртуализации 1.

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

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

$$vir(I[X;Y]): XY \rightarrow X^*Y^*, \quad (4)$$

где общий вид процесса виртуализации характеризуется как

$$I[X;Y] + \Psi[I;I^*] = I[X^*;Y^*]. \quad (5)$$

Из (5) следует, что выполнение условия (3) требует изменения характеристики преобразования формы информационного потока (1) на величину  $\Psi[I;I^*]$ , определяемую как *функционал виртуализации*. Функционал  $\Psi[I;I^*]$  – 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.

**Теорема 1.** Пусть  $I[X;Y]$  – характеристика изменения формы информационного потока. Тогда, если условие виртуализации  $I[X^*;Y^*] = Q$ , то функционал виртуализации, обеспечивающий оптимизацию информационного потока относительно данного условия, определяется как

$$\Psi[I;I^*] = Q - I[X] + I[X/Y] = Q - I[Y] + I[Y/X]. \quad (6)$$

*Доказательство.* Выражение (6) можно привести к виду

$$\Psi[I;I^*] = I[X^*;Y^*] - I[X;Y]. \quad (7)$$

Подставив в (7) выражения (1.63) и (1.65) для  $I[X;Y]$  и  $I[X^*;Y^*]$ , получаем

$$\Psi[I; I^*] = Q - I[X] + I[X/Y]. \quad (8)$$

Учитывая свойство симметричности взаимной информации, имеем

$$I[X; Y] = I[Y; X] = I[Y] - I[Y/X]. \quad (9)$$

Подставив (3) и (9) в (7), получаем

$$\Psi[I; I^*] = Q - I[Y] + I[Y/X]. \quad (10)$$

Что и требовалось доказать.

Функционал виртуализации в (5) на основании теорем 1.2.4–1.2.9 в [1] формирует проекцию на область абсолютно оптимальных решений, заданную условием виртуализации 1 (2).

Учитывая, что ансамбль является ансамблем источника, задача оптимизации информационного потока сводится к оптимизации формы представления информационного потока на выходе преобразования кодирования  $I[Y]$ , т.е. к определению  $I[Y^*]$ . Подставив в (5) выражение для функционала виртуализации (8) и преобразовав  $I[X^*; Y^*]$  на основании свойства симметричности взаимной информации, получим:

$$I[Y] - I[Y/X] + Q - I[X] + I[X/Y] = I[Y^*] - I[Y^*/X^*], \quad (11)$$

Откуда

$$I[Y^*] = I[Y] + (I[Y^*/X^*] - I[Y/X]) + (Q - I[X]) + I[X/Y]. \quad (12)$$

Выражение отражает общий вид решения задачи оптимизации формы преобразования информационного потока относительно условия 1. С этих позиций  $I[Y^*]$  можно рассматривать как проекцию формы представления информационного потока на выходе преобразования кодирования на область абсолютно оптимальных решений, заданную условием 1. Переход от общего решения (12) к конкретным решениям обеспечивается введением следующих условий виртуализации.

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

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

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

**2. Алгоритм и модель кодирования.** Условия виртуализации 2–4 открывают возможность проекции общего решения (12) на выборочное пространство совместного ансамбля  $XYX^*Y^*$ . Осуществив привязку этой проекции ко времени, окончательно получаем:

$$y_i^* = y_i + \Phi_{i-l} \left( \left( \Phi_{i-r}^{-1}(y_{i-r}^*) - \Phi_{i-n}^{-1}(y_{i-n}) \right) + (q_{i-p} - x_{i-j}) \right). \quad (13)$$

Выражение (13) представляет общий алгоритм помехоустойчивого кодирования, обеспечивающий оптимизацию комплексного решения задач обеспечения информационной безопасности и обеспечения помехоустойчивости относительно общего вида условия оптимизации (3).

Конкретизация условия оптимизации осуществляется путем конкретизации  $Q$  в (3). Так, пусть  $Q = I[X^*]$ . Тогда выражение (13) приводится к виду

$$y_i^* = y_i + \Phi_{i-l} \left( \left( \Phi_{i-r}^{-1} (y_{i-r}^*) - \Phi_{i-n}^{-1} (y_{i-n}) \right) + (x_{i-p}^* - x_{i-j}) \right). \quad (14)$$

Выражение (14) представляет алгоритм кодирования, обеспечивающий оптимизацию информационного потока относительно условия  $Q = I[X^*]$ . Модель кодирования, соответствующая этому алгоритму для  $r = p$ , приведена на рис. 1.

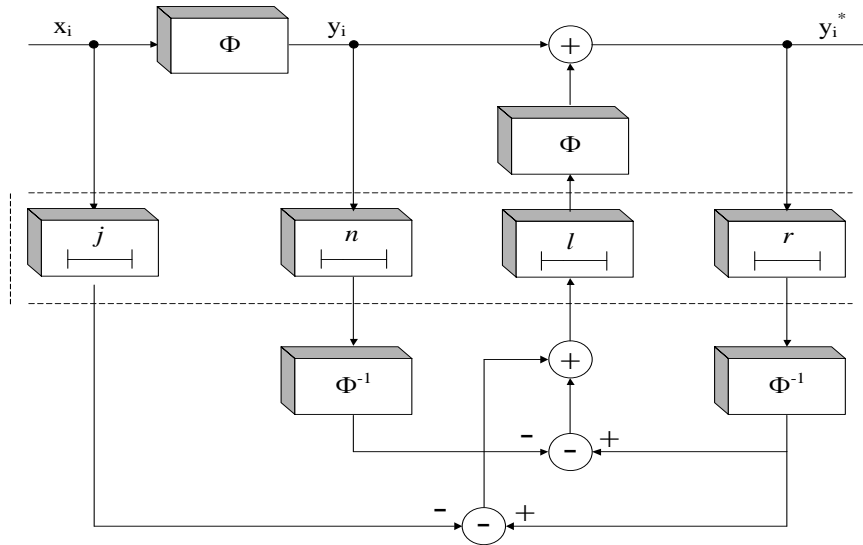


Рис. 1. Модель кодирования, оптимизирующего комплексное решение задач обеспечения информационной безопасности и помехоустойчивости относительно условия виртуализации  $Q = I[X^*]$

**3. Алгоритм и модель декодирования.** Девиртуализация, определяемая условием (3), состоит в инъективном отображении совместного ансамбля  $X^*Y^*$  в совместный ансамбль  $XY$ :

$$dvir(I[X^*; Y^*]): X^*Y^* \rightarrow XY, \quad (15)$$

где общий вид процесса виртуализации характеризуется как

$$I[X^*; Y^*] - \Psi[I; I^*] = I[X; Y]. \quad (16)$$

Функционал виртуализации в (16) формирует проекцию области абсолютно оптимальных решений, заданную условием виртуализации 1, на область решений, определенную постановкой задачи. Подставив в (16) выражение для функционала виртуализации (8), получим общий вид решения задачи девиртуализации оптимальной формы представления информационного потока на входе преобразования декодирования относительно условия 1:

$$I[Y] = I[Y^*] - \left[ \left( I[Y^*/X^*] - I[Y/X] \right) + (Q - I[X]) + I[X/Y] \right]. \quad (17)$$

Применив к (17) условия виртуализации 2–4 и осуществив привязку ко времени, получаем:

$$y_i = y_i^* - \Phi_{i-l} \left( \left( \Phi_{i-r}^{-1} (y_{i-r}^*) - \Phi_{i-n}^{-1} (y_{i-n}) \right) + (x_{i-p}^* - x_{i-j}) \right). \quad (18)$$

Принимая во внимание, что  $x_i = \Phi_i^{-1}(y_i)$ , окончательно имеем:

$$x_i = \Phi_i^{-1} \left( y_i^* - \Phi_{i-l} \left( \left( \Phi_{i-r}^{-1} (y_{i-r}^*) - \Phi_{i-n}^{-1} (y_{i-n}) \right) + (x_{i-p}^* - x_{i-j}) \right) \right). \quad (19)$$

Выражение (19) представляет алгоритм декодирования, оптимизирующий комплексное решение задач обеспечения информационной безопасности и помехоустойчивости относительно условия  $Q = I[X^*]$ . Модель декодирования, соответствующая этому алгоритму для  $r = p$ , приведена на рис. 2.

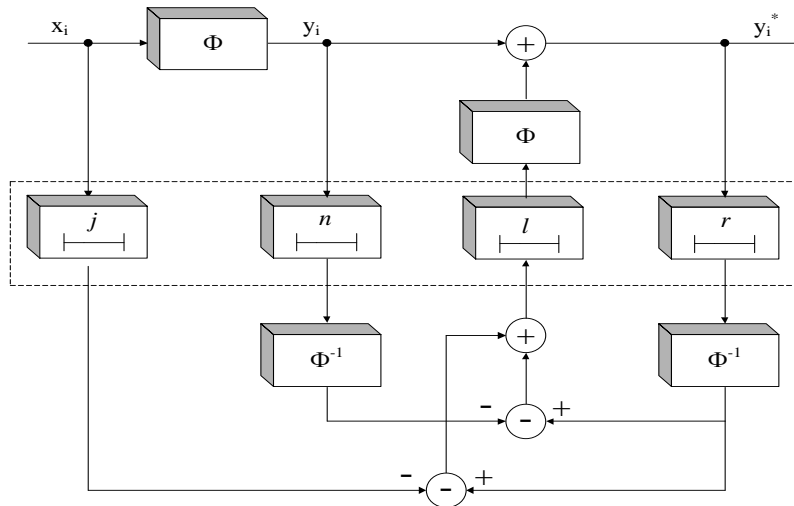


Рис. 2. Модель декодирования, оптимизирующего комплексное решение задач обеспечения информационной безопасности и помехоустойчивости относительно условия виртуализации  $Q = I[X^*]$

**4. Анализ моделей кодирования и декодирования.** Анализ моделей рис. 2 и 3 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, характеризующуюся 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 деко-

дирования значениям  $lmpj$ , 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.

Приведенный вариант конкретизации общего вида решения задач оптимизации формы преобразований информационного потока на выходе преобразования кодирования (14) и на входе преобразования декодирования (19) показывает значительные потенциальные возможности подхода, основанного на виртуализации информационных потоков.

### 5. Экспериментальный анализ

Компьютерная реализация предложенных алгоритмов и моделей в виде программного комплекса (рис. 3) позволила произвести экспериментальный анализ предложенного подхода. Анализ эффективности защиты информации осуществлялся из следующих соображений.

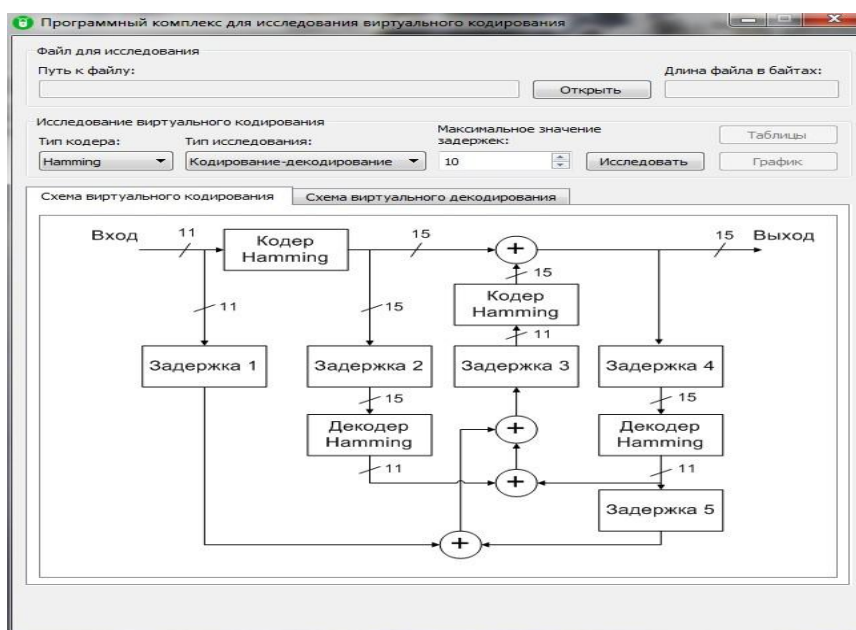


Рис. 3. Интерфейс программного комплекса исследования виртуального помехоустойчивого кодирования

Вполне понятно, что 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. Значения вероятности ошибки декодирования без МВП для кода CRC (16, 8) при различных значениях задержек приведены в табл. 1.

Анализ приведенных значений показывает, что виртуализация информационных потоков при кодировании кодом CRC (16, 8) приводит к средней вероятности ошибки декодирования, равной 0,996088. При этом минимальное значение вероятности ошибки декодирования составляет 0,995878, а максимальное – 0,996220.

Таблица 1

**Эффективность кода CRC8 (16, 8)**

Значения задержек		Значение задержки Z4									
Z1, Z2, Z3, Z5		1	2	3	4	5	6	7	8	9	10
1	0,996134	0,996147	0,996057	0,996122	0,996099	0,996036	0,99616	0,996046	0,996065	0,99613	
2	0,996002	0,996122	0,996072	0,996117	0,996138	0,996088	0,996096	0,996068	0,996124	0,996035	
3	0,99607	0,996175	0,996004	0,996119	0,99609	0,996025	0,996108	0,9961	0,996079	0,996036	
4	0,996187	0,99612	0,996105	0,995878	0,996048	0,996071	0,996127	0,996094	0,996041	0,996108	
5	0,996023	0,996067	0,996192	0,996023	0,995984	0,99622	0,996091	0,996074	0,996141	0,996074	
6	0,996055	0,996081	0,996146	0,996143	0,996056	0,996044	0,996052	0,996107	0,996163	0,996165	
7	0,996078	0,996106	0,996104	0,996091	0,996083	0,996131	0,99611	0,996169	0,996151	0,996069	
8	0,996066	0,996106	0,996053	0,996089	0,99614	0,99605	0,996081	0,99613	0,996071	0,996104	
9	0,996046	0,996082	0,996104	0,996052	0,996099	0,996114	0,99603	0,996129	0,99605	0,996062	
10	0,996097	0,99608	0,996084	0,996141	0,996033	0,996063	0,996043	0,99604	0,996089	0,99607	
Среднее	0,996076	0,996109	0,996092	0,996078	0,996077	0,996084	0,99609	0,996096	0,996097	0,996085	

Значения вероятности ошибки декодирования без МВП для кода Hamming (15, 11) при различных значениях задержек приведены в табл. 2. 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. Значения вероятности ошибки декодирования без МВП для кода Hamming (21, 16) при различных значениях задержек приведены в таблице 3. Анализ приведенных значений показывает, 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.

Таблица 2

**Эффективность кода Hamming (15, 11)**

Значения задержек		Значение задержки Z4									
Z1, Z2, Z3, Z5		1	2	3	4	5	6	7	8	9	10
1	0,999553	0,999523	0,9995	0,999522	0,999505	0,999505	0,999495	0,999514	0,999515	0,999513	
2	0,999513	0,999502	0,999512	0,999489	0,999516	0,999486	0,999508	0,999487	0,99948	0,999485	
3	0,999544	0,999514	0,999506	0,999529	0,999499	0,999522	0,999482	0,999512	0,999486	0,999501	
4	0,999494	0,999487	0,999514	0,999511	0,999497	0,999506	0,999512	0,999513	0,999496	0,999503	
5	0,999522	0,999474	0,999544	0,999508	0,999486	0,999537	0,999532	0,999514	0,9995	0,999485	
6	0,999508	0,999477	0,999521	0,999526	0,999497	0,999525	0,999456	0,999492	0,999503	0,999474	
7	0,999508	0,999513	0,999503	0,999523	0,999536	0,999507	0,999503	0,999523	0,999476	0,999498	
8	0,999523	0,999523	0,9995	0,999492	0,999496	0,999536	0,999489	0,999483	0,99952	0,9995	
9	0,999506	0,999499	0,999491	0,999518	0,999496	0,99948	0,999478	0,999502	0,999515	0,999498	
10	0,999491	0,999505	0,999494	0,999509	0,999516	0,999522	0,999529	0,999497	0,999504	0,999483	
Среднее	0,999516	0,999502	0,999509	0,999513	0,999504	0,999513	0,999498	0,999504	0,9995	0,999494	



Таблица 3

## Эффективность кода Hamming (21, 16)

Значения задержек Z1, Z2, Z3, Z5	Значение задержки Z4									
	1	2	3	4	5	6	7	8	9	10
1	0,995315	0,995317	0,995325	0,995356	0,995328	0,995353	0,995344	0,995274	0,995341	0,995288
2	0,995386	0,995312	0,995322	0,995319	0,995328	0,995395	0,995372	0,995375	0,995298	0,995288
3	0,995329	0,995354	0,995393	0,995345	0,995336	0,995371	0,995322	0,995346	0,995314	0,99532
4	0,995312	0,99537	0,995244	0,995396	0,995354	0,995343	0,995345	0,995371	0,995254	0,995353
5	0,995364	0,995337	0,995293	0,995296	0,995286	0,99531	0,995353	0,995397	0,995355	0,99537
6	0,995336	0,995307	0,995344	0,995367	0,995269	0,995337	0,995395	0,995318	0,995293	0,995266
7	0,9953	0,995318	0,995308	0,99533	0,995321	0,995356	0,995308	0,995342	0,995343	0,995309
8	0,995352	0,995368	0,995363	0,995341	0,995257	0,995354	0,995313	0,995315	0,995317	0,995347
9	0,995345	0,995339	0,995349	0,995331	0,995254	0,995324	0,995281	0,995228	0,995313	0,995265
10	0,995302	0,995281	0,995353	0,995344	0,99537	0,995349	0,995372	0,995303	0,995334	0,995288
Среднее	0,995334	0,99533	0,995329	0,995343	0,99531	0,995349	0,995341	0,995327	0,995316	0,995309

Полученные результаты 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.

**Заключение.** В работе предложена и обоснована стратегия комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования:

1. Передачу информации от источника к получателю можно представить в виде информационного потока, изначально представляющего поток сообщений. Согласно принятой общей модели передачи информации [1], форма этого потока в ходе передачи подвергается изменениям (преобразованиям).
2. Виртуализацию информационного потока можно рассматривать как проекцию формы представления информационного потока на выходе преобразования кодирования на область абсолютно оптимальных решений, заданную условием виртуализации 1.
3. Переход от общего решения к конкретным решениям обеспечивается введением условий виртуализации 2–4.
4. Функционал виртуализации формирует проекцию на область абсолютно оптимальных решений, заданную условием виртуализации 1.
5. Виртуализация реализуется включением на выходе преобразования кодирования и на входе преобразования декодирования модуля виртуализации информационного потока.
6. Открывается возможность идентификации и аутентификации источника информации. В качестве идентификатора источника при этом выступает последовательность значений задержек, устанавливаемых в модуле виртуализации.
7. Сложение исходных кодограмм с кодограммами повторного кодирования можно интерпретировать как преобразование защиты информации. С этих позиций кодограммы повторного кодирования выступают в роли ключевой последовательности.
8. Включение разности исходных и виртуальных сообщений в формирование ключевой последовательности будет обеспечивать решение задачи имитозащиты.

## 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.* 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. – № 1 (76). – 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. – 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. Патент 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.
11. *Котенко В.В.* Оценка информационного образа исследуемого объекта с позиций теории виртуального познания // Известия ТРТУ. – 2006. – № 4 (48). – С. 42-48.
12. *Котенко В.В.* Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 140-147.
13. *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.
14. *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.
15. *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.
16. *Ховансков 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.
17. *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.
18. *Котенко В.В., Першин И.М., Котенко С.В.* Особенности идентификационного анализа на основе информационной виртуализации изображений местоположения объектов в ГИС // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 212-219.

19. *Котенко В.В., Румянцев К.Е., Котенко С.В.* Методология идентификационного анализа инфокоммуникационных систем: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2014. – 226 с.
20. *Котенко С.В.* Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 152-158.

## 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.* 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.
4. *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 konferentsii]. Moscow: Izd-vo Sputnik, 2011, pp. 36-40.
5. *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.
6. *Kotenko V.V., Polikarpov S.V.* Strategiya formirovaniya virtual'nykh vyborochnykh prostanstv 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.
7. *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.
8. *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.
9. *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.
10. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V.* Sposob shifrovaniya dvoichnoy informatsii [A method of encrypting binary data]. Patent RF, No. 2260916, 2005.
11. *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.
12. *Kotenko V.V.* Virtualizatsiya protsessa zashchity nepreryvnoy informatsii otositel'no usloviy teoreticheskoy nedeshifruemosti [Virtualization is the process of continuous protection of information concerning the conditions of theoretical nedeshifruemosti], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information Counter Terrorist Threats], 2013, No. 20, pp. 140-147.

13. *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.
14. *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.
15. *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.
16. *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.
17. *Kotenko V.V., Kotenko S.V., Ermolaev A.Yu., Krutakov Yu.B.* Printsipy identifikatsionnogo 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.
18. *Kotenko V.V., Pershin I.M., Kotenko S.V.* Osobennosti identifikatsionnogo analiza na osnove informatsionnoy virtualizatsii izobrazheniy mestopolozheniya ob"ektov v GIS [Features of the analysis based on the identification information of virtualization image the location of objects in the GIS], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 212-219.
19. *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 pp.
20. *Kotenko S.V.* Virtualizatsiya protsessa zashchity nepreryvnoy informatsii otnositel'no usloviy teoreticheskoy nedeshifruemosti [Virtualization is the process of continuous protection of information concerning the conditions of theoretical nedeshifruemosti], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter terrorism threats], 2013, No. 20, pp. 152-158.

Статью рекомендовал к опубликованию д.т.н. И.И. Сныткин

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

**Миргородский Сергей Владимирович** – кафедра ВП; доцент.

**Лукин Максим Юрьевич** – Министерство обороны РФ; Москва, Чечерский проезд, 32, кв. 114; инженер.

**Kotenko Vladimir Vladimirovich** – Southern Federal University; e-mail: virtsecurity@mail.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: 88634315507; the department IBTKS; associate professor.

**Mirgorodsky Sergey Vladimirovich** – the department VP; associate professor.

**Lukin Maksim Jrievich** – The Ministry of Defence of the Russian Federation; 32, Chechersk travel, ap. 114, Moscow, Russia; engineer.