Polikarpov Sergey Vitalievich – Southern Federal University; e-mail: polikarpovsv@gmail.com; 2, Chekhova street, Taganrog, 347922, Russia; phone: +78634371902; the department of Information security of telecommunication; cand. of eng. sc.; associate professor.

Kozhevnikov Aleksey Alekseevich – e-mail: leha.kozhevnikov@gmail.com; the department of Information security of telecommunication; assistant lecturer.

УДК 621.39

В.В. Котенко, С.В. Котенко

ИДЕНТИФИКАЦИОННЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ИДЕНТИФИКАТОРОВ*

На фоне значительных достижений в части идентификации пользователей в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация информационных процессов. Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях влияния идентификационных признаков на качество защиты информации. Цель исследования состоит в разработке и обосновании принципов идентификационного анализа криптографических алгоритмов. Фундаментальную основу предлагаемого подхода к идентификационному анализу составляют авторские методы теории виртуализации: метод формирования виртуальных информационных образов, метод моделирования оценок виртуальных информационных образов, методы виртуализации информационных процессов, методы виртуализации идентификаторов. Решения задачи идентификационного анализа криптографических алгоритмов включает два этапа: 1) идентификационный анализ с позиций виртуализации информационных идентификаторов ансамблей процесса шифрования; 2) идентификационный анализ с позиций информационных оценок эффективности шифрования. Полученные результаты открывают принципиально новую область исследований в направлении расширения возможностей управления защитой информации на основе интеллектуального анализа данных и поддержки принятия решения при ситуационном управлении в условиях угроз информационных вторжений с адаптацией к возможному изменению широкого спектра идентификаторов источников угроз.

Защита информации; идентификация; аутентификации; шифрование; виртуализация; оптимизация; информационный поток; информационная безопасность.

V.V. Kotenko, S.V. Kotenko

ANALYSIS OF CRYPTOGRAPHIC IDENTIFICATION ALGORITHMS WITH POSITIONS VIRTUALISATION IDENTIFIERS

Against the backdrop of significant advances in the identification of the user in tasks of processing, protection and transmission of information almost overlook the identification of information processes. The criticality of the situation is revealed in the recent patterns of influence on the quality of the identification features of data protection. The purpose of the study is to develop an identification and justification of the principles of the analysis of cryptographic algorithms. The fundamental basis for the proposed approach to the identification methods of analysis constitute the author's theory of virtualization: virtual information method of forming images, a method of modeling assessments virtual information, the method of information processes virtualization, virtualization techniques identifiers. Solving the problem identification analysis of cryptographic algorithms involves two stages: 1) identification analysis from the point of virtualization information encryption process identifiers ensembles; 2) identification information analysis from the standpoint of effectiveness evaluations encryption. These results open up an entirely new field of

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

research in the direction of empowering security management information based on the data mining and decision support at situational management under threat information intrusion adapting to possible changes in a wide range of sources of threats to identity.

Information security; identification; authentication; encryption; virtualization; optimization; information flow; information security.

Введение. Идентификационный анализ телекоммуникационных систем является комплексным понятием, включающим идентификацию информационно-телекоммуникационных процессов и пользовательского уровня. Анализ ситуации, сложившейся в данном научном направлении показывает отсутствие решений проблемы комплексной идентификации (аутентификации) пользовательского уровня и информационных процессов телекоммуникационных систем. При этом на фоне значительных достижений в части идентификации пользователей в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация (аутентификация) информационно-телекоммуникационных процессов. Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях влияния идентификационных признаков на качество защиты информации. Цель исследования состоит в разработке и обосновании принципов идентификационного анализа криптографических алгоритмов с позиций теории виртуализации [1, 2].

1. Идентификационный анализ с позиций виртуализации информационных идентификаторов ансамблей процесса шифрования. Особенностью решения задачи идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования является применение двух видов идентификаторов: информационных и виртуальных информационных.

К информационным идентификаторам относятся:

1. Информационная емкость ансамбля ансамбля криптограмм E:

$$\mathrm{H}_{\max}[\mathrm{U}] = \log_2 M_{\mathrm{U}}, \tag{1}$$

$$\mathrm{H}_{\max}[\mathrm{E}] = \log_2 M_{\mathrm{E}}, \tag{2}$$

где M_{U} и M_{E} – размерность выборочных пространств ансамблей сообщений и криптограмм соответственно.

2. Энтропия ансамбля сообщений и ансамбля криптограмм:

$$\mathrm{H}[\mathrm{U}] = -\sum_{u_i} p(\mathrm{u}_i)\log_r\left(p(\mathrm{u}_i)\right), \tag{3}$$

$$\mathrm{H}[\mathrm{E}] = -\sum_{\mathrm{e}_i} p(\mathrm{e}_i)\log_r\left(p(\mathrm{e}_i)\right). \tag{4}$$

3. Избыточность $\mathrm{B}[\mathrm{U}]$ и коэффициент избыточности μ_{U} ансамбля сообщений:

$$\mathrm{B}[\mathrm{U}] = \mathrm{H}_{\max}[\mathrm{U}] - \mathrm{H}[\mathrm{U}], \tag{5}$$

$$\mu_{\mathrm{U}} = 1 - \frac{\mathrm{H}[\mathrm{U}]}{\mathrm{H}_{\max}[\mathrm{U}]}\ . \tag{6}$$

4. Избыточность $\mathrm{B}[\mathrm{E}]$ и коэффициент избыточности μ_{E} и ансамбля криптограмм:

$$\mathrm{B}[\mathrm{E}] = \mathrm{H}_{\max}[\mathrm{E}] - \mathrm{H}[\mathrm{E}], \tag{7}$$

$$\mu_{\mathrm{E}} = 1 - \frac{\mathrm{H}[\mathrm{E}]}{\mathrm{H}_{\max}[\mathrm{E}]}\ . \tag{8}$$

5. Стохастичность (вариабельность) ансамбля сообщений и ансамбля криптограмм:

$$G[U] = \frac{H[U]}{H_{max}[U] - H[U]}, \tag{9}$$

$$G[E] = \frac{H[E]}{H_{max}[E] - H[E]}. \tag{10}$$

К виртуальным информационным идентификаторам относятся:

1. Информационный спектр сообщений.
2. Информационный спектр криптограмм.

Формирование виртуальных информационных идентификаторов производится на основе системы условий виртуализации вида:

1. Количество информации в сообщении является вещественной величиной.
2. Количество информации в криптограмме является вещественной величиной.
3. Изменение количества информации во времени представляет непрерывный случайный процесс.
4. Количество информации в сообщениях во времени представляет последовательность отсчетов (выборок) $J[u_i]$ соответствующего непрерывного случайного процесса.
5. Количество информации в криптограммах во времени представляет последовательность отсчетов (выборок) $J[e_i]$ соответствующего непрерывного случайного процесса.

В рамках установленных условий виртуализации математическая модель оценки информационного спектра сообщений определяется как

$$\begin{aligned} J^*(u_i) &= \exp(-\alpha T) J^*(u_{i-1}) + \\ &+ K_i^{(k)} \left[J_\psi(u_i) - \exp(-\alpha T) J^*(u_{i-1}) - h_0 \right] + h_0, \end{aligned} \tag{11}$$

$$J_U^*(t) = J^*(u_i) \exp(-\alpha(t - t_i)), \tag{12}$$

$$S_U^*(\omega_J) = \int_0^\infty J_U^*(t) \exp(-j\omega_J t)\, dt. \tag{13}$$

Математическая модель оценки информационного спектра криптограмм определяется в виде:

$$\begin{aligned} J^*(e_i) &= \exp(-\alpha T) J^*(e_{i-1}) + \\ &+ K_i^{(k)} \left[J_\psi(e_i) - \exp(-\alpha T) J^*(e_{i-1}) - h_0 \right] + h_0, \end{aligned} \tag{14}$$

$$J_E^*(t) = J^*(e_i) \exp(-\alpha(t - t_i)), \tag{15}$$

$$S_E^*(\omega_J) = \int_0^\infty J_E^*(t) \exp(-j\omega_J t)\, dt. \tag{16}$$

Выражения (11)–(16) составляют фундаментальную теоретическую основу методики идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования и определяют ее содержание:

1. Формирование блоков логических элементов ансамблей входа (ансамблей сообщений) и блоков логических элементов ансамблей выхода (ансамблей криптограмм) криптографического алгоритма.
2. Определение вероятностной меры логических элементов в блоках сообщений и криптограмм.
3. Вычисление значений количества информации в логических элементах и формирование блоков количеств информации в сообщениях и блоков количеств информации в криптограммах.

4. Вычисление информационных идентификаторов сообщений и криптограмм (1)–(10).
5. Формирование информационного спектра сообщений (11)–(13) и информационного спектра криптограмм (14)–(16).
6. Определение области идентификации криптографического алгоритма.

Компьютерное моделирование методики рис.1 позволило определить основные принципы идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования.

Компьютерная модель рис. 1 применялась для идентификацинного анализа криптографических алгоритмов AES 128 и AES 256. В качестве сообщений использовались текстовые сообщения, формируемые в свободной форме различными индивидумами, которые рассматривались как источники информации.

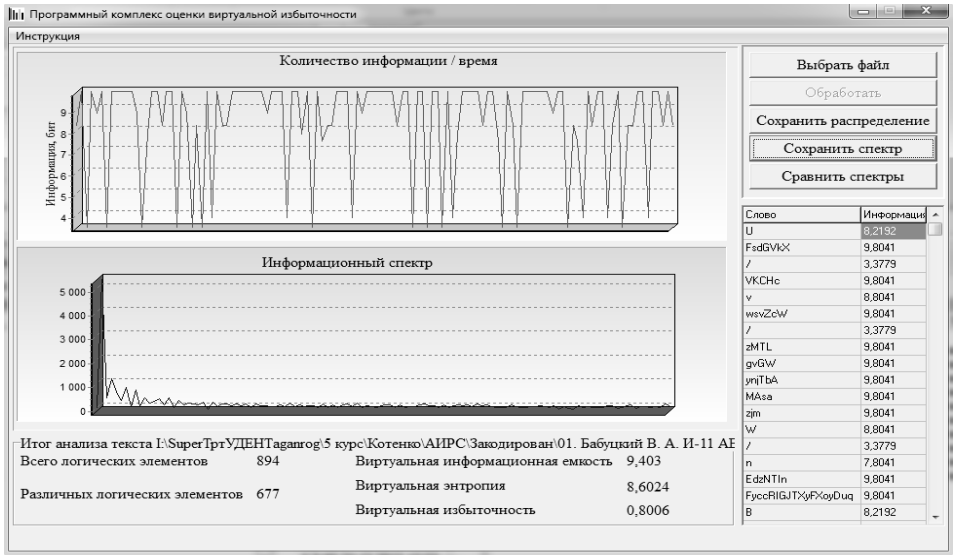


Рис. 1. Интерфейс компьютерной модели методики идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования

Характерные варианты полученныхъ результатов для информационных идентификаторов приведены на рис. 2–5 и в табл. 1–4: значения информационной емкости – в табл. 1 и рис. 2; значения энтропии – в табл. 2 и рис. 3; значения избыточности – в табл. 3 и рис. 4; значения стохастичности (вариабельности) – в табл. 4 и рис. 5.

Таблица 1

Значения информационной емкости

	Source №01	Source №02	Source №03	Source №04	Source №05	Source №06	Source №07	Source №08	Source №09	Source №10
Шифрование по алгоритму AES 128										
H|gmax	8,592	8,189	8,523	8,519	8,741	7,554	8,804	8,479	8,543	8,247
Шифрование по алгоритму AES 256										
H|gmax	9,403	9,348	9,853	9,856	9,918	8,861	9,865	9,590	9,779	9,453

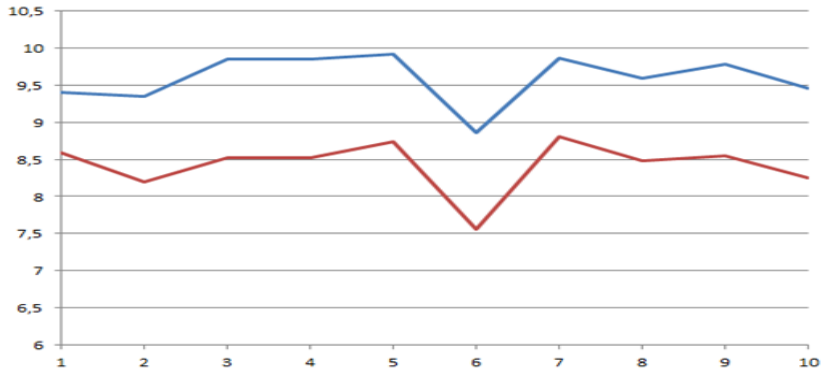


Рис. 2. Графики зависимости информационной емкости криптограмм от источников сообщений для криптографических алгоритмов: 1 – AES 128; 2 – AES 256

Таблица 2

Значения энтропии

	Source №01	Source №02	Source №03	Source №04	Source №05	Source №06	Source №07	Source №08	Source №09	Source №10
Шифрование по алгоритму AES 128										
H|в	7,628	7,372	7,551	7,543	7,647	6,743	7,918	7,749	7,753	7,287
Шифрование по алгоритму AES 256										
H|в	8,602	8,481	8,914	8,886	9,008	8,248	8,902	8,928	8,840	8,659

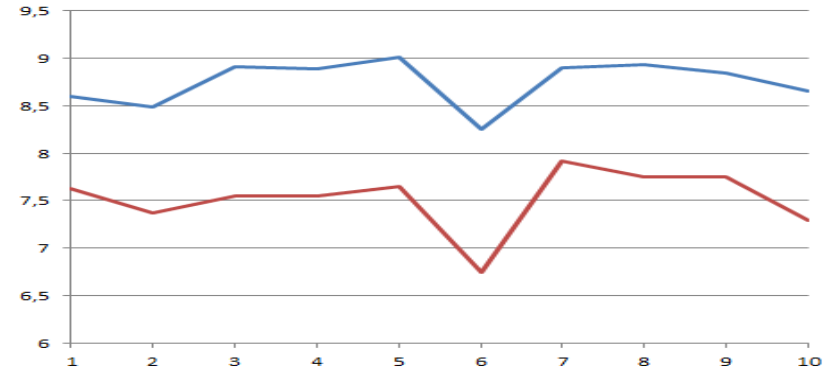


Рис. 3. Графики зависимости энтропии криптограмм от источников сообщений для криптографических алгоритмов: 1 – AES 128; 2 – AES 256

Таблица 3

Значения избыточности

	Source №01	Source №02	Source №03	Source №04	Source №05	Source №06	Source №07	Source №08	Source №09	Source №10
Шифрование по алгоритму AES 128										
μв	0,112	0,0998	0,114	0,129	0,125	0,107	0,100	0,086	0,092	0,116
Шифрование по алгоритму AES 256										
μв	0,0851	0,0927	0,095	0,098	0,091	0,069	0,097	0,069	0,096	0,085

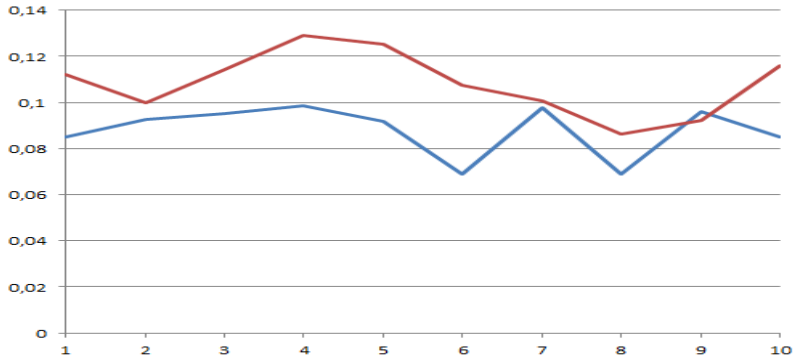


Рис. 4. Графики зависимости избыточности криптограмм от источников сообщений для криптографических алгоритмов:1 – AES 128; 2 – AES 256

Таблица 4

Значения стохастичности (вариабельности)

	Source №01	Source №02	Source №03	Source №04	Source №05	Source №06	Source №07	Source №08	Sourc e№09	Source №10
Шифрование по алгоритму AES 128										
GB	7,916	9,022	8,765	7,728	6,987	8,317	8,944	10,605	9,823	7,591
Шифрование по алгоритму AES 256										
GB	10,744	9,785	9,495	9,157	9,889	13,464	9,246	13,482	9,409	10,91

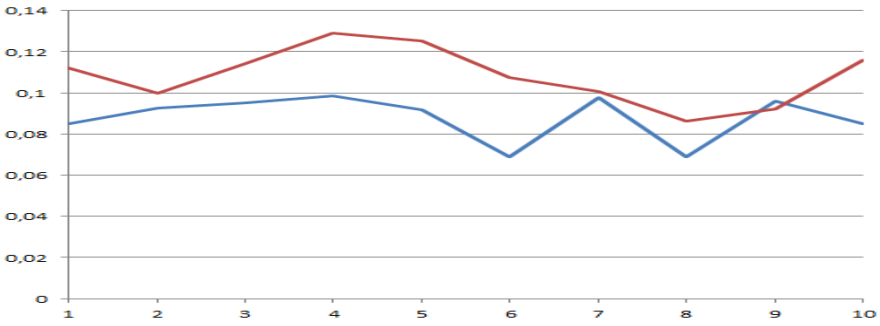


Рис. 5. Графики зависимости стохастичности (вариабельности) криптограмм от источников сообщений для криптографических алгоритмов: 1 – AES 128; 2 – AES 256

Характерные варианты полученных результатов для виртуальных информационных идентификаторов приведены на рис. 6.

Анализ полученных результатов показал, что вероятность пересечения областей изменения информационных идентификаторов для криптографических алгоритмов AES 128 и AES 256 находится в пределах 10^{-3}. Это значение характеризует точность идентификации. Анализ виртуальных информационных идентификаторов показал, что каждому криптографическому алгоритму соответствует строго определенный диапазон изменения ширины информационного спектра, что позволяет значительно повысить точность идентификации и обеспечивает аутентификацию.

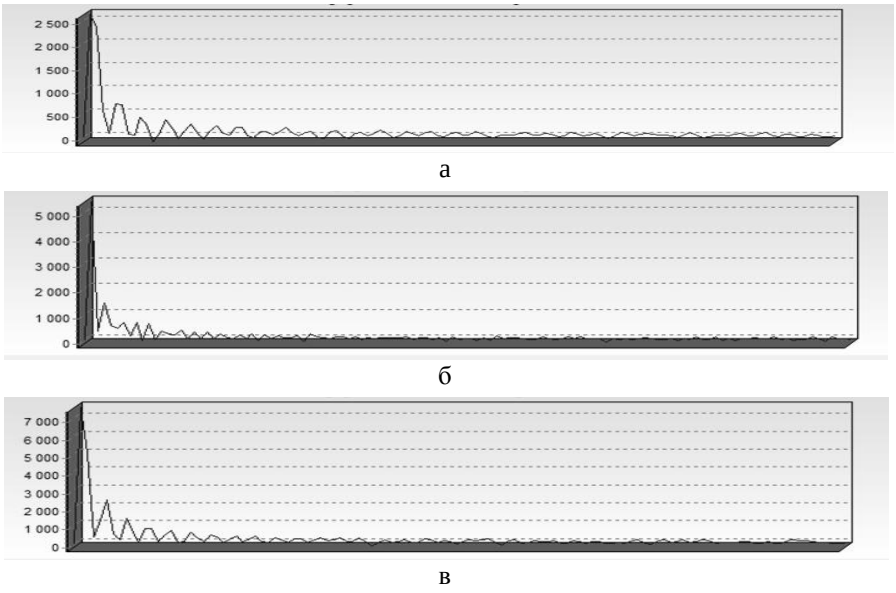


Рис. 6. Информационный спектр: а – открытого текста; б – зашифрованного текста по алгоритму AES 128; в – зашифрованного текста по алгоритму AES 256

Полученные результаты свидетельствуют о принципиально новой области исследований и требуют дальнейшей более детальной проработки. Однако уже на настоящем этапе могут быть сформулированы следующие из них базовые принципы идентификационного анализа криптографических алгоритмов с позиций информационных идентификаторов процесса шифрования.

Во-первых, это наличие четырех областей идентификации, заданных информационными идентификаторами. Во-вторых, наличие одной области идентификации, заданной виртуальными информационными идентификаторами. В-третьих, возможность измерения информационных и виртуальных информационных идентификаторов ансамблей сообщений на входе криптографического алгоритма. В-четвертых, это три этапа идентификационного анализа: грубая идентификация на основе информационных идентификаторов; точная идентификация на основе виртуальных информационных идентификаторов; дополнительная идентификация на основе информационных и виртуальных информационных идентификаторов ансамблей сообщений.

2. Идентификационный анализ с позиций информационных оценок эффективности шифрования. Запишем выражение для среднего количества информации об элементах ансамблей сообщений U^* и ключей K^* в элементах ансамбля криптограмм E^*

$$I[U^*K^*;E^*]= I[U^*;E^*]+ I[K^*; U^*/E^*]. \quad (17)$$

Из теоремы шифрования [2] следует, что существование теоретически недешифруемого шифра Φ_0 возможно тогда, когда среднее количество взаимной информации $I[U^*K^*;E^*]$ будет равно нулю. С учетом этого для общего случая, предполагающего статистическую зависимость сообщений и ключей, выражение (17) может быть представлено в виде

$$- I[U^*;E^*]=I[K^*; U^*/E^*]. \quad (18)$$

Знак минус при $I[U^*; E^*]$ в (18) можно трактовать как введение в криптограммы ложной информации о сообщениях путем установления статистической зависимости между ключами и криптограммами при шифровании.

В свою очередь, если в выражении (18) учесть, что

$$I[K^*; U^*/E^*] = I[K^*;U^*E^*] - I[K^*;U^*] = \\ = H[K^*/U^*E^*] - H[K^*/U^*], \quad (19)$$

то становится понятным его общий физический смысл. Оказывается, что теоретически недешифруемые шифры могут существовать и при статистической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование предполагает увеличение средней условной неопределенности ключей. Причем это увеличение должно сопровождаться введением ложной информации о сообщениях в формируемые криптограммы. Таким образом, можно считать, что $I[K^*; U^*/E^*]$ характеризует эффективность шифрования Ф

$$D(\Phi,U^*) = C(\Phi,U^*) - H[K^*/U^*], \quad (20)$$

где $C(\Phi, U^*)$ – стойкость шифрования, причем $C(\Phi, U^*) = H[K^*/U^*E^*]$.

Исходя из теоремы шифрования, можно выделить две области возможных значений эффективности шифрования:

1) область неотрицательных значений $D(\Phi,U^*)\geq 0$, соответствующих теоретически недешифруемым шифрам;

2) область отрицательных значений $D(\Phi,U^*)<0$, при которых теоретическая недешифруемость не обеспечивается.

В частном случае, когда ансамбли U^* и K^* статистически независимы, выражение (20) принимает вид

$$D(\Phi,U^*) = C(\Phi,U^*) - H[K],$$

где $C(\Phi,U^*) = H[K^*/E^*]$.

С позиции традиционного подхода, предполагающего обязательное выполнение неравенства $H[K^*] \geq H[K^*/E^*]$ при шифровании Ф, диапазон возможных значений $D(\Phi,U^*)$, в данном случае, определяется как

$$-H[K^*] < D(\Phi,U^*) \leq 0. \quad (21)$$

При этом диапазон значений стойкости шифрования находится в пределах

$$0 < C(\Phi,U^*) \leq H[K^*]. \quad (22)$$

Теоретическая недешифруемость обеспечивается только при достижении $D(\Phi, U^*)$ и $C(\Phi, U^*)$ верхних границ отмеченных диапазонов, т.е. при $D(\Phi, U^*) = 0$ и $C(\Phi, U^*) = H[K^*]$. Нетрудно заметить, что в этом случае шифр, недешифруемый теоретически, на практике таковым может не оказаться. Так, дискретный ансамбль предполагает конечную энтропию, которая при несанкционированном доступе может быть сведена к минимуму путем простого последовательного перебора элементов выборочного пространства K^*.

В случае представления ансамбля ключей в виде совместного ансамбля X^*Y^* ключевых данных и ключевых последовательностей эффективность шифрования определяется выражением вида

$$D(\Phi,U^*) = \sup_X D_p(\Phi,U_p^*),$$

$$D_p(\Phi,U_p^*) = \sum_{ijn} p(U_i Y_j E_n) \log \frac{p(Y_j / U_i)}{p(Y_j / U_i E_n)},$$

где верхняя грань берется по всем разбиениям ансамбля U^*, всем разбиениям ансамбля E^* и всем разбиениям ансамбля Y^*, заданных ансамблем X^*.

Стойкость шифрования в данном случае может быть определена как

$$C(\Phi,U^*) = \sup_X C_p(\Phi,U_p^*),$$

$$C_p(\Phi,U_p^*) = \sum_{ijn} p(U_i Y_j E_n) \log \frac{1}{p(Y_j / U_i E_n)}, \quad (23)$$

где верхняя граница берется по всем разбиениям ансамбля U^*, всем разбиениям ансамблей E^* и Y^*, заданных ансамблем X^*.

Преобразовав (23) к виду

$$C_p(\Phi,U_p^*) = \sum_{ijn} p(U_i Y_j E_n) \log \frac{p(U_i E_n)}{p(Y_j)\, p(U_i / Y_j)\, p(E_n / U_i Y_j)},$$

получаем

$$C_p(\Phi,U_p^*) = H[Y_p^*] + H[U_p^*/Y_p^*] + \\ + H[E_p^*/U_p^* Y_p^*] - H[U_p^*] - H[E_p^*/U_p^*],$$

Откуда

$$C_p(\Phi,U_p^*) = H[Y_p^*] - I[U_p^*;Y_p^*] - H[E_p^*;Y_p^*/U_p^*]. \quad (24)$$

Выражения (20)–(24) определяют математическую модель оценки эффективности шифрования. Компьютерное моделирование этой модели позволило определить основные принципы идентификационного анализа криптографических алгоритмов с позиций оценки эффективности шифрования.

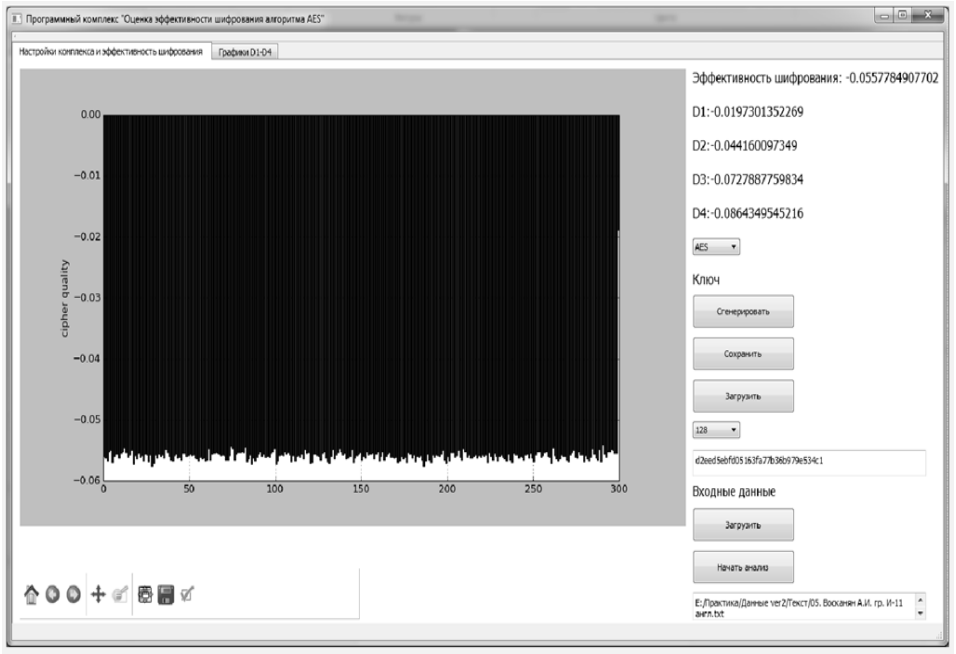


Рис. 7. Интерфейс компьютерной модели и идентификационного анализа криптографических алгоритмов с позиций оценки эффективности шифрования

Компьютерная модель рис. 7 применялась для идентификацинонного анализа криптографических алгоритмов AES 128, AES 256 и Serpent 128. В качестве сообщений использовались текстовые сообщения на русском и английском языках, формируемые в свободной форме различными индивидумами, которые рассматривались как источники информации. Характерные варианты полученных результатов приведены на рис. 8–10 и в табл. 5–6.

Таблица 5

Эффективность шифрования русского текста

Source	AES 128, D_{RUS}	AES 256, D_{RUS}	Serpent 128, D_{RUS}
Source №01	-0.0550600151792	-0.0556715029894	-0.0544901238786
Source №02	-0.0551337589268	-0.0554223342502	-0.0545516056531
Source №03	-0.0551406515286	-0.0557784434072	-0.0546357409543
Source №04	-0.0550530792622	-0.0556795099601	-0.0545056846809
Source №05	-0.0551572685118	-0.0556859992645	-0.0544837597364
Source №06	-0.0552765261727	-0.055719526973	-0.0546931733133
Source №07	-0.0551327982721	-0.0554954852299	-0.054506965216
Source №08	-0.0549852377967	-0.0555122345043	-0.0545440980044
Source №09	-0.0550650373036	-0.0555254629327	-0.0545016493565
Source №10	-0.0551318746769	-0.0556222166469	-0.0545783241499

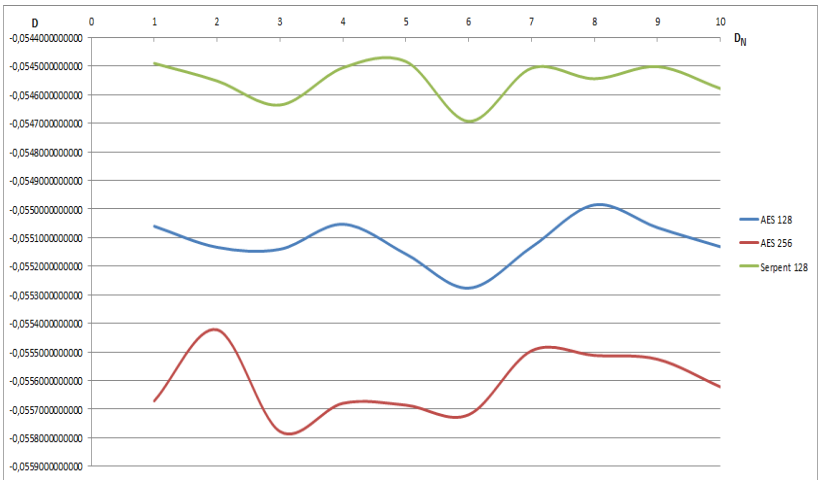


Рис. 8. Идентификационные области криптографических алгоритмов относительно значений оценки эффективности шифрования источников русского языка

Таблица 6

Эффективность шифрования английского текста

Source	AES 128, D_{ENG}	AES 256, D_{ENG}	Serpent 128, D_{ENG}
Source №01	-0.055721919645	-0.0562248232453	-0.0553849833713
Source №02	-0.0557720758638	-0.0562856116225	-0.0554557511884
Source №03	-0.0558135367716	-0.0565495779734	-0.0555687149165
Source №04	-0.0557388286719	-0.0565114743239	-0.0555380402309
Source №05	-0.0557784907702	-0.056506986724	-0.0555058444533
Source №06	-0.0557145047151	-0.056159704492	-0.0554135654246
Source №07	-0.0559539888972	-0.056593481323	-0.0555827459775
Source №08	-0.0557333703661	-0.0564226674607	-0.0554004951753
Source №09	-0.055830044096	-0.0564168131194	-0.055627820498
Source №10	-0.0558554052116	-0.056529203872	-0.0555175826376

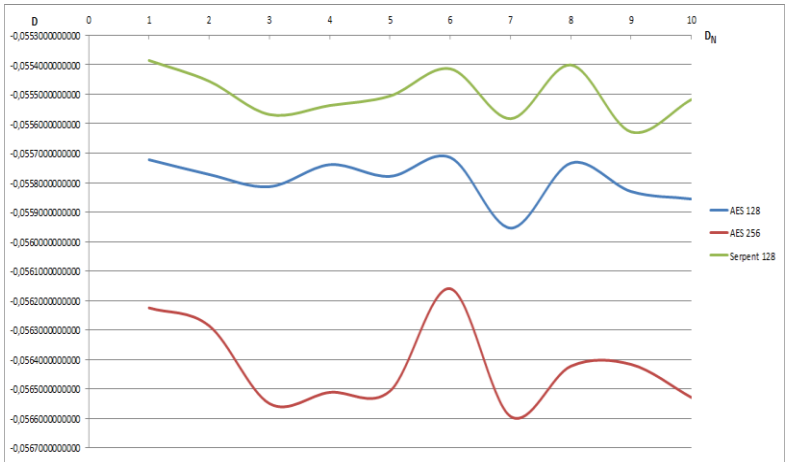
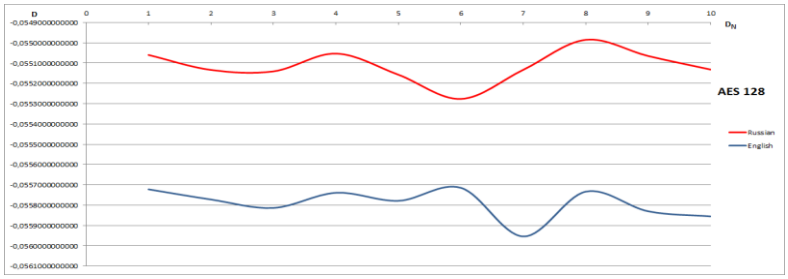
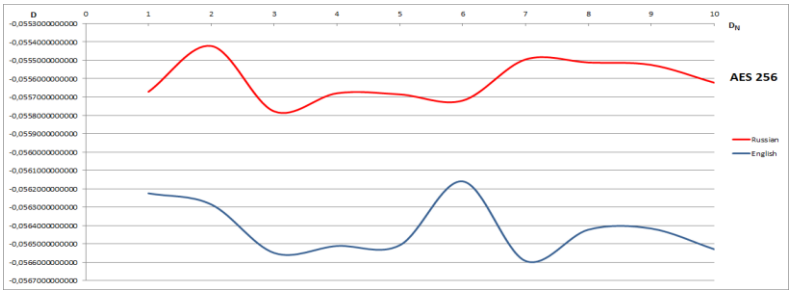


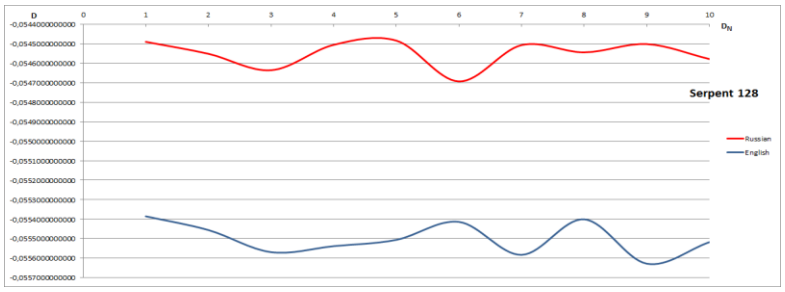
Рис. 9. Идентификационные области криптографических алгоритмов относительно значений оценки эффективности шифрования источников английского языка



a



b



c

Рис. 10. Идентификационные области русских и английских источников для криптографических алгоритмов: a – AES 128; b – AES 256; c – Serpent 128

Анализ полученных результатов показал, что идентификационные области значений оценок эффективности шифрования для криптографических алгоритмов не пересекаются, что свидетельствует о высокой точности идентификации. При этом идентификационные области криптографических алгоритмов делятся на непересекающиеся подобласти, определяемые лингвинистическим видом шифруемого источнка информации.

Заключение. Полученные результаты открывают принципиально новую область исследований и требуют дальнейшей более детальной проработки. Однако уже на настоящем этапе могут быть сформулированы следующие из них базовые принципы идентификационного анализа криптографических алгоритмов:

1. Наличие четырех областей идентификации, заданных информационными идентификаторами.
2. Наличие одной области идентификации, заданной виртуальными информационными идентификаторами.
3. Возможность измерения информационных и виртуальных информационных идентификаторов ансамблей сообщений на входе криптографического алгоритма.
4. Три этапа идентификационного анализа: грубая идентификация на основе информационных идентификаторов; точная идентификация на основе виртуальных информационных идентификаторов; дополнительная идентификация на основе информационных и виртуальных информационных идентификаторов ансамблей сообщений.
5. Формирование блоков сообщений, ключей и криптограмм, участвующих в процессе шифрования.
6. Вычисление собственных и условных собственных количеств информации.
7. Вычисление среднего количества информации и условного среднего количества информации.
8. Определение стойкости шифрования.
9. Формирование оценки эффективности шифрования.
10. Идентификация криптографического алгоритма путем анализа соответствия значения оценки эффективности шифрования идентификационной области конкретного алгоритма.

Развитие отмеченных и производных от них принципов вызывает интерес, прежде всего и потому, что способствует реализации возможности адаптивного относительно эффективности шифрования управления процессами защиты информации в телекоммуникациях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Котенко С.В.* Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 152-158.
2. *Котенко В.В.* Теория виртуализации и защита телекоммуникаций: Монография. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.
3. *Котенко В.В., Румянцев К.Е.* Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. – 369 с.
4. *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.
5. *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.

6. *Котенко В.В.* Стратегия применения теории виртуализации информационных потоков при решении задач информационной безопасности // Известия ЮФУ. Технические науки. – 2007. – № 1 (76). – С. 26-37.
7. *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.
8. *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.
9. *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. – М., 2007. – № 9 (39). – С. 46-56.
10. *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.
11. Пат. № 2260916 РФ. Способ шифрования двоичной информации / *Котенко В.В., Румянцев К.Е., Поликарпов С.В.;* опубл.: 20.09.2005, Бюл. № 26. – С. 1-3.
12. *Котенко В.В.* Оценка информационного образа исследуемого объекта с позиций теории виртуального познания // Известия ТРТУ. – 2005. – № 4 (48). – С. 42-48.
13. *Котенко В.В.* Виртуализация процесса защиты непрерывной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 140-147.
14. *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.
15. *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.
16. *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.
17. *Хованcков 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.
18. *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.
19. *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.
20. *Котенко В.В., Поликарпов С.В.* Методика синтеза алгоритмов определения виртуальной оценки // Информационное противодействие угрозам терроризма. – 2003. – № 1. – С. 54-58.

REFERENCES

1. *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.
2. *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.

3. *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.
4. *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.
5. *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* [Proceedings of the II International Scientific and Practical konferentsii]. Moscow: Izd-vo Sputnik, 2011, pp. 36-40.
6. *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.
7. *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.
8. *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.
9. *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]. Moscow, 2007, No. 9 (39), pp. 46-56.
10. *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.
11. *Kotenko V.V., Rumyantsev K.E., Polikarpov S.V.* Sposob shifrovaniya dvoichnoy informatsii [A method of encrypting binary data]. Patent RF No. 2260916, 2005.
12. *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], 2005, No. 4 (48), pp. 42-48.
13. *Kotenko V.V.* Virtualizatsiya protsessa zashchity nepreryvnoy informatsii otnositel'no usloviy teoreticheskoy nedeshifruemosti [Virtualization is the process of continuous protection of information concerning conditions of the theoretical necesitaremos], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counter terrorist threats], 2013, No. 20, pp. 140-147.
14. *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.
15. *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.
16. *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.

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 identifika-tsionnogo 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.