4. Dolnicar S., Knezevic Cvelbar L., Grün B. A sharing-based approach to enticing tourists to behave more environmentally friendly. *Journal of Travel Research*, 2019, vol. 58 (2), pp. 241–252. DOI: 10.1177/0047287517746013.
5. *O companyi CHRISAL* [About CHRISAL]. URL: https://chrisal-product.ru/publikatsii/o-kompanii-crisal (accessed: 02.06.2019). (In Russian).
6. *Rossiya v zifrah* [Russia in Numbers]. Moscow: Rosstat, 2018, 522 p. (In Russian).
7. Gulin K.A. *Problema othodov v Rossii i eje territorialnye vozmojnosti* [The problem of waste in Russia and its territorial features.]. URL: https://cyberleninka.ru/article/v/problema-othodov-v-rossii-i-ee-territorialnye-osobennosti (accessed: 04.06.2019). (In Russian).
8. *Website agentstva delovoy informazii RosBiznessKonsalting (RBK). Chislo polzyvateleyi Instagram dostiglo 1 mlrd* [Site of the Agency of Business Information «RosBusinessConsulting». The number of Instagram users has reached 1 billion]. URL: https://www.rbc.ru/rbcfreenews/5b2aa6c49a7947e32da2ea8b (accessed: 19.12.2019). (In Russian).
9. Krechetova A. *Issledovaniye auditoria Instagram: servisom polzyetsia kajduy desatyi v Rossii, bolshuunstvo – jenshiny»* [Instagram audience research: every tenth in Russia uses the service, most of them are women]. URL: https://www.forbes.ru/tehnologii/343331-issledovanie-auditorii-instagram-servisom-polzuetsya-kazhdyy-desyatyy-v-rossii (accessed: 19.12.2019). (In Russian).
10. Rojkpva J. *Statistika po Instagram, kotoryu doljen znat kajdyi k 2020 gody* [Statistics on Instagram, which you need to know by 2020]. URL: https://www.likeni.ru/analytics/statistika-po-instagram-kotoruyu-nuzhno-znat-k-2020-godu (accessed: 19.12.2019). (In Russian).
11. *Russkaya slujba BBC NEWS. Statya Greta Tunberg – chelovek goda po versii Time. Moloje ee nikogo ne bylo»* [The Russian service of BBC News. Greta Tunberg is the person of the year according to Time. No one was younger than her]. URL: https://www.bbc.com/russian/news-50742196 (accessed: 20.12.2019). (In Russian).

Received 20.12.2019

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 621.372.552

ДВУХКОМПОНЕНТНАЯ СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА НА ОСНОВЕ ОТНОШЕНИЯ ЛИНЕЙНЫХ ФУНКЦИЙ ДВУХ СИГНАЛОВ, ИСПОЛЬЗУЮЩАЯ АДДИТИВНЫЙ ВИД СВЯЗИ ВСТРАИВАЕМЫХ СИГНАЛОВ

Шакурский М.В.
Самарский государственный технический университет, Самара, РФ
E-mail: m.shakurskiy@gmail.com

Формирование двухкомпонентного контейнера позволяет значительно расширить возможности известных стеганографических методов за счет возникновения новых свойств. Двухкомпонентный контейнер представляет собой две функции двух переменных, одна из которых представляет собой скрываемый сигнал, другая – сигнал контейнера. В статье рассматриваются функции формирования компонент на основе отношения линейных функций двух сигналов. Выражения для формирования компонент и выражение для восстановления скрытого сигнала представляют собой дроби и имеют точки разрыва, что требует проведения анализа и определения условий формирования контейнера. В статье приводятся результаты анализа двухкомпонентной стеганографической системы с нелинейным контейнером в области разрыва функции восстановления информативного сигнала. Определяются ключевые коэффициенты с точки зрения обеспечения наибольшей чувствительности системы к вносимой в значение коэффициента ошибке. Проводится анализ влияния ошибки, вносимой в ключевой коэффициент, на форму восстановленного сигнала. Дается оценка полученных результатов.

Ключевые слова: *двухкомпонентная стеганографическая система, нелинейный контейнер, ключевой коэффициент, инвариантность к маскирующему сигналу*

Введение

В двухкомпонентной стеганографической системе контейнер содержит два сигнала, в формировании которых участвуют маскирующий сигнал и два информативных сигнала. Последние функционально связаны с входным маскируемым сигналом [1–10]. Задача извлечения скрытых сигналов сводится к решению системы двух уравнений с двумя неизвестными. Форма уравнений определяется выбором алгоритма смешивания сигналов.

Алгоритмы могут быть линейные и нелинейные. Алгоритмы восстановления информативного сигнала инвариантны к маскирующему сигналу, что существенно упрощает задачу вскрытия контейнера. Кроме этого, функции восстановления информативного сигнала содержат разрывы, в области которых на несколько порядков возрастает чувствительность функции к ошибкам задания коэффициентов функции.

В статье рассматривается нелинейный алгоритм формирования двухкомпонентного контейнера, использующий отношение линейных функций смешиваемых сигналов, и приводится анализ чувствительности функции восстановления к вариации коэффициентов с целью выбора ключевого (секретного) коэффициента.

Математическая модель системы

Отношение линейных функций двух сигналов имеет вычисляется как:

$$y = \frac{a_1 + b_1 u_1}{a_2 + b_2 u_2}. \quad (1)$$

Данное выражение преобразуется к виду

$$y = \frac{1 + a u_1}{b + c u_2}. \quad (2)$$

Полученное выражение представляет собой общую форму маскировки сигнала. В роли маскирующего сигнала может выступать как сигнал u_1, так и сигнал u_2. В данной статье рассмотрим вариант, когда в роли маскирующего сигнала выступает сигнал u_2. В этом случае две компоненты передаваемого сигнала будут иметь вид:

$$\begin{cases} y_1 = \dfrac{1 + a_1 u_1}{b_1 + c_1 \xi}, \\ y_2 = \dfrac{1 + a_2 u_2}{b_2 + c_2 \xi}, \end{cases} \quad (3)$$

где a, b и c – коэффициенты преобразования; ξ – сигнал контейнера (маскирующий сигнал); u_1 и u_2 – встраиваемые сигналы, сформированные из входного информативного сигнала u:

$$\begin{cases} u_1 = u, \\ u_2 = K - u_1. \end{cases} \quad (4)$$

Решим систему (3), выразив из второго уравнения сигнал ξ:

$$\xi = \frac{1 + a_2 u_2 - b_2 y_2}{c_2 y_2}. \quad (5)$$

Подставим (5) в первое уравнение (3) и преобразуем к виду

$$\begin{aligned} & a_1 c_2 y_2 u_1 - a_2 c_1 y_1 u_2 - c_1 y_1 + c_2 y_2 + \\ & + y_1 y_2 \left(b_2 c_1 - b_1 c_2 \right) = 0. \end{aligned} \quad (6)$$

Подставим в (6) второе выражение (4):

$$\begin{aligned} & \grave{u}\grave{u}_1(\grave{u}\grave{u}\grave{u}_{1\,2\,2} + {}_{2\,1\,1}) - {}_{2\,1\,1} - \\ & - c_1 y_1 + c_2 y_2 + y_1 y_2 \left(b_2 c_1 - b_1 c_2 \right) = 0. \end{aligned} \quad (7)$$

Решая уравнение (7), получим:

$$\begin{aligned} & u = u_1 = \\ & = \frac{c_1 y_1 \left(a_2 K + 1 \right) - c_2 y_2 - y_1 y_2 \left(b_2 c_1 - b_1 c_2 \right)}{a_1 c_2 y_2 + a_2 c_1 y_1}. \end{aligned} \quad (8)$$

Выражение (8) позволяет восстановить скрытый сигнал.

Исследование

Получим выражения для чувствительности (8) к вариации коэффициентов. Для этого определим дифференциал u_1 через приращения коэффициентов. Число коэффициентов в (8) равно шести. Помимо этого, используется значение K. Выражение для абсолютной чувствительности алгоритма восстановления ищем в виде

$$\begin{aligned} \Delta_{u_1} &= S_{a_1} \Delta_{a_1} + S_{a_2} \Delta_{a_2} + S_{b_1} \Delta_{b_1} + \\ &+ S_{b_2} \Delta_{b_2} + S_{c_1} \Delta_{c_1} + S_{c_2} \Delta_{c_2} + S_K \Delta_K . \end{aligned} \quad (9)$$

Получим необходимые производные для перехода к приращениям в выражении (9). Максимальная чувствительность стеганографической системы достигается вблизи точки разрыва функций декодирования сигнала. Заметим, что y_1 и y_2 представляют собой дроби. Поэтому знаменатель (8) не позволяет определить точку разрыва функции. Подставляя значения y_1 и y_2 в выражение (8) и выделяя знаменатель выражения, получим условия попадания в область разрыва:

$$\begin{cases} b_2 c_1 - b_1 c_2 = 0, \\ a_1 + a_2 + a_1 a_2 K = 0, \\ a_1 b_1 c_2 + a_2 b_2 c_1 + a_1 a_2 b_1 c_2 K = \sigma \\ \text{при } \sigma \to 0. \end{cases} \quad (10)$$

Первое условие позволяет исключить влияние сигнала u_1 на точку разрыва, второе условие дает возможность исключить влияние сигнала ξ на

точку разрыва. При выполнении первого и второго условий (10) третье условие обращается в ноль. Одновременное выполнение первого, второго и третьего условий (10) невозможно.

Так как σ стремится к нулю, приравняем второе условие к σ. В этом случае положение точки разрыва не зависит от сигнала u_1, но продолжает зависеть от ξ. Перепишем (10) как

$$\begin{cases} c_2 = \dfrac{b_2 c_1}{b_1}, \\ a_2 = \dfrac{\sigma - a_1}{1 + a_1 K}, \text{ при } \sigma \to 0. \end{cases} \tag{11}$$

Определим значение ξ, при котором знаменатель функции восстановления равен нулю:

$$\xi = -\frac{b_1}{c_1}. \tag{12}$$

Найдем выражения коэффициентов чувствительности S в (9). Для этого используем производные по всем коэффициентам:

$$S_{a_1} = \frac{du_1}{da_1} = -\Big[c_2 y_2 \left(c_1 y_1 - c_2 y_2 + \right.$$
$$\left. + y_1 y_2 \left(b_1 c_2 - b_2 c_1\right) + a_2 c_1 K y_1\right)\Big] / \tag{13}$$
$$/\left(a_2 c_1 y_1 + a_1 c_2 y_2\right)^2,$$

$$S_{a_2} = \frac{du_1}{da_2} = \Big[c_1 y_1 \left(c_2 y_2 - c_1 y_1 + \right.$$
$$\left. + y_1 y_2 \left(b_2 c_1 - b_1 c_2\right) + a_1 c_2 K y_2\right)\Big] / \tag{14}$$
$$/\left(a_2 c_1 y_1 + a_1 c_2 y_2\right)^2,$$

$$S_{b_1} = \frac{du_1}{db_1} = \frac{c_2 y_1 y_2}{a_2 c_1 y_1 + a_1 c_2 y_2}, \tag{15}$$

$$S_{b_2} = \frac{du_1}{db_2} = -\frac{c_1 y_1 y_2}{a_2 c_1 y_1 + a_1 c_2 y_2}, \tag{16}$$

$$S_{c_1} = \frac{du_1}{dc_1} =$$
$$= \frac{c_2 y_1 y_2 \left(a_1 + a_2 - a_2 b_1 y_1 - a_1 b_2 y_2 + a_1 a_2 K\right)}{\left(a_2 c_1 y_1 + a_1 c_2 y_2\right)^2}, \tag{17}$$

$$S_{c_2} = \frac{du_1}{dc_2} =$$
$$= -\frac{c_1 y_1 y_2 \left(a_1 + a_2 - a_2 b_1 y_1 - a_1 b_2 y_2 + a_1 a_2 K\right)}{\left(a_2 c_1 y_1 + a_1 c_2 y_2\right)^2}, \tag{18}$$

$$S_K = \frac{du_1}{dK} = \frac{a_2 c_1 y_1}{a_2 c_1 y_1 + a_1 c_2 y_2}. \tag{19}$$

Зная коэффициенты преобразования (3), с помощью выражений (13)–(19) можно оценить чувствительность системы к вариации того или иного коэффициента и выбрать коэффициент, наиболее подходящий на роль ключевого коэффициента, который является секретным. Для наглядности определения, какой из коэффициентов наиболее эффективно использовать в качестве ключевого, определим характер искажения восстановленного полезного сигнала при внесении ошибки в тот или иной коэффициент. Для этого воспользуемся численным моделированием. Зададимся исходными значениями:

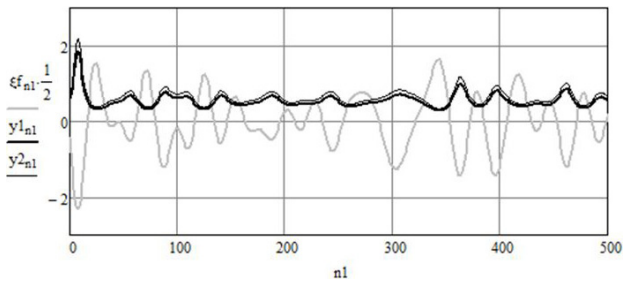

Рисунок 1. Диаграммы маскирующего сигнала и сигналов компонент контейнера

$$a_1 = 0{,}3; \quad b_1 = 2; \quad b_2 = 1{,}3;$$
$$c_1 = 0{,}3; \quad K = 1; \quad \sigma = 1 \cdot 10^{-9}.$$

С помощью (11) найдем a_2, c_2:

$$a_2 = \frac{\sigma - a_1}{1 + a_1 K} = -0{,}231;$$

$$c_2 = \frac{b_2 c_1}{b_1} = 0{,}195.$$

Здесь важно отметить, что при формировании сигналов y_1 и y_2 используются дроби, которые, в свою очередь, также могут иметь точки разрыва. Приближение к точкам разрыва приводит к тому, что значение амплитуды компонент может стать недопустимо высоким. Заметим, если диапазон значений ξ не захватывает точку (12), знаменатель y_1 не будет равен нулю. При этом, с учетом условий (10) и (11) знаменатель y_2 также не будет равен нулю.

На рисунке 1 приведены зависимости маскирующего сигнала и сигналов передаваемых компонент y_1 и y_2. Видно, что форма сигналов компонент сходна с формой маскирующего сигнала. При заданных параметрах системы коэффициенты корреляции компонент и полезного сигнала равны 0,38, что говорит об удовлетворительном сокрытии сигнала. При внесении в значения коэффициентов ошибки, равной $\delta = 1 \cdot 10^{-10}$, получены зависимости, приведенные далее. Заметим, что характер зависимостей при внесении ошибки в коэффициенты первой и второй компонент сходен. Поэтому на рисунках представлены только зависимости, полученные при внесении ошибки в коэффициенты первой компоненты.

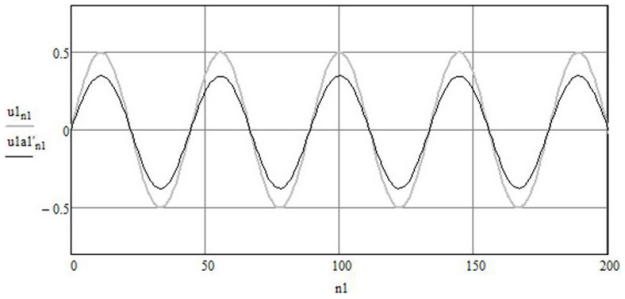

Рисунок 2. Исходный и декодированный информационные сигналы при ошибке в коэффициенте a_1

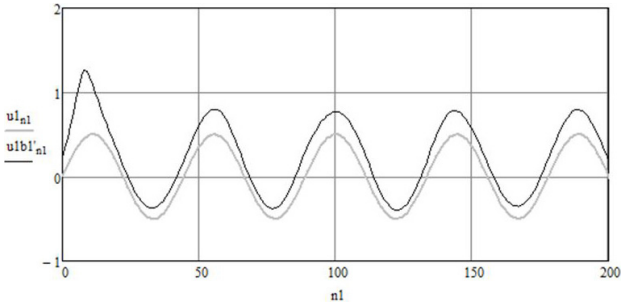

Рисунок 3. Исходный и декодированный информационные сигналы при ошибке в коэффициенте b_1

На рисунке 2 приведены графики исходного и восстановленного сигналов при внесении ошибки в коэффициент a_1. Видно, что в этом случае, помимо постоянной составляющей, имеет место искажение сигнала, однако отсутствует маскировка случайным сигналом. Следовательно, использование в качестве ключа коэффициентов a в данном алгоритме восстановления допустимо, но малоэффективно.

На рисунке 3 показаны графики исходного и восстановленного сигналов при внесении ошибки в коэффициент b_1. Видно, что в этом случае, помимо изменения амплитуды, имеет место искажение сигнала, однако отсутствует маскировка случайным сигналом. Следовательно, использование в качестве ключа коэффициентов a в данном алгоритме восстановления допустимо, но малоэффективно.

На рисунке 4 построены графики исходного и восстановленного сигналов при внесении погрешности в коэффициент c_1. Видно, что в этом случае информативный сигнал маскируется случайным сигналом, но при данных значениях ключа амплитуда случайного сигнала достаточно мала и слабо изменяется при изменении вносимой ошибки. Таким образом, использование коэффициента c в качестве ключа допустимо, но также малоэффективно.

При внесении ошибки в коэффициент K при декодировании появляется постоянная состав-

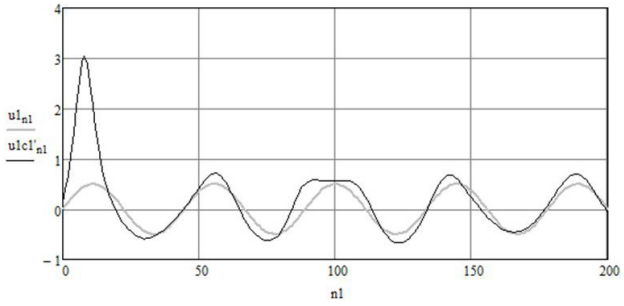

Рисунок 4. Исходный и декодированный информационные сигналы при ошибке в коэффициенте c_1

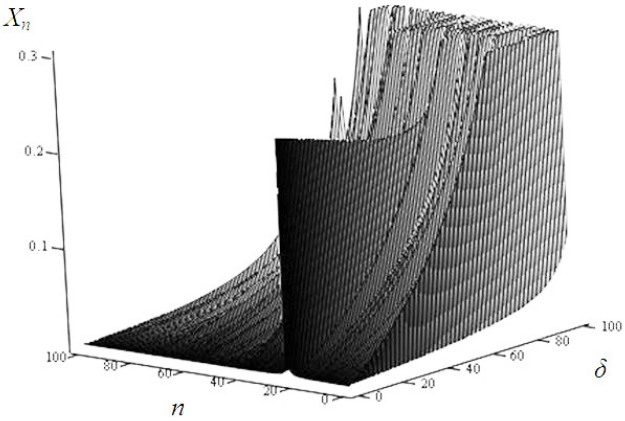

Рисунок 5. Зависимость спектра восстановленного сигнала от ошибки, внесенной в коэффициент c_1

ляющая, которая легко исключается из сигнала. Следовательно, использование в качестве ключа коэффициента K в данном алгоритме восстановления исключается.

Рассмотрим влияние изменения ошибки значения коэффициента c на спектр восстановленного сигнала. На рисунке 5 приведена поверхность, показывающая изменение спектра восстановленного сигнала от ошибки $\delta = 1 \cdot 10^{-10}$ в значении коэффициента c_1 от изменения δ. Видно, что при нулевой ошибке спектр состоит из одной гармоники. При увеличении ошибки гармоника информативного сигнала скрывается в спектре случайного сигнала.

Отметим, что при $\sigma = 10^{-9}$ и ошибке значения $c_1 = 8 \cdot 10^{-10}$ гармоника информативного сигнала полностью скрывается в спектре маскирующего сигнала.

Выводы

1. Использование алгоритма маскировки сигнала, описываемого выражениями (3), является эффективным.

2. Использование коэффициентов c_1 и c_2 в качестве ключа обеспечивает наибольшую устойчивость системы.

3. Для обеспечения сокрытия полезного сигнала необходимо задавать достаточно малые значения коэффициента a_1, что может привести к потере данных при округлении.

Литература

1. Шакурский М.В. Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 2 (121). С. 8–13.
2. Шакурский В.К., Шакурский М.В. Сжимающие отображения в инвариантных преобразователях и системах стеганографии. Самара: СНЦ РАН, 2014. 159 с.
3. Шакурский М.В. Формирование контейнера для стеганографической системы на основе сжимающих отображений // Радиотехника. 2015. № 2. С. 134–139.
4. Шакурский М.В., Шакурский В.К. Стеганографическая система на основе сжимающих отображений // Вопросы защиты информации. 2015. № 2. С. 74–78.
5. Шакурский М.В., Шакурский В.К. Оценка стойкости двухкомпонентной стеганографической системы // Успехи современной радиоэлектроники. 2015. № 11. С. 87–91.
6. Шакурский М.В., Шакурский В.К. Двухканальная система сокрытия информации с взаимным зашумлением каналов // Радиотехника. 2016. № 2. С. 96–99.
7. Патент РФ 2546307. Шакурский М.В., Шакурский В.К. Устройство сокрытия информации. № 2014123943/08, заявл. 10.06.2014, опубл. 10.04.2015. Бюл. № 10.
8. Патент РФ 2546306. Шакурский М.В., Шакурский В.К. Способ скрытой передачи информации. № 2014123912/08, заявл. 10.06.2014, опубл. 10.04.2015. Бюл. № 10.
9. Патент РФ 167074. Шакурский М.В. Устройство сокрытия информации. № 2016102913/08, заявл. 28.01.2016, опубл. 20.12.2016. Бюл. № 35.
10. Патент РФ 174362. Шакурский М.В., Шакурский В.К., Козловский В.Н., Сорокин А.Г. Устройство сокрытия информации. № 2017109750, заявл. 23.03.2017, опубл. 11.10.2017. Бюл. № 29.

Получено 20.01.2020

Шакурский Максим Викторович, к.т.н., доцент кафедры теоретической и общей электротехники Самарского государственного технического университета. 443001, Российская Федерация, г. Самара, ул. Молодогвардейская, 224. Тел. +7 927 772-98-73. E-mail: m.shakurskiy@gmail.com

TWO-COMPONENT STEANOGRAPHIC SYSTEM BASED ON RATIO OF LINEAR FUNCTIONS OF TWO SIGNALS USING AN ADDITIVE TYPE OF EMBEDDED SIGNAL COMMUNICATION

Shakurskiy M.V.
Samara State Technical University, Samara, Russian Federation
E-mail: m.shakurskiy@gmail.com

The implementation of a two-component container can significantly expand the capabilities of known steganographic methods due to occurrence of new properties. A two-component container consists of two functions of two variables, one of which is a hidden signal and the other is a container signal. The article considers the functions of component formation based on the ratio of the linear functions of two signals. The expressions for forming the components and the expression for restoring the hidden signal are ratios and have break points. It requires analysis and determination of the conditions for the formation of the container. The article presents the results of the analysis of a two-component steganographic system with a non-linear container in the area of the break of the restore function of the informative signal. Key coefficients are determined from the point of view of ensuring the greatest sensitivity of the system to the error introduced in the value of the coefficient. An analysis is made of the influence of the error added into the key coefficient on the shape of the recovered signal.

Keywords: *two-component steganographic system, non-linear container, key coefficient, invariance to a masking signal*

DOI: 10.18469/ikt.2020.18.1.09

Shakurskiy Maxim Victorovich, Samara State Technical University, 244, Molodogvardeyskaya Street, Samara, 443001, Russian Federation; Assistant Professor of Department of Theoretical and General Electrical Engineering, PhD in Technical Science. Tel. +7 927 772-98-73. E-mail: m.shakurskiy@gmail.com

References

1. Shakurskiy M.V. Matematicheskiye modeli dvukhkomponentnykh invariantnykh steganograficheskikh sistem, ispol'zuyushchikh razlichnyye algoritmy svyazi vstraivayemykh signalov [Mathematical models of two-component invariant steganographic systems using various embedded signal coupling algorithms]. *Voprosy zashchity informatsii*, 2018, no. 2 (121), pp. 8–13. (In Russian).
2. Shakurskiy V.K., Shakurskiy M.V. *Szhimayushchiye otobrazheniya v invariantnykh preobrazovatelyakh i sistemakh steganografii* [Contraction Mapping in Invariant Transducers and Steganography Systems]. Samara: SNC RAN, 2014, 159 p. (In Russian).
3. Shakurskiy M.V. Formirovaniye konteynera dlya steganograficheskoy sistemy na osnove szhimayushchikh otobrazheniy [Forming a container for a steganographic system based on compressive mappings]. *Radiotekhnika*, 2015, no. 2, pp. 134–139. (In Russian).
4. Shakurskiy M.V., Shakurskiy V.K. Steganograficheskaya sistema na osnove szhimayushchikh otobrazheniy [Steganography system based on contraction mapping]. *Voprosy zashchity informatsii*, 2015, no. 2, pp. 74–78. (In Russian).
5. Shakurskiy M.V., Shakurskiy V.K. Otsenka stoykosti dvukhkomponentnoy steganograficheskoy sistemy [Evaluation of the durability of a two-component steganographic system]. *Uspekhi sovremennoy radioelektroniki*, 2015, no. 11, pp. 87–91. (In Russian).
6. Shakurskiy M.V., Shakurskiy V.K. Dvukhkanal'naya sistema sokrytiya informatsii s vzaimnym zashumleniyem kanalov [The dual-channel system of concealment of information with mutual channel noising]. *Radiotekhnika*, 2016, no. 2, pp. 96–99. (In Russian).
7. Patent RF. no. 2546307. Shakurskiy M.V., Shakurskiy V.K. *Ustrojstvo sokrytiya informacii* [Information hiding device]. No. 2014123943/08, decl. 10.06.2014, publ. 10.04.2015. Bul. no. 10.
8. Patent RF. no. 2546306. Shakurskiy M.V., Shakurskiy V.K. Sposob skrytoj peredachi informacii [The method of covert information transfer]. No. 2014123912/08, decl. 10.06.2014, publ. 10.04.2015. Bul. no. 10.
9. Patent RF. no. 167074. Shakurskiy M.V. Ustrojstvo sokrytiya informacii [Information hiding device]. No. 2016102913/08, decl. 28.01.2016, publ. 20.12.2016. Bul. no. №35.
10. Patent RF. no. 174362. Shakurskiy M.V., Shakurskiy V.K., Kozlovskijy V.N., Sorokin A.G. Ustrojstvo sokrytiya informacii [Information hiding device]. No. 2017109750, decl. 23.03.2017, publ. 11.10.2017. Bul. no. 29.

Received 20.01.2020

УДК 004.725.5

КОРПОРАТИВНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ: ПРОЦЕДУРЫ АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ

Василенко К.А.[1], Золкин А.Л.[2], Абрамов Н.В.[3], Курганов Д.О.[3]

[1] Владивостокский государственный институт экономики и сервиса, Владивосток, РФ

[2] Волжский государственный университет водного транспорта (Самарский филиал), Самара, РФ

[3] Дальневосточный федеральный университет, Владивосток, РФ

E-mail: k2857@mail.ru, alzolkin@list.ru, nikolay.abramov1990@mail.ru, kurganov_vl@mail.ru

В статье рассматриваются проблемы защиты персональных данных и информации от злоумышленников, способы аутентификации и идентификации в корпоративных сетях. Приведены различные методы аутентификации и идентификации в компьютерных сетях. Авторами проведен их сравнительный анализ, выделены особенности и недостатки в различных сферах использования, при этом проанализированы риски и возможный ущерб от нарушения конфиденциальности данных. Величина нарушений конфиденциальности, доступности и целостности информации с каждым годом все больше растет, вместе с тем растет и нанесенный ущерб, что вызывает необходимость у специалистов информационной безопасности все тщательней и углубленно вести анализ всех рисков незаконного доступа к информации, а затем прибегать к внедрению современных средств аутентификации, использовать новые методы шифрования, все чаще генерировать новые пароли доступа к системе. На сегодняшний день существует множество способов и методов аутентификации, но специфика их применения зависит от расположения хранилища информации и ее ценности. Между тем методы аутентификации не являются безупречными методами защиты, они также уязвимы, иногда многое зависит от навыков злоумышленников.

Ключевые слова: *корпоративные вычислительные сети, пароли, токены, аутентификация, идентификация, информационная безопасность, алгоритм действия*