ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION PROTECTION

УДК 004.056.5
https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Поступила в редакцию 16.12.2019
Received 16.12.2019

Принята к публикации 21.02.2020
Accepted 21.02.2020

Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей

М. Л. Радюкевич[1]✉, В. Ф. Голиков[2]

[1]Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», Минск, Беларусь
✉E-mail: 1218a@list.ru

[2]Белорусский национальный технический университет, Минск, Беларусь

Аннотация. Рассматриваются основные варианты формирования общего секрета с использованием синхронизируемых искусственных нейронных сетей и возможные модели поведения криптоаналитика. Для решения задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа, предлагается применять смешивание некоторого числа результатов отдельных синхронизаций (свертку). В качестве функции смешивания рассматривается свертка векторов весовых коэффициентов сетей побитовым сложением по модулю 2 всех результатов отдельных синхронизаций. Показывается, что вероятность успеха криптоаналитика уменьшается экспоненциально с увеличением количества слагаемых в свертке и может быть выбрана сколь угодно малой. При этом закон распределения сформированного ключа после свертки близок к равномерному, а равномерность возрастает с увеличением количества слагаемых в свертке.

Ключевые слова: синхронизируемые искусственные нейронные сети, общий секрет, криптографический ключ, функция сжатия, криптоанализ

Для цитирования. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Информатика. – 2020. − Т. 17, № 1. – С. 102–108. https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks

Maryna L. Radziukevich[1]✉, Vladimir F. Golikov[2]

[1]Scientific Production-Republican Unitary Enterprise "Research Institute for the Technical Protection of Information", Minsk, Belarus
✉E-mail: 1218a@list.ru

[2]Belarusian National Technical University, Minsk, Belarus

Abstract. The main options for the formation of a shared secret using synchronized artificial neural networks and possible patterns of behavior of a cryptanalyst are considered. To solve the problem of increasing the confidentiality of the generated shared secret, if it is used as a cryptographic key, it is proposed to use the mixing a certain number of results of individual synchronizations (convolution). As a mixing function, we

consider the convolution of the vectors of network weights by bitwise addition modulo 2 of all the results of individual synchronizations. It is shown that the probability of success of a cryptanalyst is reduced exponentially with an increase of the number of terms in the convolution and can be chosen arbitrarily small. Moreover, the distribution law of the generated key after convolution is close to uniform and the uniformity increases with the number of terms in the convolution.

Key words: synchronized artificial neural networks, shared secret, cryptographic key, compression function, cryptanalysis

For citation. Radziukevich M. L., Golikov V. F. Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks. *Informatics*, 2020, vol. 17, no. 1, pp. 102−108 (in Russian). https://doi.org/10.37661/1816-0301-2020-17-1-102-108

Введение. Формирование общего секретного числа с помощью синхронизируемых искусственных нейронных сетей (СИНС) предложено в работах [1, 2], анализировалось в статье [3], развивалось и конкретизировалось в публикациях [4–6]. Основное достоинство данной технологии в случае ее использования в криптографических приложениях состоит в простоте реализации и исключении применения классических однонаправленных математических функций, обеспечивающих конфиденциальность формируемых криптографических ключей. Между тем процесс формирования общего секретного числа по технологии СИНС носит стохастический характер, поэтому уровень его секретности может оказаться недостаточным для использования в ответственных криптосистемах [6]. Для преодоления указанного недостатка представляет интерес модификация технологии СИНС.

Основные варианты формирования общего секрета и модели поведения криптоаналитика.

Протокол AB-1 включает несколько пунктов:

1. Абоненты A и B, формирующие общее секретное число с помощью СИНС [7], выбирают предельное число тактов синхронизации d, обеспечивающее при выбранных параметрах своих ИНС (n – количество входов каждого персептрона, K – количество персептронов, $\pm L$ – интервал возможных значений весовых коэффициентов персептронов) достижение полной синхронизации сетей с высокой вероятностью при следующем условии:

$$P(t_{AB} \le d) \ge P_{\text{тр}},$$

где t_{AB} – число тактов синхронизации, при котором весовые коэффициенты (ВК) сетей A и B будут равны друг другу; $P_{\text{тр}}$ – требуемая вероятность синхронизации. Число d определяется по результатам моделирования для сетей с выбранными параметрами [7].

2. Абоненты A и B случайным образом выбирают начальные значения ВК $\vec{W}^A(0)$, $\vec{W}^B(0)$ и проводят d тактов синхронизации, а также фиксируют значения векторов ВК своих сетей $\vec{W}^A(d)$, $\vec{W}^B(d)$, не оглашая их.

3. Абоненты A и B определяют совпадение полученных векторов одним из возможных способов. Например, абонент A может зашифровать сформированным ключом некий секретный текст и отправить его B. Если B правильно его расшифрует, то ключи совпадают. Возможен вариант, когда абонент A по договоренности с B выбирает надежный алгоритм шифрования и шифрует им $\vec{W}^A(d)$, используя в качестве ключа часть этого вектора. Абонент B, действуя аналогично, расшифровывает и сравнивает полученный результат с $\vec{W}^B(d)$. Если оказалось, что $\vec{W}^A(d) = \vec{W}^B(d)$, то общий секрет $S^{AB} = \vec{W}^A(d) = \vec{W}^B(d)$.

4. Если окажется, что $\vec{W}^A(d) \ne \vec{W}^B(d)$, то сеанс синхронизации повторяется с новыми значениями $\vec{W}^A(0)$, $\vec{W}^B(0)$ до тех пор, пока не закончится успешно.

Оценим необходимое количество синхронизаций сетей A и B для получения хотя бы одного успеха. Поскольку каждая синхронизация проводится в одинаковых условиях, а вероятность успеха каждой синхронизации $P_{AB} = P(t_{AB} \le d)$ и синхронизации не зависят друг от друга, то количество успешных синхронизаций имеет биномиальный закон распределения вероятностей

$$P(i = l) = C_m^l \; P_{AB}^l \; (1 - P_{AB})^{m-l},$$

где m – количество синхронизаций; l – количество успешных синхронизаций, l = 0, 1, 2, …, m.

Вероятность получения хотя бы одного успеха в серии из m определяется выражением

$$P(l \geq 1) = \sum_{l=1}^{m} C_m^l \; P_{AB}^l \; (1 - P_{AB})^{m-l} = 1 - P(l = 0) = 1 - (1 - P_{AB})^m.$$

Если задать нижнюю границу $P_{\text{тр}}$ этой вероятности, то можно рассчитать число синхронизаций m_{AB}, которое обеспечит появление хотя бы одной успешной синхронизации:

$$1 - (1 - P_{AB})^{m_{AB}} \; \geq P_{\text{тр}},$$

где $m_{AB} \geq \frac{\ln(1-P_{\text{тр}})}{\ln(1-P_{AB})}$.

На практике синхронизации можно проводить последовательно до первого успеха, а значение m_{AB} просто указывает на возможное их число. В табл. 1 приведены значения m_{AB} для различных вероятностей P_{AB} и $P_{\text{тр}}$.

Таблица 1

Количество сеансов синхронизации для обеспечения необходимых значений вероятностей

P_{AB} \ $P_{\text{тр}}$	0,70	0,80	0,90	0,95	0,99
0,90	2	2	1	1	1
0,95	3	2	2	1	1
0,99	4	3	2	2	1

Протокол ABE-1 заключается в следующем. Криптоаналитик *E*, прослушивая канал связи между *A* и *B*, синхронизирует свою сеть, например, с сетью *A*. Для сеанса, в котором оказалось, что *A* и *B* достигли синхронизации и подтвердили, что $\vec{W}^A(d) = \vec{W}^B(d)$, криптоаналитик *E* проверяет совпадение $\vec{W}^E(d)$ с $\vec{W}^A(d)$, если это возможно при выбранном *A* и *B* варианте сравнения, либо предполагает, что $\vec{W}^E(d) = \vec{W}^A(d)$. Вероятность совпадения $\vec{W}^E(d)$ с $\vec{W}^A(d)$ обозначим как $P_{EA} = P(t_{EA} \leq d)$. Результаты имитационного моделирования [7] показывают, что эта вероятность существенно зависит от параметров сети, выбранных *A* и *B*. Структура сети криптоаналитика *E* и ее параметры, как это указывалось ранее, должны быть полностью идентичны структуре и параметрам сетей абонентов *A* и *B*, а поскольку абоненты *A* и *B* хотят защитить конфиденциальность формируемого секрета от *E*, то они должны, учитывая наличие сети криптоаналитика *E*, выбирать такие параметры, которые обеспечивают высокие значения P_{AB} при минимально возможных значениях P_{EA}. Однако при относительно приемлемом предельном числе тактов $d \leq 5000$ не удается снизить вероятность P_{EA} меньше чем до (0,01–0,05), что может не соответствовать заданным криптографическим требованиям.

Повышение секретности. Из изложенного выше следует актуальность задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа. Идея такого метода в самом обобщенном виде в терминах информационно-вероятностного подхода изложена в работе [8]: «…усиление секретности – это искусство выделения секретной совместно используемой информации, возможно, для использования в качестве криптографического ключа, из большого объема совместно используемой информации, которая является частично секретной». Иначе говоря, если *A* и *B* имеют общую секретную информацию *W*, а *E* известна ее некоторая часть *V* (*A* и *B* не знают, какая), то, преобразовав *W* специальным образом, можно свести *V* к сколь угодно малой величине, пожертвовав размером *W*.

Постановка задачи усиления секретности следующая. Абоненты *A* и *B* сформировали секретный ключ *W* в виде битовой строки размером *n*. Криптоаналитик *E*, прослушивая процесс формирования ключа, имеет информацию *V*, коррелированную с *W* и дающую знание *t* бит из *n*, т. е. условная энтропия для криптоаналитика $H(W/V) \geq n - t$. Абоненты *A* и *B* хотят публично выбрать функцию сжатия g: $\{0, l\}^n$ в $\{0, l\}^b$, чтобы частичная информация *E* о *W* и ее полная информация о g дали произвольно мало информации о $K = g(W)$.

В работе [8] доказано, что при наличии некоторых ограничений можно выбрать функцию сжатия *G*, назначив $s < n - t$, и преобразовать $\{0,1\}^n$ в $\{0,1\}^b$, где $b = n - t - s$. Увеличивая *s* и публично выбирая функцию сжатия g из множества *G*, можно экспоненциально уменьшать информацию *E* о новом значении ключа *K*, правда, меньшего размера. Этот подход конкретизирован для формирования общего ключа с использованием квантового канала [9] и интерпретирован в монографии [10]. Применительно к рассматриваемой задаче исходная ситуация следующая. Абоненты *A* и *B* согласно протоколу *AB*-1 сформировали битовые строки S^A, S^B, по их мнению, секретным образом. Однако криптоаналитик *E*, используя протокол *ABE*-1, сформировал битовую строку S^E, которая с вероятностью P_{EA} совпадает с S^A. Для использования идеи повышения секретности абоненты *A* и *B* вместо одной строки формируют *r* строк, повторяя *r* раз пп. 1 и 2 протокола *AB*-1, но без проверки совпадения битовых строк для каждого сеанса. Абоненты *A* и *B* предполагают, что некоторое число строк S^A может совпадать с S^E, и, чтобы исключить это, сжимают полученные строки в итоговую строку заданного размера:

$$\{S_1^A, S_2^A, \ldots, S_r^A\}^{rb} \to \{K^A\}^b, \quad \{S_1^B, S_2^B, \ldots, S_r^B\}^{rb} \to \{K^B\}^b,$$

где b – длина $S_i^{A(B)}$ в битах. Далее *A* и *B* проверяют идентичность сформированных строк K^A и K^Bодним из способов, описанных ранее, а в случае совпадения имеют общий секрет $K^{AB} = K^A = K^B$.

При такой стратегии абонентов *A* и *B* криптоаналитик *E* вынужден выполнять те же операции, что *A* и *B*, в итоге получает $\{S_1^E, S_2^E, \ldots, S_r^E\}^{rb} \to \{K^E\}^b$ и может сравнить K^E с K^B. Однако строка $\{S_1^E, S_2^E, \ldots, S_r^E\}^{rb}$ с высокой вероятностью содержит хотя бы один элемент S_i^E, не совпадающий с S_i^A. Таким образом, параметр *r* в данном алгоритме имеет смысл параметра *s* из работы [8].

Анализ безопасности сформированного секрета. Оценим безопасность K^{AB}. Так как *A* и *B* провели *r* независимых сеансов синхронизации, не проверяя их результатов, вероятность того, что все сеансы закончились успехом, определяется выражением

$$P_{AB,r} = \prod_{i=1}^{r} P_{ABi} = (P_{AB})^r.$$

Согласно протоколу *AB*-1 следует обеспечить $P_{AB,r} \geq P_{\text{тр}}$. Для этого может понадобиться $m_{AB,r}$ серий по *r* синхронизаций в каждой. По аналогии с m_{AB} получим неравенство

$$m_{AB,r} \geq \frac{\ln(1 - P_{\text{тр}})}{\ln(1 - P_{AB,r})}.$$

В табл. 2 приведены значения $m_{AB,r}$, рассчитанные для вероятности $P_{\text{тр}} = 0{,}95$ и различных значений r и P_{AB}.

Таблица 2

Количество сеансов синхронизации *A* и *B* при различных значениях *r* для обеспечения необходимых значений вероятностей

r \ P_{AB}	0,8	0,90	0,95	0,99
5	8	4	3	1
10	27	7	4	2
20	259	24	7	2
50	209 895	580	38	4

Криптоаналитик E участвует во всех сеансах синхронизаций, которые проводят A и B, и останавливается в той серии, когда A и B получили K^{AB}. Вероятность того, что значение K^E совпадет со значением K^{AB}, определяется выражением $P_{EA,r} = \prod_{i=1}^{r} P_{EAi} = (P_{EA})^r$. Значения этой вероятности приведены в табл. 3.

Таблица 3

Вероятность совпадения значения K^E со значением K^{AB} при разных значениях P_{EA} и r

P_{EA} \ r	5	10	20	50
0,01	$1{,}0 \cdot 10^{-10}$	$1{,}0 \cdot 10^{-20}$	$1{,}0 \cdot 10^{-40}$	$1{,}0 \cdot 10^{-100}$
0,05	$3{,}1 \cdot 10^{-7}$	$9{,}7 \cdot 10^{-14}$	$9{,}5 \cdot 10^{-27}$	$8{,}8 \cdot 10^{-66}$
0,10	$1{,}0 \cdot 10^{-5}$	$1{,}0 \cdot 10^{-10}$	$1{,}0 \cdot 10^{-20}$	$1{,}0 \cdot 10^{-50}$
0,20	$3{,}2 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-7}$	$1{,}0 \cdot 10^{-14}$	$1{,}1 \cdot 10^{-35}$

Если, например, абоненты A и B выбрали K = 3, N = 1000, L_1 = 8, L_2 = –7, d = 3500, $P_{\text{тр}}$ = 0,95, а по результатам моделирования P_{AB} = 0,951 и P_{EA} = 0,043, то при r = 50 необходимое количество серий синхронизаций m_{AB} = 38. При этом $P_{EA,r} = 8{,}8 \cdot 10^{-66}$.

Таким образом, величина $P_{EA,r}$ зависит от r экспоненциально и может быть выбрана сколь угодно малой путем увеличения r, в то время как для A и B вероятность успешного сеанса поддерживается за счет увеличения m_{AB}. Вместе с тем надо иметь в виду, что описанный эффект будет иметь место при таких параметрах сетей абонентов A и B, когда имеет место $P_{EA,r} \ll 1$, а $P_{AB,r} \approx 1$.

Возникает вопрос о выборе вида функции $K = g(S_1, S_2, \ldots, S_r)$, т. е. выборе функции свертки, и о плате за полученное увеличение конфиденциальности. В качестве функции свертки можно выбирать любое преобразование, свертывающее множество размером rb в r, при котором выходная величина зависит от всех битов входной. Таким свойством обладают, например, хеш-функции, в том числе и стандартизованного типа (СТБ 34.101.31–2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности). Однако стандартизованные хеш-функции имеют стандартные размеры выходных величин, которые будут ограничивать размер сформированного секрета, поэтому можно использовать и другие преобразования. Например, можно применять свертку побитовым сложением по модулю 2 всех битов множества $\{S_i\}$:

$$K^{A(B)} = \sum_i^r S_i^{A(B)} (\text{mod } 2).$$

В результате получаем битовую последовательность длиной b, в которой каждый бит – сумма битов по модулю 2 из r слагаемых.

Размер сформированного секрета в битах будет равен размеру вектора ВК сетей абонентов A и B, который легко может быть изменен в случае необходимости изменением K или N. Важным положительным моментом является то, что закон распределения сформированного ключа близок к равномерному, причем равномерность возрастает с ростом r. В табл. 4 приведены значения отклонений частот повторения десятичных чисел, составляющих K^{AB}, от равномерного значения, выраженные в процентах. Данные отклонения были получены моделированием для K = 3, N = 1000, $L_1 = -7$, L_2 = 8, d = 3500, $r = 10$. В табл. 4 значение Δ_i рассчитывается по формуле

$$\Delta_i = \frac{(f_i - f_0)}{f_0} \cdot 100,$$

где f_i – частота i-го значения, f_0 – частота при равномерном распределении $f_0 = \frac{1}{L_2 - L_1 + 1} = 0{,}0625$, j_i – значение чисел из диапазона $[L_1, L_2]$. (Отрицательные значения чисел из всего диапазона $j_{i\,\text{исх}}$ переведены в положительные для правильности подсчета при моделировании.)

Таблица 4

Отклонение вероятности от равномерного распределения

j_i	0	1	2	3	4	5	6	7
$j_{i\text{исх}}$	0	1	2	3	4	5	6	7
Δ, %	–0,04	–0,17	0,26	0,34	–0,26	0,21	–0,27	–0,08
j_i	8	9	10	11	12	13	14	15
$j_{i\text{исх}}$	8	–1	–2	–3	–4	–5	–6	–7
Δ, %	–0,03	–0,42	0,35	0,41	–0,16	0,03	–0,03	0,38

Незначительная неравномерность, зафиксированная при моделировании, скорее всего, объясняется его ограниченным объемом (10^3 серий по 10 сеансов в каждой).

Заключение. Для решения задачи повышения конфиденциальности формируемого общего секрета, если он будет использоваться в качестве криптографического ключа, предлагается применять функцию сжатия g. В настоящей работе в качестве функции сжатия была рассмотрена свертка побитовым сложением по модулю 2 всех элементов множества $S_i^{A(B)}$. Таким образом, вероятность успеха $P_{EA,r}$ криптоаналитика зависит от величины r экспоненциально и может быть выбрана сколь угодно малой за счет увеличения r, в то время как для абонентов A и B вероятность успешного сеанса поддерживается за счет увеличения m. Закон распределения сформированного ключа после функции сжатия близок к равномерному, причем равномерность возрастает с увеличением r.

Список использованных источников

1. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. − 2005. – Vol. 5, no. 1. – P. 130−140.

2. Kinzel, W. Neural cryptography / W. Kinzel, I. Kanter // 9th Intern. Conf. on Neural Information Processing, Singapore, 2002. – Singapore, 2002. – Vol. 3. – P. 1351–1354.

3. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, W. Kinzel // Physical Review E. – 2007. – Vol. 75, iss. 5. – P. 1–9.

4. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович ; под ред. И. М. Жарского // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск : БГТУ, 2005. – С. 161–164.

5. Голиков, В. Ф. О некоторых проблемах в задачах распределения криптографических ключей с помощью искусственных нейронных сетей / В. Ф. Голиков, Н. В. Брич, В. Л. Пивоваров // Системный анализ и прикладная информатика. – 2014. – № 1–3. – С. 42–46.

6. Голиков, В. Ф. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР. – 2017. – № 8. – С. 48–53.

7. Голиков, В. Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В. Ф. Голиков, М. Л. Радюкевич // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 49–56.

8. Generalized privacy amplification / C. H. Bennett [et al.] // IEEE Transaction on Information Theory. – 1995. – Vol. 41, no. 6. – P. 1915–1923.

9. Боумейстер, Д. Физика квантовой информации / Д. Боумейстер, А. Экерт, А. Цайлингер. – М. : Постмаркет, 2002. – 276 с.

10. Килин, С. Я. Квантовая криптография: идеи и практика / С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. – Минск : Беларус. навука, 2007. – 391 с.

References

1. Kanter I., Kinzel W. *The Theory of Neural Networks and Cryptography, Quantum Computers and Computing*, 2005, vol. 5, no. 1, pp. 130−140.

2. Kinzel W., Kanter I. Neural cryptography. *9th International Conference on Neural Information Processing, Singapore, 2002*. Singapore, 2002, vol. 3, pp. 1351–1354.

3. Ruttor A., Kanter I., Kinzel W. Dynamics of neural cryptography. *Physical Review E*, 2007, vol. 75, iss. 5, pp. 1–9.

4. Plonkovski M., Urbanovich P. P., Zharsky I. M. (ed.). Kriptograficheskoye preobrazovaniye informatsii na osnove neyrosetevykh tekhnologii [Cryptographic transformation of information based on neural network technology]. Trudy Belorusskogo gosudarstvennogo tehnologicheskogo universiteta. Ser. VI. Fiziko-matematicheskiye nauki i informatika [*Proceedings of the Belarusian State Technical University. Ser. VI. Physics and Mathematics and Computer Science*]. Minsk, Belarusian State Technical University, 2005, pp. 161–164 (in Russian).

5. Golikov V. F., Brich N. V., Pivovarov V. L. O nekotorykh problemakh v zadachakh raspredeleniya kriptograficheskikh klyuchey s pomoshch'yu iskusstvennykh neyronnykh setey [About some problems in the distribution of cryptographic keys using artificial neural networks]. Sistemnyy analiz i prikladnaya informatika [*System Analysis and Applied Informatics*], 2014, no. 1–3, pp. 42–46 (in Russian).

6. Golikov V. F., Ksenevich A. Yu. Ataka na sinkhroniziruyemyye iskusstvennyye neyronnyye seti, formiruyushchiye obshchiy sekret, metodom otlozhennogo perebora [Attack on synchronized artificial neural networks, forming a common secret, by delayed brute force method]. Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radiojelektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2017, no. 8, pp. 48–53 (in Russian).

7. Golikov V. F., Radziukevich M. L. Formirovaniye obshchego sekreta s pomoshch'yu iskusstvennykh neyronnykh setey [The formation of a common secret using artificial neural networks]. Sistemnyy analiz i prikladnaya informatika [*System Analysis and Applied Informatics*], 2019, no. 2, pp. 49–56 (in Russian).

8. Bennett C. H., Brassard G., Crepeau C., Maurer U. M. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 1995, vol. 41, no. 6, pp. 1915–1923.

9. Boumeyster D., Ekert A., Tsaylinger A. Fizika kvantovoy informatsii. *Physics of Quantum Information*. Moscow, Postmarket, 2002, 276 p. (in Russian).

10. Kilin S. Ya., Khoroshko D. B., Nizovtsev A. P. Kvantovaya kriptografiya: idei i praktika. *Quantum cryptography: Ideas and Practice*. Minsk, Belaruskaya navuka, 2007, 391 p. (in Russian).

Информация об авторах

Радюкевич Марина Львовна, магистр технических наук, начальник испытательной лаборатории по требованиям безопасности информации, Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», Минск, Беларусь, победитель конкурса молодых ученых на XXIV научно-практической конференции «Комплексная защита информации».
E-mail: 1218a@list.ru

Голиков Владимир Федорович, доктор технических наук, профессор кафедры «Информационные технологии в управлении», Белорусский национальный технический университет, Минск, Беларусь.

Information about the authors

Maryna L. Radziukevich, Master Sci. (Eng.), Head of the Testing Laboratory for Information Security Requirements, Scientific Production-Republican Unitary Enterprise "Research Institute for the Technical Protection of Information", Minsk, Belarus, Winner of the competition of young scientists at the XXIV scientific-practical conference "Comprehensive information protection."
E-mail: 1218a@list.ru

Vladimir F. Golikov, Dr. Sci. (Eng.), Professor of the Department of Information Technologies in Management, Belarusian National Technical University, Minsk, Belarus.