СПОСОБ ОБЕСПЕЧЕНИЯ УНИВЕРСАЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕСЫЛАЕМОЙ ПО КАНАЛУ СВЯЗИ

Иванов М.А.[1]

Аннотация *Отмечается трудоемкость решения задач защиты информации в условиях появления и развития новых IT-технологий, широкое распространение которых не только создает новые проблемы кибербезопасности, но и представляет, казалось бы, решенные ранее вопросы совершенно в новом ракурсе. В качестве выхода из создавшейся ситуации предлагаются методы внесения непредсказуемости в работу средств и объектов защиты, которые принято называть стохастическими. Приводится пример использования рандомизации для обеспечения универсальной защиты информации, пересылаемой по каналу связи.*

Целью *данной работы является обоснование эффективности стохастических методов защиты информации на примере обеспечения универсальной защиты информации, пересылаемой по каналу связи.*

Метод *достижения цели заключается в совместном использовании стохастического кодирования С.А. Осмоловского и Российского стандарта криптозащиты.*

Полученные результаты: *представлен способ решения всех трех задач защиты информации, возникающих при передаче данных по каналу связи, а именно: обеспечения помехоустойчивости, конфиденциальности и имитозащиты пересылаемых данных.*

Ключевые слова: *стохастические методы защиты информации, генератор псевдослучайных чисел, стохастический код, универсальная защита.*

DOI: *10.21681/2311-3456-2019-3-45-50*

1. Введение

Бурное развитие IT-технологий, появление и широкое распространение уязвимых суперкомпьютерных, мобильных, киберфизических, RFID-технологий существенно расширило возможности злоумышленников. В связи с этим возникли не только новые проблемы кибербезопасности, но и уже, казалось бы, решенные вопросы вновь проявились совершенно в новом ракурсе [1-4].

Основными угрозами кибербезопасности являются (в порядке повышения опасности и трудоемкости нейтрализации) вредоносное ПО (Malicious Software или Malware), вредоносное аппаратное обеспечение (Malicious Hardware), скрытые каналы передачи информации и воздействия на киберсистемы (Covert, Subliminal, Side Channels; Backdoors) и, наконец, использование технологий защиты по двойному назначению (например, Malicious Cryptography). При этом можно констатировать, что даже с простейшим видом вредоносного ПО, компьютерными вирусами, справиться до сих пор не удается [5].

2. Причины ненадежности киберсистем в защищенном исполнении

На первый взгляд, положение в сфере кибербезопасности кажется безнадежным. Однако надежду вселяет знание основных ошибок, которые уже были сделаны и которые можно попытаться исправить в ближайшем будущем. Можно выделить четыре основные ошибки прошлого [5].

1. Повсеместно получил распространение системный подход к решению задач защиты информации (ЗИ). Что это означает в рассматриваемом случае? Условно говоря, в рамках одной системы собираются лучшие представители традиционных средств ЗИ (IDS, межсетевой экран, антивирус, Honeypot и т.п.) и после этого считается, что она является защищенной. Однако фраза о защищенности системы будет являться справедливой в лучшем случае только в момент ее произнесения. На самом деле в задачах ЗИ системный подход не работает. Эффективная система ЗИ – это не какая-то фиксированная совокупность методов и программно-аппаратных средств, это непрерывный процесс анализа защищенности системы на всех уровнях (элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО) и опережающее совершенствование методов и средств защиты. Иначе говоря, нужен процессный, а еще лучше эволюционный подход к решению задач ЗИ.

2. Повсеместно задачи ЗИ решаются по остаточному принципу, когда новая технология, новая система, новый продукт уже созданы. В результате все сводится к латанию все новых и новых «дыр», а не к кардинальному решению проблемы. Необходимо решать задачи ЗИ одновременно с созданием новой технологии, системы или продукта. Да, это удлиняет сроки разработки и повышает стоимость продукта. Но пора задать себе простой вопрос: вокруг нас огромное количество уязвимых систем и технологий, зачем нам еще одна?

3. Очень часто используются реактивные или пассивные методы ЗИ, которые развиваются по мере появления новых механизмов проведения атак на киберсистемы, например, новых видов того же вредоносного ПО. В результате такого подхода сторона защиты хотя бы на полшага, но отстает от нападающей стороны. А учитывая, что защищаться намного сложнее, чем нападать (хотя и, несомненно, благороднее), защита всегда находится в заведомо проигрышном положении перед напа-

1 Иванов Михаил Александрович, доктор технических наук, профессор, заведующий кафедрой безопасности цифровой экономики ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Россия, E-mail: msadozen18@mail.ru.

дением. Необходима разработка проактивных или превентивных методов и средств ЗИ, механизмов защиты от активного противника. Только в этом случае можно при профессиональной реализации попытаться предоставить защите преимущество перед нападением.

4. Очень часто при проектировании алгоритмов ЗИ используется не та модель доверительных отношений, которая имеет место на практике. Например, многие криптографические алгоритмы (КА) исходят из модели черного ящика (Black Box), когда предполагается, что злоумышленнику известны в лучшем случае входная и выходная информация, ему не известен только используемый ключ, и в условиях действия именно данной модели обеспечивают требуемый уровень защиты. На практике же чаще всего имеет место модель серого ящика (Grey Box), когда в процессе работы криптоалгоритма происходит утечка информации о времени выполнения отдельных актов алгоритма, о потребляемой мощности, об особенностях работы кэша и прочее; и поэтому возможны так называемые атаки по побочным каналам (Side Channel Attacks). Реже, возможна и модель белого ящика (White Box), когда компьютер, в котором реализованы какие-либо механизмы ЗИ находится полностью в руках злоумышленника и в его распоряжении находятся сотни хакерских утилит, позволяющих «снять» любую защиту. Необходимо проектировать криптоалгоритмы, свободные от утечек по побочным каналам, иначе говоря, обеспечивающие требуемый уровень защиты в условиях действия модели серого ящика (Leakage-Resilient Cryptography, Grey Box Cryptography).

3. Стохастические методы защиты информации

Когда защита может получить преимущество перед нападением? На первый взгляд, ответ очевиден – никогда. На самом деле это не так, решение есть. И это решение называется стохастические методы ЗИ (обфускация, пермутация, полиморфизм, рандомизация). Учитывая, что любая атака начинается с исследования поведения объекта на модели, либо на реальной системе, защита может получить преимущество перед нападением в том случае, когда атакующий не понимает поведение объекта атаки и средств его защиты. Стохастическими принято называть методы ЗИ, обеспечивающие непредсказуемое поведение средств и объектов защиты. Внести непредсказуемость можно во все что угодно: в последовательность выполнения отдельных актов алгоритма, во время выполнения отдельных шагов алгоритма, в механизм функционирования и даже в результат работы алгоритма ЗИ. Базовыми элементами стохастических механизмов ЗИ являются генераторы псевдослучайных чисел (ГПСЧ) и хеш-функции, от качества которых и зависит эффективность защиты [6-8].

Наиболее известными примерами применения стохастических методов являются технологии ASLR и ISR. ASLR (Address Space Layout Randomization), рандомизация адресного пространства – технология, применяемая в операционных системах, при использовании которой непредсказуемым образом меняется расположение в адресном пространстве процесса таких важных структур данных, как образ исполняемого файла, подгружаемые библиотеки, куча и стек. ISR (Instruction Set Randomization), рандомизация набора команд – технология, позволяющая создать для каждой выполняемой программы индивидуальную среду исполнения.

Стохастические методы применяются и в криптографии. Одним из первых примеров такого рода стала технология OAEP (Optimal Asymmetric Encryption Padding). Существуют вероятностные схемы симметричного, асимметричного, гибридного шифрования, электронной цифровой подписи. Все перечисленные механизмы вносят непредсказуемость в результат работы соответствующих криптоалгоритмов [9, 10].

4. Пример стохастического метода защиты информации

Рассмотрим потенциальные возможности стохастических методов ЗИ на примере построения универсальной защиты информации, пересылаемой по каналу связи. В задачах надежной передачи данных по каналам связи для обеспечения помехозащищенности традиционно используется теория кодирования. Существует огромное множество кодов, обнаруживающих и исправляющих ошибки: коды Хэмминга, Рида-Соломона, БЧХ, Файра и другие [11, 12]. Проблема в том, что в большинстве случаев ни один из них не обеспечивает заранее заданную вероятность правильного приема информации. Речь может идти только о гарантированной доле ошибок, которые могут быть обнаружены и исправлены. Все дело в том, что все эти коды исходят из модели двоичного симметричного канала (ДСК), и только в условиях этой модели действительно по-настоящему эффективны. Однако свойства реальных каналов связи очень многообразны и чаще всего не соответствуют модели ДСК. Все ситуации, приводящие к ошибке декодирования, можно заранее зафиксировать, однако вероятности этих ситуаций рассчитать не представляется возможным.

На рис. 1 показана схема стохастического кодека С.А. Осмоловского – уникального российского изобретения, способного обеспечить универсальную защиту информации, передаваемой по каналу связи, где И – источник информации, К – кодер, R и R^{-1} – блоки соответственно прямого и обратного стохастического преобразования, ДК – декодер, Пр – приемник информации. Действие ошибок в реальном канале связи традиционно описывается элементом XOR, на одном входе которого – передаваемая информации, на другом – вектор ошибок, позиции «1» в котором соответствуют позициям искаженных бит сообщений.

Что предложил автор стохастических кодов? Раз свойства реальных каналов связи нас не устраивают, необходимо создать свой собственный виртуальный (преобразованный) канал связи с нужными нам свойствами. Автор назвал этот канал Q-ичным симметричным каналом, обосновал оптимальный выбор значения Q: $Q = 2^{32}$. Преобразованный канал связи образует «тройка» – блок R, реальный канал связи и блок R^{-1}, при этом действие преобразованного ка-

нала описывается преобразованным вектором ошибок, действующим на выходе блока R^{-1}. Параметры преобразования в блоках R и R^{-1} снимаются с выхода ГПСЧ на передающей и принимающей стороне. Свойство, которым должен обладать преобразованный канал, – все ситуации, в которых происходят ошибки декодирования, должны быть равновероятны. Только в этом случае, зная эти вероятности, можно заранее рассчитать вероятность ошибки декодирования, а значит и вероятность правильного приема информации. С.А. Осмоловский разработал целое семейство кодов (которые начали использоваться в 90-е годы) для каналов с различными свойствами с точки зрения вероятности возникновения помех [13-15].

Однако возможности стохастических кодов значительно шире, как утверждает автор, и с ним нельзя не согласиться. Они могут при соответствующей реализации обеспечить дополнительно секретность и контроль целостности передаваемой информации. Проблема в том, что указанные две дополнительные возможности в этом случае должны быть реализованы на основе использования стохастических преобразований, специфицированных в российском стандарте[2] криптозащиты [16]. А как это сделать, было непонятно.

Предлагается способ решения проблемы, а именно стохастический алгоритм обработки данных. Уравнения работы схемы преобразования данных показаны ниже. На взгляд автора, оптимальное решение – использование в качестве блоков R и R^{-1} многораундовых взаимно обратных блочных стохастических преобразований E^r (прямое) и D^r (обратное) (например, имеющих конструкцию Х. Фейстеля), а для генерации параметров стохастического преобразования – многовыходного PRNG, имеющего двухступенчатую конструкцию (Counter Mode) и специфицированного в Российском ГОСТе для реализации шифрования методом гаммирования.

Схемы прямого и обратного стохастического преобразования показаны соответственно на рис.2, a и b, а уравнения их работы имеют вид (1) и (2)

$$\begin{cases} PRS(t) = F_{out}(K, Q(t)), \\ PRS(t) = K_0 \| K_1 \| K_2 \| \dots \| K_{r-1}, \\ Q(t+1) = (Q(t)+1) \bmod M, \\ C(t) = E(K_{r-1}, (\dots E(K_2, (E(K_1, (E(K_0, P(t))))))))), \end{cases} \quad (1)$$

$$\begin{cases} PRS(t) = F_{out}(K, Q(t)), \\ PRS(t) = K_0 \| K_1 \| K_2 \| \dots \| K_{r-1}, \\ Q(t+1) = (Q(t)+1) \bmod M, \\ P(t) = D(K_0, (\dots D(K_{r-3}, (D(K_{r-2}, (D(K_{r-1}, C(t))))))))), \end{cases} \quad (2)$$

где $Q(t)$ и $Q(t+1)$ – состояние ГПСЧ, работающего в режиме счетчика, в моменты времени *t* и *(t + 1)* соответственно, $Q_0 = S_0$ – начальное состояние ГПСЧ, F_{out} – нелинейная функция выхода ГПСЧ, *M* – число состояний счетчика, *K* – секретный ключ, *PRS(t)*– элемент выходной псевдослучайной последовательности (ПСП) в момент времени *t*, K_0, K_1, ... , K_{r-1} – раундовые ключи, *r* – число раундов преобразования, *E* и *D* – соответственно прямое и обратное раундовое преобразование, *P(t)* и *C(t)* – соответственно исходный и преобразованный блок данных.

Предлагаемый вариант стохастического преобразования может рассматриваться как своеобразная модификация известных схем преобразования простой замены и гаммирования (см. табл. 1). Главный недостаток режима простой замены – преобразование всех блоков данных на одном и том же ключе по одному и тому же алгоритму. В результате при анализе преобразованных данных можно делать предположения об исходной информации, что недопустимо. В предлагаемой схеме этот недостаток «исчез», так как каждый блок открытого текста преобразуется на сво-

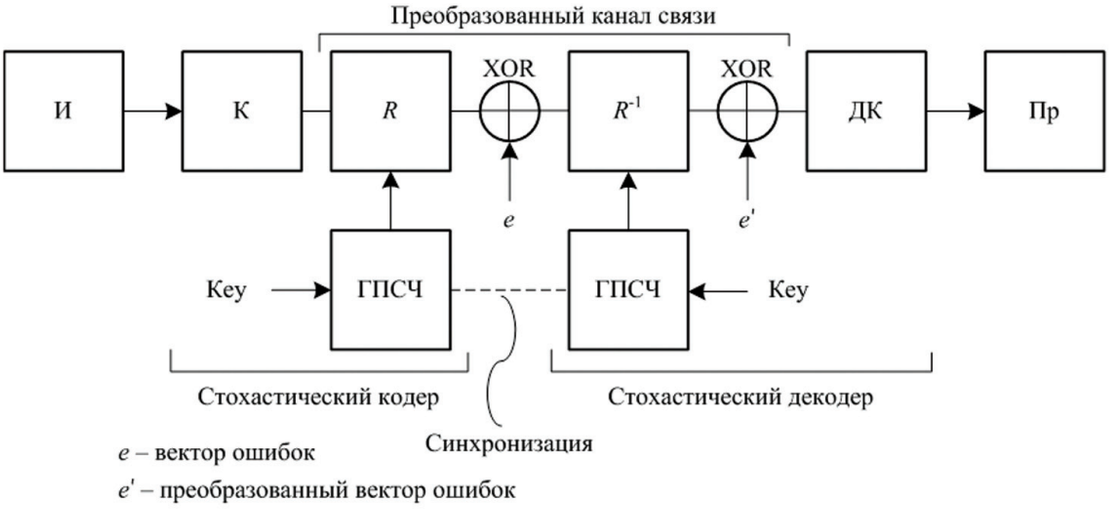

Рис. 1 – Схема системы передачи данных по каналу связи при использовании стохастического кодирования С.А. Осмоловского.

2 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

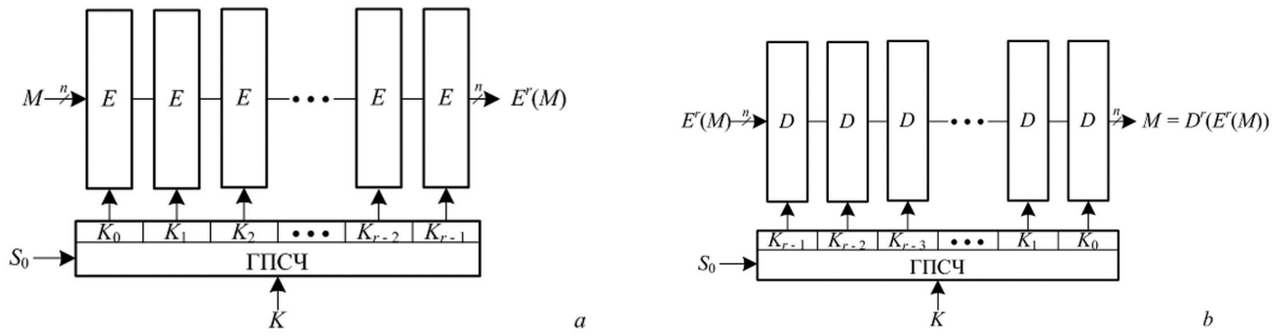

Рис. 2 – Схема стохастического преобразования: прямое (a) и обратное (b) преобразование.

Таблица 1 – Сравнение трех способов стохастического преобразования информации.

Характеристика	Режим простой замены	Режим гаммирования	Предлагаемый режим преобразования
Все элементы М преобразуются одним и тем же образом на одном и том же ключе	Да	Нет	Нет
Каждый элемент М преобразуется на своем элементе гаммы	Нет	Да	Да
Наложение псевдослучайной последовательности преобразование	Нет	Операция XOR	Стохастическое Возможность внесения
Возможность внесения предсказуемых изменений в преобразованный текст	Да	Да	Нет
Возможность контроля целостности	Нет	Нет	Да

ем элементе ПСП. Принципиальное отличие от классической схемы гаммирования: наложение ПСП на открытую информацию осуществляется не с помощью операции XOR, а с помощью сложной нелинейной функции E^r, реализующей многораундовое преобразование. В результате злоумышленник лишен возможности вносить предсказуемые изменения в преобразованный текст.

Реализация предложенной схемы передачи данных позволяет обеспечить универсальную защиту передаваемых данных. Все необходимые элементы стохастического помехоустойчивого кодирования присутствуют, а≈значит обеспечивается помехозащищенность за счет использования в схемах кодера и декодера идей Осмоловского. При этом за счет иных схем (криптографических по сути) прямого и обратного стохастического преобразования, а также ГПСЧ, специфицированного в Российском ГОСТе, обеспечивается секретность и целостность передаваемой информации.

5. Выводы

Проанализированы основные причины ненадежности киберсистем в защищенном исполнении. Предложены пути исправления ситуации на основе использования стохастических методов защиты информации, обеспечивающих непредсказуемое поведение средств и объектов защиты. Рассмотрен пример обеспечения универсальной защиты информации, пересылаемой по каналу связи, на основе использования идеи стохастического кодирования С.А. Осмоловского. Дана сравнительная характеристика традиционных способов и предлагаемого решения.

Литература

1. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” ComputerNetworks, vol. 76, pp. 146–164, 2015.
2. Internet of Things. IoT Governance, Privacy and Security Issues. European Research Cluster on the Internet of Things, January, 2015.
3. Pankaj Pathak, Nitesh Vyas. Security Challenges for Communications on IOT & Big Data. International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017, pp. 431-436.
4. A Security Framework for the Internet of Things in the Future Internet Architecture. Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe. Future Internet 2017, 9, 27.

5. Иванов М.А. Защищенные компьютерные технологии: миф или реальность? Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2015), Moscow, Russia, May 22-23, 2015, pp.300-302.
6. A. Rock. Pseudorandom Number Generators for Cryptographic Applications, Salzburg, 2005.
7. O. Goldreich, A Primer on Pseudorandom Generators, vol. 55 of University Lecture Series. Providence, RI: American Mathematical Society, 2010.
8. Georg T. Becker, Marc Fyrbiak, Christian Kison. Hardware Obfuscation. Springer, 2017.
9. V. Mao. Modern Cryptography. Theory and Practice. Prentice Hall PTR, 2003.
10. M. Bellare, S. Goldwasser, and D. Micciancio, Pseudo-Random number generation within cryptographic algorithms: The DDS case, in CRYPTO, vol. 1294 of Lecture Notes in Computer Science, pp. 277–291, Springer, 1997.
11. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ. – М.: Мир, 1976.
12. Блейхут Р. Б68 Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Книга. по Требованию, 2013. – 566 с.
13. Осмоловский С.А. Стохастические методы передачи данных. – М.: Радио и связь, 1991.
14. Осмоловский С.А. Стохастические методы защиты информации. – М.: Радио и связь, 2003.
15. Осмоловский С. А. Стохастическая информатика: инновации в информационных системах. – М.: Горячая линия-Телеком, 2011.
16. Иванов М.А., Рослый Е.Б., Стариковский А.В. Алгоритмы преобразования данных, ориентированные на использование в системах поточного шифрования и стохастического кодирования информации. Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2018), Moscow, Russia, May 29-31, 2018. pp. 332-335.

A WAY TO ENSURE UNIVERSAL PROTECTION OF INFORMAATION TRANSMITTED VIA COMMUNICATION CHANNELS

***Ivanov M.A.*[3]**

The purpose of this paper is to substantiate the effectiveness of stochastic methods for information protection through the example of universal protection of information transmitted via a communication channel.

The authors note the labor-consuming nature of handling the information protection tasks as more and more new IT technologies emerge and develop. Their wide distribution not only creates new cybersecurity problems, but also presents already seemingly solved ones from a totally new perspective. Proposed as a way out of this situation are methods for introducing unpredictability in the operation of protection means and objects, which are commonly called stochastic. An example is given of using randomization to provide universal protection of information transmitted via a communication channel.

The goal achieving method consists in combined use of S.A. Osmolovsky's stochastic coding and the Russian cryptoprotection standard.

***Results:** A method is presented for solving all the three data protection problems that arise when data is transmitted via a communication channel, i.e. noise immunity, confidentiality and falsified data entry protection.*

***Keywords:** stochastic information security methods, pseudorandom number generator, stochastic code, universal security.*

References

1. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," ComputerNetworks, vol. 76, pp. 146–164, 2015.
2. Internet of Things. IoT Governance, Privacy and Security Issues. European Research Cluster on the Internet of Things, January, 2015.
3. Pankaj Pathak, Nitesh Vyas. Security Challenges for Communications on IOT & Big Data. International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017, pp. 431-436.
4. A Security Framework for the Internet of Things in the Future Internet Architecture. Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe. Future Internet 2017, 9, 27.
5. Ivanov M.A. Zashchishchennye komp'yuternye tekhnologii: mif ili real'nost'? Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2015), Moscow, Russia, May 22-23, 2015, pp.300-302.
6. A. Rock. Pseudorandom Number Generators for Cryptographic Applications, Salzburg, 2005.
7. O. Goldreich, A Primer on Pseudorandom Generators, vol. 55 of University Lecture Series. Providence, RI: American Mathematical Society, 2010.

3 Mikhail Ivanov, Dr.Sc., Professor, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, msadozen18@mail.ru

8. Georg T. Becker, Marc Fyrbiak, Christian Kison. Hardware Obfuscation. Springer, 2017.
9. V. Mao. Modern Cryptography. Theory and Practice. Prentice Hall PTR, 2003.
10. M. Bellare, S. Goldwasser, and D. Micciancio, Pseudo-Random number generation within cryptographic algorithms: The DDS case, in CRYPTO, vol. 1294 of Lecture Notes in Computer Science, pp. 277–291, Springer, 1997.
11. Piterson U., Uehldon EH. Kody, ispravlyayushchie oshibki. Per. s angl. – M.: Mir, 1976.
12. Blejhut R. B68 Teoriya i praktika kodov, kontroliruyushchih oshibki / Blejhut R. – M.: Kniga. po Trebovaniyu, 2013. – 566 s.
13. Osmolovskij S.A. Stohasticheskie metody peredachi dannyh. – M.: Radio i svyaz', 1991.
14. Osmolovskij S.A. Stohasticheskie metody zashchity informacii. – M.: Radio i svyaz', 2003.
15. Osmolovskij S. A. Stohasticheskaya informatika: innovacii v informacionnyh sistemah. – M.: Goryachaya liniya-Telekom, 2011.
16. Ivanov M.A., Roslyj E.B., Starikovskij A.V. Algoritmy preobrazovaniya dannyh, orientirovannye na ispol'zovanie v sistemah potochnogo shifrovaniya i stohasticheskogo kodirovaniya informacii. Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2018), Moscow, Russia, May 29-31, 2018. pp. 332-335.