НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2016 Том 16 № 5 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2016 Vol. 16 No 5 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.056

ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ, ПЕРЕДАВАЕМЫХ МЕЖДУ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ И НАЗЕМНОЙ СТАНЦИЕЙ УПРАВЛЕНИЯ, НА ОСНОВЕ ШИФРА ВЕРНАМА

И.А. Авдонин[a], М.Б. Будько[a], В.А. Грозов[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: vladimirgrozov@mail.ru

Информация о статье
Поступила в редакцию 22.06.16, принята к печати 29.08.16
doi: 10.17586/2226-1494-2016-16-5-850-855
Язык статьи – русский

Ссылка для цитирования: Авдонин И.А., Будько М.Б., Грозов В.А. Организация защиты данных, передаваемых между беспилотным летательным аппаратом и наземной станцией управления, на основе шифра Вернама // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5. С. 850–855. doi: 10.17586/2226-1494-2016-16-5-850-855

Аннотация

Рассмотрены вопросы защиты от несанкционированного доступа к данным, передаваемым между беспилотным летательным аппаратом и наземной станцией управления. Это связано с тем, что стандартные средства сетевой защиты не всегда обеспечивают должный уровень безопасности или не удовлетворяют ограничениям, связанным с особенностями беспилотных летательных аппаратов – относительно небольшим объемом вычислительных ресурсов бортового компьютера беспилотного аппарата, работой в режиме реального времени. В целях введения дополнительных мер защиты данных в работе предложено использовать шифр Вернама (одноразовый блокнот), сочетающий такие преимущества, как теоретически доказанная абсолютная криптостойкость, простота программной реализации, высокая скорость шифрования, а также малая нагрузка на процессор, что особенно важно для шифрования больших объемов данных, таких как видеоинформация. В рамках проведенных экспериментальных исследований для генерации одноразового шифроблокнота использован способ получения псевдослучайной последовательности битов на основе криптографической гаммы блочного шифра ГОСТ 28147-89 в режиме гаммирования с обратной связью. Применение шифра Вернама предполагает уничтожение использованных страниц шифроблокнота. Для обеспечения этого требования и одновременной экономии памяти предложено выполнять замещение использованных страниц шифроблокнота шифротекстом. Это дает возможность использовать память, выделенную для шифроблокнота, не только для хранения ключевых последовательностей, но и для накапливания зашифрованных данных в памяти бортового компьютера. Реализация предложенного метода позволит повысить уровень защиты данных без привлечения значительной вычислительной мощности и большого объема памяти.

Ключевые слова

шифр Вернама, одноразовый шифроблокнот, шифр ГОСТ 28147-89, гаммирование с обратной связью, беспилотный летательный аппарат, наземная станция управления, защита от несанкционированного доступа

Благодарности

Исследование выполнено за счет гранта Российского научного фонда (проект №16-11-00049).

VERNAM CIPHER BASED METHOD OF PROTECTION FOR DATA TRANSFERRED BETWEEN UNMANNED AIRCRAFT AND GROUND CONTROL STATION

I.A. Avdonin[a], M.B. Budko[a], V.A. Grozov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: vladimirgrozov@mail.ru

Article info
Received 22.06.16, accepted 29.08.16
doi: 10.17586/2226-1494-2016-16-5-850-855
Article in Russian

For citation: Avdonin I.A., Budko M.B., Grozov V.A. Vernam cipher based method of protection for data transferred between unmanned aircraft and ground control station. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 5, pp. 850–855. doi: 10.17586/2226-1494-2016-16-5-850-855

Abstract

The paper deals with questions of protection against unauthorized access to the data transmitted between unmanned aircraft vehicle (UAV) and ground control station (GCS). This is due to the fact that standard instruments of network security sometimes provide security of not enough proper level or do not satisfy the restrictions connected with the features of UAV: limited computing resources of the UAV on-board computer and real-time operation. We have offered to use Vernam cipher (one-time pad) as an additional measure for data protection. Vernam algorithm combines such advantages as theoretically proved absolute cryptographic security, ease of implementation, high speed of encryption and low processor load. It is especially important for large volumes of data encryption (e.g. video information). Within the bounds of experimental researches the technique is used based on cryptographic gamma of block cipher GOST 28147-89 in the Cipher Feedback Mode for a one-time pad generation. Application of Vernam cipher means the deletion of used one-time pad pages. The replacement of used one-time pad pages by cipher text is proposed for assurance of the above-named requirement and for simultaneous computer memory saving. It gives additionally the opportunity not only to save key sequences but also to accumulate encrypted data in the on-board computer memory. Realization of the offered method allows increasing the data protection level without engaging large computing power and memory capacity.

Keywords

Vernam cipher, one-time pad, GOST 28147-89 cipher, cipher feedback mode, unmanned aircraft vehicle (UAV), ground control station, protection against unauthorized access

Acknowledgements

This study was performed under a grant by the Russian Science Foundation (Project 16-11-00049).

Введение

Одним из перспективных направлений в области интеллектуальных технологий управления и обработки информации является разработка мобильных робототехнических систем, в частности, беспилотных летательных аппаратов (БЛА). В нашей стране велик интерес к созданию и использованию БЛА. Ведутся разработки электронных компонентов, автономных источников питания; развиваются новые методы автоматического и интеллектуального управления. Одной из актуальных проблем беспилотных летательных аппаратов является обеспечение информационной безопасности при передаче данных как между приборами, узлами и модулями самого аппарата, так и между БЛА и наземной станцией управления (НСУ).

Различные вопросы, связанные с разработкой и эксплуатацией беспилотных летательных аппаратов, а также обеспечением безопасной передачи информации рассматриваются, например, в работах [1–8]. В настоящей работе рассматривается защита управляющих команд и телеметрической информации от несанкционированного доступа, так как угроза перехвата и искажения таких данных представляет наибольшую опасность с точки зрения потери управления и утраты БЛА.

Эффективным методом защиты данных является шифрование. Растущие возможности криптоаналитики и мощности применяемой вычислительной техники заставляют искать новые способы шифрования или совершенствовать уже известные [9]. Кроме того, специфика БЛА накладывает ограничения на выбор средств криптозащиты. В условиях малой несущей способности БЛА, ограниченных вычислительных ресурсов и потенциально высокой степени угроз основными критериями выбора подходящего криптоалгоритма являются его высокие криптостойкость и скорость шифрования, а также простота реализации. Этим требованиям во многом отвечает шифр Вернама (одноразовый блокнот) – единственный алгоритм, имеющий теоретически доказанную абсолютную криптостойкость [10, 11]. В последнее время опубликовано большое количество работ, использующих идею этого шифра как в теоретических исследованиях, так и в прикладных целях, например, [7, 12–16].

Целью предлагаемой работы является организация криптографической защиты управляющих команд и телеметрической информации от несанкционированного доступа при их передаче между БЛА и НСУ. Задачей работы является разработка метода защиты данных на борту БЛА на основе абсолютно криптостойкого алгоритма шифрования – шифра Вернама (одноразового блокнота).

Обоснование выбора шифра Вернама

С учетом специфики передачи данных между БЛА и НСУ требуются быстрые и не требующие значительной вычислительной мощности и большого объема памяти алгоритмы шифрования. В то же время должны быть обеспечены повышенная криптостойкость, простота реализации и использования.

В целом криптостойкость современных шифров основана на невозможности дешифрования за приемлемое время. В перспективе быстрый рост вычислительных возможностей компьютеров и развитие криптоаналитических методов могут лишить смысла использование классических систем шифрования. Криптостойкость существующих криптоалгоритмов неуклонно снижается по мере роста мощности и возможностей вычислительной техники. Почти все системы шифрования обладают условной криптостойкостью, так как могут быть раскрыты при наличии достаточных ресурсов. Их криптостойкость может оказаться недостаточной, например, в случае возможных в будущем атак с использованием квантовых механизмов.

В связи с этим все больший интерес вызывают совершенные шифры [17]. По Шеннону [10], шифр считается совершенным, если полученные из шифротекста сведения о соответствующем ему открытом тексте не дают никаких сведений об открытом тексте (кроме, возможно, его длины). К таким шифрам при выполнении некоторых условий относятся шифры гаммирования со случайной равновероятной гаммой, и в том числе – шифр Вернама (одноразовый блокнот). Одноразовый блокнот представляет собой набор ключевых последовательностей (страниц), каждая из которых используется только один раз. Шифруемое сообщение должно иметь длину не большую, чем длина страницы одноразового блокнота. Шифрование заключается в наложении на открытый текст секретной гаммы (ключа) с помощью операции XOR.

По типу одноразовый блокнот относится к симметричным поточным синхронным шифрам, имеет простой алгоритм и доказанную теоретически абсолютную криптостойкость. Другим важным свойством шифра Вернама является высокая скорость шифрования. Поскольку генерация шифроблокнота и шифрование разнесены по времени, весь процесс шифрования сводится к выполнению элементарной операции XOR, которая во многих процессорах реализована аппаратно. Потому использование шифра Вернама не приводит к дополнительной нагрузке на процессор. Это особенно важно для использования в системах с ограниченными вычислительными ресурсами, а также при шифровании больших объемов данных (например, видеоинформации).

Таким образом, шифр Вернама (одноразовый блокнот) представляется наиболее подходящим для защиты управляющих команд и телеметрической информации от несанкционированного доступа.

Организация защиты данных на основе шифра Вернама

При организации защиты данных необходимо обеспечить корректное использование одноразового блокнота и экономное использование памяти.

Абсолютная криптостойкость шифра Вернама доказана при следующих требованиях к системе шифрования [10, 11]:

1. ключевая последовательность (страница шифроблокнота) должна быть истинно случайной последовательностью, длина которой не меньше, чем длина открытого текста;
2. ключ должен быть одноразовым;
3. использованную страницу шифроблокнота следует уничтожать после использования.

Рассмотрим реализацию перечисленных требований.

Принципиально сложной и трудоемкой частью реализации алгоритма Вернама является создание одноразового блокнота. В идеале он должен представлять собой истинно случайную последовательность битов. Однако на практике получение истинно случайной последовательности труднодостижимо. Для получения таких последовательностей можно использовать разные подходы, основанные на: криптографических алгоритмах (стойких блочных шифрах, например, генератор из стандарта ANSI X9.17); вычислительно сложных математических задачах (например, алгоритм BBS, Blum – Blum – Shub [18]); специальных реализациях (файл */dev*/*random* в Linux) [11, 19]; физических генераторах шума [11]. Необходимая степень случайности таких последовательностей зависит от решаемых задач.

Получение истинно случайной последовательности битов не является предметом настоящей работы. Для экспериментальных исследований в рамках работы с целью получения одноразового блокнота был выбран способ, аналогичный используемому в распространенном стандарте ANSI X9.17, с заменой блочного шифра Triple DES на шифр ГОСТ 28147-89[1] в режиме гаммирования с обратной связью. Этот шифр базируется на сети Фейстеля. Длина ключа составляет 256 бит. Как показано в [20], результат работы блочного шифра, основанного на сети Фейстеля, дает сильную псевдослучайную последовательность после четырех раундов шифрования. ГОСТ 28147-89 использует 32 раунда шифрования, что обеспечивает получение сильной псевдослучайной последовательности. Набор таких последовательностей образует шифроблокнот.

Особые требования при использовании блочных шифров предъявляются к ключу шифрования. Ключом, отвечающим требованиям шифра Вернама, является массив статистически независимых битов, в котором значения 0 и 1 равновероятны. Такая последовательность битов может быть получена с помощью датчика истинно случайных чисел.

В качестве такого датчика для формирования криптостойкого ключа был использован механизм */dev*/*random* ядра операционной системы Linux, позволяющий получить случайную последовательность битов, источником которых является шум из драйверов устройств.

Шифроблокнот формируется в виде набора страниц (банк страниц). Размер страницы определяется объемом передаваемых данных. Количество страниц зависит от частоты опроса датчиков и длительности полета.

[1] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 01.07.90. М.: Изд-во стандартов, 1996. 28 с.

При организации криптозащиты передаваемых данных нужно решить следующие проблемы: обеспечение одноразовости шифроблокнота, экономия используемой памяти. В настоящей работе предлагается следующий метод.

Для того чтобы применение шифра Вернама было корректным, требуется полностью исключить возможность повторного использования страниц шифроблокнота. В работе предлагается совмещать шифрование/расшифровывание данных с замещением страницы блокнота результатом шифрования/расшифровывания, т.е. производить запись зашифрованных данных поверх уже использованных байтов страницы шифроблокнота (рис. 1). Это гарантирует одноразовость шифроблокнота. Одновременно это решает и вторую проблему, уменьшая объем необходимой памяти, что существенно для имеющего небольшие вычислительные ресурсы бортового компьютера малого БЛА.

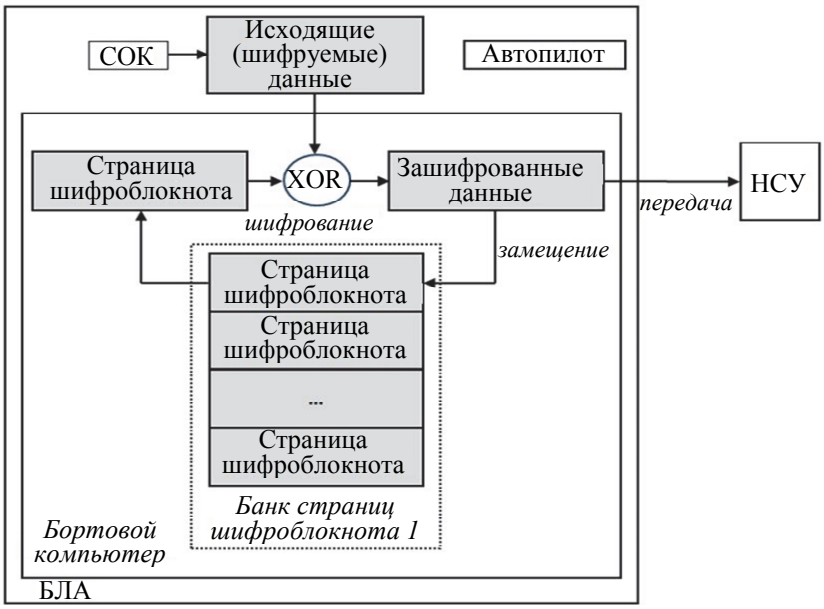

Рис. 1. Шифрование. Вариант с заменой страницы шифроблокнота шифротекстом

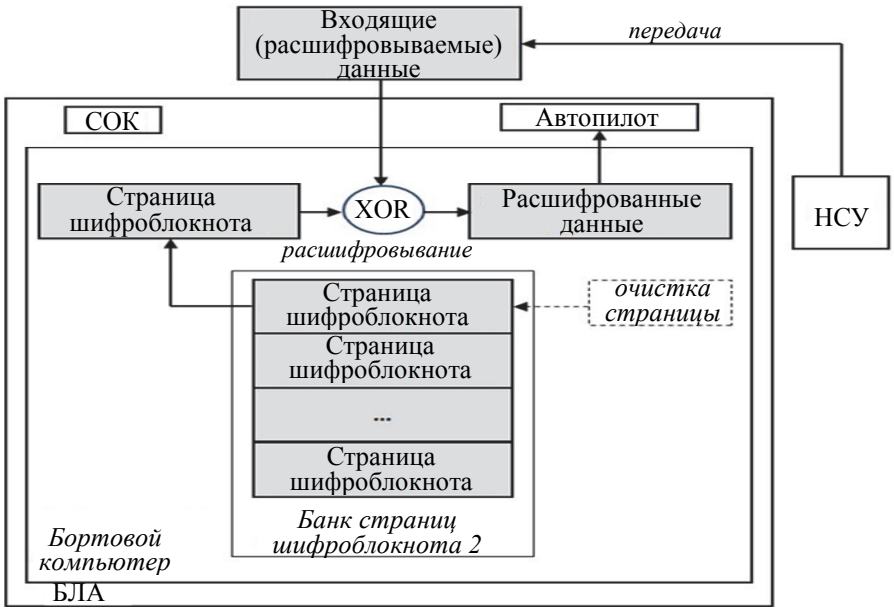

Рис. 2. Расшифровывание. Вариант с очисткой страницы шифроблокнота

Особенностью предлагаемой схемы шифрования является необходимость использования двух разных шифроблокнотов:

1. для работы с исходящими (шифруемыми) данными;
2. для работы с входящими (расшифровываемыми) данными.

К первым относятся данные телеметрии и видеоданные, получаемые со средств объективного контроля (СОК) и передаваемые с БЛА на НСУ. Ко вторым относятся команды управления, передаваемые с НСУ на БЛА.

Таким образом, при шифровании данных происходит замещение байтов, которые участвовали в шифровании, получаемым шифротекстом.

При получении внешних (командных) данных выполняется их расшифровывание с последующей передачей на автопилот. При этом использованная страница шифроблокнота либо очищается, либо при необходимости замещается полученными зашифрованными данными (рис. 2).

Таким образом, в процессе шифрования/расшифровывания шифротекст замещает используемую страницу шифроблокнота, исключая их одновременное существование в памяти бортового компьютера. Это обеспечивает невозможность дешифрования сообщений при перехвате БЛА.

Предложенный метод дополнительно дает возможность превратить использованные страницы шифроблокнота в базу данных шифротекстов. Это позволяет собирать информацию о состоянии аппарата и ходе полета непосредственно на БЛА с последующей детальной ее обработкой после штатной посадки, а также сохранение данных даже в случае отсутствия связи с НСУ.

В результате при использовании каждой страницы шифроблокнота одновременно выполняются:

– шифрование/расшифровывание очередного набора данных;
– уничтожение очередной страницы шифроблокнота путем замещения страницы шифротекстом.

Заключение

В работе рассмотрен метод защиты от несанкционированного доступа данных, передаваемых между беспилотным летательным аппаратом и наземной станцией управления, на основе шифра Вернама (одноразового блокнота), использующий такие преимущества этого шифра, как теоретически доказанная абсолютная криптостойкость, высокая скорость шифрования и простота программной реализации. Он позволяет использовать память, выделенную для шифроблокнота, не только для хранения ключевых последовательностей, но и для накапливания зашифрованных данных. Такое замещение страниц шифроблокнота также решает проблему обеспечения одноразовости шифроблокнота и экономии памяти.

Предложенный метод позволяет повысить уровень защиты данных без привлечения значительной вычислительной мощности и большого объема памяти, что решает задачу, поставленную в работе.

Дальнейшие исследования планируется продолжить в следующих направлениях: повышение качества шифроблокнота (приближение используемой псевдослучайной последовательности к истинно случайной); решение проблем целостности и доступности используемых данных; реализация разработанного метода защиты данных в рамках платформы построения мультироторного беспилотного летательного аппарата, разработанной на кафедре МиПИУ Университета ИТМО и его интеграция в широко используемый для связи с малыми беспилотными летательными аппаратами протокол MAVLink (Micro Air Vehicle Link).

Литература

1. Моисеев В.С. Основы теории эффективного применения беспилотных летательных аппаратов. Казань: Ред.-изд. центр «Школа», 2015. 444 с.
2. Фетисов В.С., Неугодникова Л.М., Адамовский В.В., Красноперов Р.А. Беспилотная авиация: терминология, классификация, современное состояние. Уфа: ФОТОН, 2014. 217 с.
3. Благодырев В.А., Хачумов В.М. Информационная защита вычислительных систем управления космическими аппаратами // Авиакосмическое приборостроение. 2012. № 8. С. 11–25.
4. Mansfield K., Eveleigh T., Holzer T.H., Sarkani S. Unmanned aerial vehicle smart device ground control station cyber security threat model // Proc. 13th IEEE Int. Conf. on Technologies for Homeland Security (HST). Waltham, USA, 2013. P. 722–728. doi: 10.1109/THS.2013.6699093
5. Hartmann K., Steup C. The vulnerability of UAVs to cyber attacks – an approach to the risk assessmen // Proc. 5th Int. Conf. on Cyber Conflict. Tallinn, Estonia, 2013. P. 1–23.
6. Боев Н.М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами // Вестник СибГАУ. 2012. № 2 (42). С. 86–91.
7. Saarelainen T., Jormakka J. Tools for future battlefield warriors // Proc. 5th Int. Conf. on Digital Telecommunications (ICDT). Athens, Greece, 2010. P. 224–233. doi: 10.1109/ICDT.2010.15
8. Мещеряков Р.В., Росошек С.К., Сонькин М.А., Шелупанов А.А. Криптографические протоколы в системах с ограниченными ресурсами // Вычислительные технологии. 2007. Т. 12. № S1. С. 51–61.
9. Авдошин С.М., Савельева А.А. Криптоанализ: современное состояние и перспективы развития // Информационные

References

1. Moiseev V.S. *Osnovy Teorii Effektivnogo Primeneniya Bespilotnykh Letatel'nykh Apparatov* [Bases of Efficient Use Theory of Unmanned Aircraft]. Kazan', Tsenter Shkola Publ., 2015, 444 p.
2. Fetisov V.S., Neugodnikova L.M., Adamovskii V.V., Krasnoperov R.A. *Bespilotnaya Aviatsiya: Terminologiya, Klassifikatsiya, Sovremennoe Sostoyanie* [Unmanned Aircraft: Terminology, Classification, Current Status]. Ufa, Foton Publ., 2014, 217 p.
3. Blagodyrev V.A., Khachumov V.M. Protection of computing systems of space vehicles control. *Aerospace Instrument-Making*, 2012, no. 8, pp. 11–25.
4. Mansfield K., Eveleigh T., Holzer T.H., Sarkani S. Unmanned aerial vehicle smart device ground control station cyber security threat model. *Proc. 13th IEEE Int. Conf. on Technologies for Homeland Security, HST*. Waltham, USA, 2013, pp. 722–728. doi: 10.1109/THS.2013.6699093
5. Hartmann K., Steup C. The vulnerability of UAVs to cyber attacks – an approach to the risk assessmen. *Proc. 5th Int. Conf. on Cyber Conflict*. Tallinn, Estonia, 2013, pp. 1–23.
6. Boev N.M. Analysis of UAV radio control and telemetry systems. *Vestnik of SibGAU*, 2012, no. 2, pp. 86–91.
7. Saarelainen T., Jormakka J. Tools for future battlefield warriors. *Proc. 5th Int. Conf. on Digital Telecommunications, ICDT*. Athens, Greece, 2010, pp. 224–233. doi: 10.1109/ICDT.2010.15
8. Meshcheryakov R.V., Rososhek S.K., Son'kin M.A., Shelupanov A.A. Cryptographic protocol in limited resourse systems. *Computational Technologies*, 2007, vol. 12, no. S1, pp. 51–61. (In Russian)
9. Avdoshin S.M., Savelieva A.A. Cryptanalysis: current state

технологии. 2007. № S3. С. 1–24.
10. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal. 1949. V. 28. N 4. P. 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x
11. Шнайер Б. Прикладная криптография. М.: Триумф, 2002. 806 с.
12. Ryabko B.Ya. The Vernam cipher is robust to small deviations from randomness // Problems of Information Transmission. 2015. V. 51. N 1. P. 82–86. doi: 10.1134/S0032946015010093
13. Matt C., Maurer U. The one-time pad revisited // Proc. IEEE Int. Symposium on Information Theory (ISIT). Istanbul, Turkey, 2013. P. 2706–2710. doi: 10.1109/ISIT.2013.6620718
14. Shukla R., Prakash H.O., Brushan R.P., Venkataraman S., Varadan G. Unconditionally secure and authenticated one time pad cryptosystem // Proc. Int. Conf. on Machine Intelligence and Research Advancement (ICMIRA). Katra, India, 2013. P. 174–178. doi: 10.1109/ICMIRA.2013.40
15. Du R., Sun Z., Wang B., Long D. Quantum secret sharing of secure direct communication using one-time pad // International Journal of Theoretical Physics. 2012. V. 51. N 9. P. 2727–2736. doi: 10.1007/s10773-012-1147-1
16. Guo Y., Xie J., Li J., Lee M.H. An arbitrated quantum signature scheme based on chaotic quantum encryption algorithm // Journal of Modern Physics. 2013. V. 4. P. 83–88. doi: 10.4236/jmp.2013.45B014
17. Зубов А.Ю. Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.
18. Blum L., Blum M., Shub M. A simple unpredictable pseudo-random number generator // SIAM Journal of Computing. 1986. V. 15. N 2. P. 364–383. doi: 10.1137/0215025
19. Gutterman Z., Pinkas B., Reinman T. Analysis of the Linux random number generator // Proc. IEEE Symposium on Security and Privacy. Oakland, USA, 2006. P. 371–385. doi: 10.1109/SP.2006.5
20. Luby M., Rackoff C. How to construct pseudorandom permutations and pseudorandom functions // SIAM Journal of Computing. 1988. V. 17. N 2. P. 373–386. doi: 10.1137/0217022

Авторы

Авдонин Иван Александрович **–** аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, avdoninivan@mail.ru

Будько Марина Борисовна **–** кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, budkomb@mail.ru

Грозов Владимир Андреевич **–** студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, vladimirgrozov@mail.ru

and future trends. *Information Technology,* 2007, no. S3, pp. 1–24.
10. Shannon C.E. Communication theory of secrecy systems. *The Bell System Technical Journal*, 1949, vol. 28, no. 4, pp. 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x
11. Schneier B. *Applied Cryptography*. 2nd ed. Wiley, 1995.
12. Ryabko B.Ya. The Vernam cipher is robust to small deviations from randomness. *Problems of Information Transmission*, 2015, vol. 51, no. 1, pp. 82–86. doi: 10.1134/S0032946015010093
13. Matt C., Maurer U. The one-time pad revisited. *Proc. IEEE Int. Symposium on Information Theory, ISIT*. Istanbul, Turkey, 2013, pp. 2706–2710. doi: 10.1109/ISIT.2013.6620718
14. Shukla R., Prakash H.O., Brushan R.P., Venkataraman S., Varadan G. Unconditionally secure and authenticated one time pad cryptosystem. *Proc. Int. Conf. on Machine Intelligence and Research Advancement, ICMIRA*. Katra, India, 2013, pp. 174–178. doi: 10.1109/ICMIRA.2013.40
15. Du R., Sun Z., Wang B., Long D. Quantum secret sharing of secure direct communication using one-time pad. *International Journal of Theoretical Physics*, 2012, vol. 51, no. 9, pp. 2727–2736. doi: 10.1007/s10773-012-1147-1
16. Guo Y., Xie J., Li J., Lee M.H. An arbitrated quantum signature scheme based on chaotic quantum encryption algorithm. *Journal of Modern Physics*, 2013, vol. 4, pp. 83–88. doi: 10.4236/jmp.2013.45B014
17. Zubov A.Yu. *Sovershennye Shifry* [Perfect Ciphers]. Moscow, Gelios ARV Publ., 2003, 160 p.
18. Blum L., Blum M., Shub M. A simple unpredictable pseudo-random number generator. *SIAM Journal of Computing*, 1986, vol. 15, no. 2, pp. 364–383. doi: 10.1137/0215025
19. Gutterman Z., Pinkas B., Reinman T. Analysis of the Linux random number generator. *Proc. IEEE Symposium on Security and Privacy*. Oakland, USA, 2006, pp. 371–385. doi: 10.1109/SP.2006.5
20. Luby M., Rackoff C. How to construct pseudorandom permutations and pseudorandom functions. *SIAM Journal of Computing*, 1988, vol. 17, no. 2, pp. 373–386. doi: 10.1137/0217022

Authors

Ivan A. Avdonin **–** postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, avdoninivan@mail.ru

Marina B. Budko **–** PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, budkomb@mail.ru

Vladimir A. Grozov **–** student, ITMO University, Saint Petersburg, 197101, Russian Federation, vladimirgrozov@mail.ru