Оригинальные статьи / Original articles

https://doi.org/10.21869/2223-1560-2019-23-3-100-112

Вариант организации многопоточной обработки конфиденциальных данных на базе клеточных автоматов

А. Л. Марухленко [1] ✉, А. В. Плугатарев [1], М. О. Таныгин [1], Л. О. Марухленко [1], Д. О. Бобынцев [1]

[1] ФГБОУ ВО «Юго-Западный государственный университет», ул. 50 лет Октября, 94, г. Курск, 305040, Российская Федерация

✉ e-mail: proxy33@mail.ru

Резюме

Цель исследования *заключается в разработке системы многопоточной обработки на основе алгоритма шифрования с использованием клеточных автоматов и исследовании статистических показателей производительности в зависимости от аппаратной составляющей и величины входного блока, а также разработке рекомендаций для повышения криптоскойкости метода.*

Методы*. Рассмотрена математическая модель метода шифрования с использованием плавающего окна на базе клеточных автоматов [3]. Для исследования быстродействия процесса обработки конфиденциальных данных разработан вариант организации структуры программного модуля с расширенным блоком настроечных параметров, определяющих размерность матрицы, строку активации битовой окрестности обрабатываемых элементов, число параллельных вычислений (тредов) и правило расширения граничных элементов матрицы. Предложен метод формирования графической зависимости времени обработки от исходных параметров, область применения которого возможна как для обработки отдельных файлов, так и непрерывных потоков данных абонентов вычислительной сети.*

Результаты. *Разработан криптографический модуль, реализующий метод шифрования на базе клеточных автоматов, особенностью которого является многопоточный режим работы и динамическое управление блоком исходных параметров. Сформулированы рекомендации по установке окрестности активных элементов матрицы и числу потоков с учетом архитектуры центрального процессора. Проведены экспериментальные исследования, подтверждающие полноту и корректность предложенных решений. Показана целесообразность использования высокоскоростных накопителей на жестком диске и сохранение результатов шифрования в асинхронном сегментированном режиме с привязкой результата к рабочему треду.*

Заключение. *Предложенный вариант организации системы обработки конфиденциальной информации в виде программного модуля с учетом особенностей аппаратного обеспечения позволяет оптимизировать скорость обработки, а соблюдение рекомендаций по расширению окрестности при блочном преобразовании позволяет повысить криптостойкость алгоритма шифрования на базе клеточных автоматов с плавающим окном.*

Ключевые слова: *клеточный автомат; шифрование данных; параллельные вычисления; криптография; системный анализ; информационная безопасность.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Вариант организации многопоточной обработки конфиденциальных данных на базе клеточных автоматов / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, Д. О. Бобынцев // Известия Юго-Западного государственного университета. 2019; 23(3): 100-112. https://doi.org/10.21869/2223-1560-2019-23-3-100-112.

Статья поступила в редакцию 23.04..2019

Статья подписана в печать 30.05.2019

https://doi.org/10.21869/2223-1560-2019-23-3-100-112

A version of Organization of Multithread Processing of Confidential Data on the Basis of Cellular Automata

Anatoliy L. Marukhlenko [1] ✉, Aleksey V. Plugatarev [1], Maksim O. Tanygin [1], Leonid O. Marukhlenko [1], Denis O. Bobyntsev [1]

[1] Southwest State University, 94, 50 Let Oktyabrya str., Kursk, 305040, Russian Federation

✉ e-mail: proxy33@mail.ru

Abstract

Purpose of research *is to develop a multithread processing system based on an encryption algorithm using cellular automata and to study statistical performance indicators depending on the hardware components and the size of the input block, and to develop recommendations for improving the cryptostrength of the method.*

Methods*. A mathematical model of the encryption method using a floating window based on cellular automata was considered [3]. To study the speed of confidential data processing, there was developed a variant of the organization of the structure of the software module with an extended block of setting parameters that determine the dimension of the matrix, the line of activation of the bit neighborhood of the processed elements, the number of parallel computations (threads) and the rule of expansion of the boundary elements of the matrix. A method for the development of the dependence curve of the processing time and inital parameters that can be applied both to process individual files and continuous network subscriber data flow, is proposed.*

Results. *The cryptographic module implementing the encryption method on the basis of cellular automata, which specific feature is a multithread mode of operation and dynamic control of the block of initial parameters, was developed. Recommendations for setting the neighborhood of the active elements of the matrix and the number of threads taking into account the architecture of the CPU were formulated. Experimental studies were conducted to confirm the completeness and correctness of the proposed solutions. The expediency of using high-speed hard disk drives and saving the results of encryption in asynchronous segmented mode with working thread-bind results was revealed.*

Conclusion. *The proposed version of the organization of the confidential data processing system in the form of a software module, taking into account the features of the hardware, allows optimization of the processing speed, and the compliance with the recommendations for the expansion of the neighborhood in the block transformation can improve the cryptographic algorithm based on cellular automata with a floating window.*

Keywords*: cellular automaton; data encryption; parallel computing; cryptography; system analysis; information security.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Marukhlenko A. L., Plugatarev A.V., Tanygin M. O., Bobyntsev D. O. A version of Organization of Multithread Processing of Confidential Data on the Basis of Cellular Automata. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019, 23(3): 100-112 (In Russ.). https://doi.org/ 10.21869/2223-1560-2019-23-3-100-112.

Received 23.04.2019

Accepted 30.05.2019

Введение

Стремительное развитие информационных технологий предполагает непрерывное совершенствование средств, обеспечивающих информационную безопасность конфиденциальных данных [1]. Отдельное внимание уделяется защите информации от несанкционированного доступа с использованием современных криптографических методов и системного анализа в распределенных системах, работающих в масштабе реального времени [2]. Как правило, программно-аппаратные решения по обеспечению комплексной криптозащиты отличаются сложностью интеграции в состав локальной вычислительной сети, а также предполагают сопровождение с привлечением экспертов в области информационной безопасности [3, 4]. Особенный интерес для защиты конфиденциальных данных представляет метод блочной обработки, основанный на алгоритме клеточного шифрования с плавающим окном. Данный метод имеет перспективы повышения криптостойкости при поддержании высокой скорости обработки данных за счет использования параллельных вычислений.

Задача многопоточной обработки конфиденциальных данных

Задачу обеспечения защиты от несанкционированного доступа в рамках рассматриваемого метода можно описать последовательностью основных этапов, а именно: конфиденциальные данные представляются в виде двоичной матрицы, блок шифрования представляет плавающее окно, движение по матрице которого определяется входными параметрами и режимом обработки. Как правило, при обработке (шифровании) он находится в левом верхнем углу исходной матрицы, содержание этого блока выписывается в строку в соответствии с маршрутом обхода окрестности (соседних битов). Эта последовательность заменяется в соответствии с функцией переходов. Полученная шифр-последовательность сворачивается в блок в соответствии с заданным маршрутом и перезаписывается поверх элементов исходной матрицы. Далее происходит смещение и итеративный процесс повторяется до обработки всей матрицы.

Материалы и методы решения задачи

При разработке программного модуля необходимо обеспечить чтение файла с носителя или сетевого интерфейса с учетом аппаратных особенностей автоматизированной системы, произвести формирование и обработку исходной матрицы заданной ширины в соответствии с размером плавающего окна и правилами расширения матрицы для граничных элементов.

Особенностью предлагаемой схемы шифрования потоков данных с использованием параллельных вычислений на базе клеточных автоматов является использование независимых тредов. С их помощью происходит рациональное использование вычислительного ресурса

центрального процессора при обработке на одном компьютере или распределение процесса обработки с использованием сетевых терминалов [5-7].

Вариант построения системы

На рисунке 1 показан принципиальный вариант взаимодействия элементов проектируемой системы.

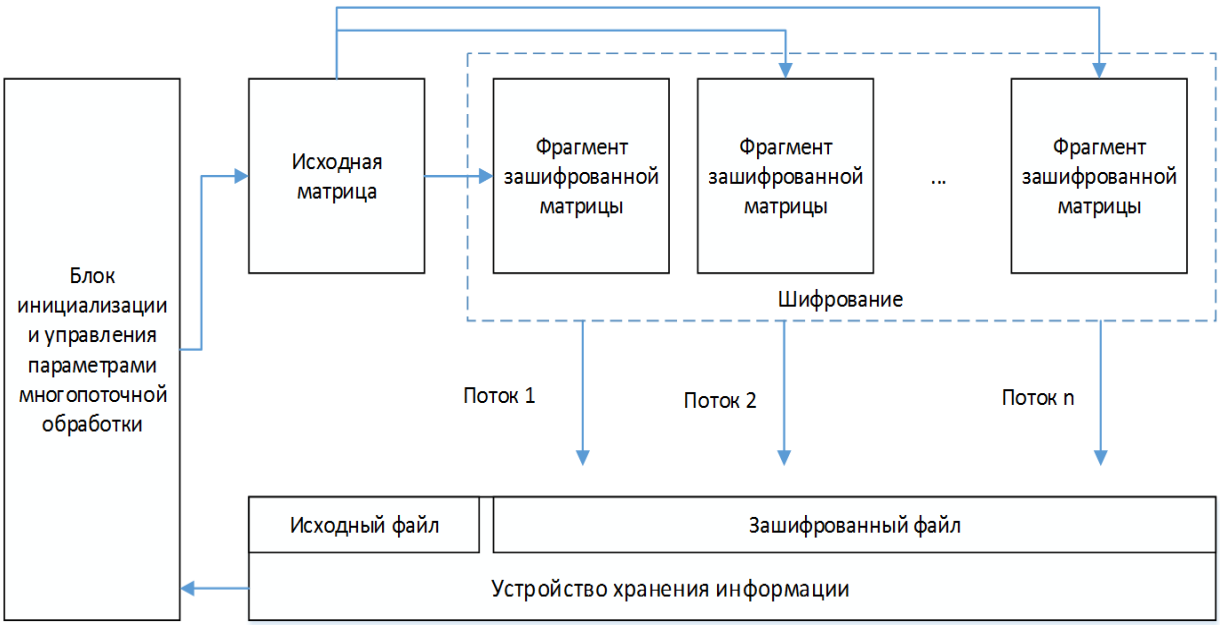

Рис. 1. Схема организации многопоточной обработки

Fig. 1. The scheme of the organization of multi-threaded processing

Зашифрованная матрица формируется поблочно, в процессе движения плавающего окна и в случае использования сегментации может быть представлена набором файлов. Это значит, что готовые блоки зашифрованного файла хранятся в оперативном запоминающем устройстве и ждут окончания процесса шифрования [8]. В зависимости от режима сохранения результирующей матрицы возникает целесообразность использования нескольких накопителей данных, т.к. при одновременной записи несколькими потоками слабым звеном в цепочке производительности становится устройство хранения информации [9].

Математическая модель алгоритма

Для наглядного описания работы метода рассмотрим работу с двумерной матрицей. Размер блока шифрования (m_1,m_2) может задаваться произвольно, а количество столбцов матрицы определяется числом блоков, записанных в алфавите A={0,1}.Число строк матрицы определяется размером исходных данных, а в случае сетевого потока зависит от сеанса взаимодействия абонентов вычислительной сети [10]. Число столбцов

зависит от длины исходной информации и определяется по формуле

$$N_2 = q \cdot m_2 + 1,$$

где q – неполное частное в равенстве $T = k \cdot q + r,\ 0 \le r < k;\ k = m_1 \cdot m_2$ – площадь блока; T – длина исходного текста, а r – остаток от деления.

Клеточным автоматом с плавающим окном называют совокупность:

$CA_o =<$
$Z^n, (N_1, \dots, N_n), A, (m_1, \dots, m_n), \Psi, L >,$

где Z^n – размерность клеточного автомата $(n = 1,2,3)$;

$(N_1, \dots, N_n)$ – размер таблицы;

$(m_1, \dots, m_n)$ – размер блока шифрования;

Ψ – таблица функций переходов;

L – маршрут обхода блока шифрования клеточного автомата с плавающим окном, причем, выполняются равенства $N_1 = m_1, \dots, N_{n-1} = m_{n-1}$, а $N_n = q \cdot m_n + 1$, где q –неполное частное в равенстве $T = k \cdot q + r,\ 0 \le r < k,\ k = m_1 \cdot \dots \cdot m_n$ – число клеток в блоке шифрования; T – длина исходного текста, а r – остаток от деления.

Исходный текст записывается последовательно по слоям в таблицу исходного текста. В последнем слое будет заполнено только r клеток. Оставшиеся клетки заполняются либо нулями, либо единицами. Процесс шифрования состоит в следующем: блок шифрования находится в начале таблицы с исходным текстом, содержание этого блока выписывается в строку в соответствии с маршрутом обхода L. Эта последовательность заменяется в соответствии с функцией переходов Ψ. Полученная шифр - последовательность сворачивается в блок в соответствии с маршрутом L. Исходный блок заменяется на полученный. Блок шифрования сдвигается на одну позицию по таблице данных и процесс повторяется. Процесс шифрования завершается, когда блок шифрования не имеет возможности сдвинуться в новое положение. При дешифровании плавающее окно передвигается в противоположную сторону, начиная с последнего столбца (столбцы в функции переходов меняются местами). В ходе криптоанализа установлено, что для повышения стойкости метода следует производить расширение окрестности матрицы вместе с правилом ее дополнения на базе функции, определяющей состояние дополнительных ячеек для граничных элементов [11]. Также целесообразно применение хеш-функции, определяющей очередность обработки блоков. Указанные функции является ключевыми и должны быть известны получателю конфиденциальных данных [12].

Численное моделирование

Разработанный программный модуль показан на рисунке 2. Здесь в верхней части показан блок исходных параметров – правило дополнения матрицы, опциональное ведение лог-файла, правило обхода и размер блока, размерность матрицы (по числу блоков в строке). Слева в столбце показаны состояния зашифрованных блоков в соответ-

ствии с хэш-функцией. Кроме использования таблицы преобразований на базе хеш-функции предусмотрена возможность загрузки пользовательского справочника переходов или его генерация (при отсутствии). В целях исключения ошибки использования неверного справочника идет сопоставление размера установленного блока и мощности числа переходов [13]. Экспериментальные исследования подтвердили отсутствие зависимости скорости обработки от числа блоков в строке матрицы.

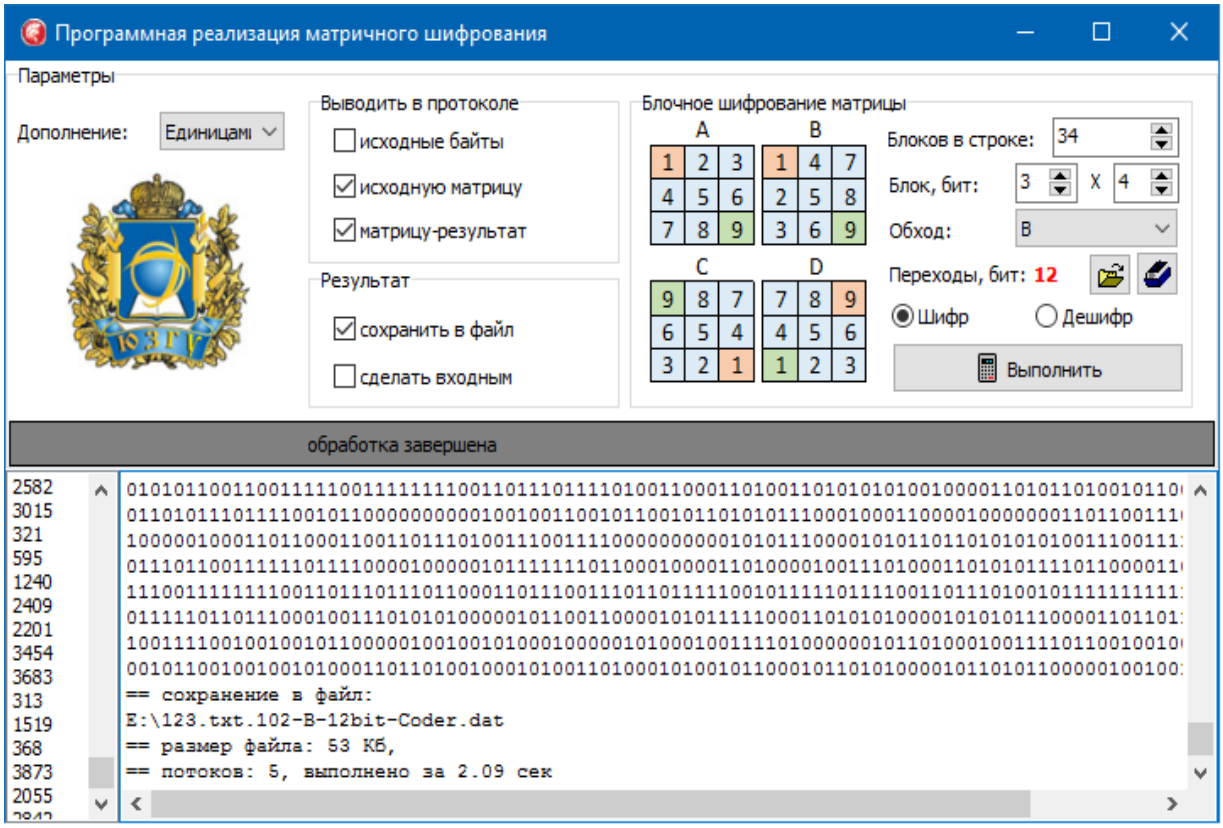

Рис. 2. Интерфейс программного модуля шифрования

Fig. 2. Encryption software interface

Перебор вариантов размеров исходных блоков показал, что скорость обработки матрицы обратно пропорциональна размеру блока. Полученные статистические показатели обработки приведены в таблице, здесь 100% соответствует наиболее продолжительному времени шифрования файла размером 5 Мб, которое составило 23,2 секунды. Исследования производились на персональном компьютере с аппаратной конфигурацией: CPU Intel i3 8100, HDD ST2000DL003, RAM 32 Гб.

Динамика роста быстродействия обоснована тем, что при увеличении размера блоков, их количество в матрице файла уменьшается, соответственно уменьшается и время захвата, подстановки и перезаписи элементов.

Зависимость времени шифрования от размера блока шифрования
The dependence of the encryption time on the size of the encryption block

Размерность блока (бит)	2x2	3x3	4x4	5x7	7x9
Относительная задержка (%)	100	75.97	61.73	41.01	26.46

Важно учитывать тот факт, что при использовании справочника подстановок, выигрыш по времени обработки достигается при наличии готовой таблицы преобразований, в противном случае время ее генерации может превысить время обработки, т.к. временные задержки на ее формирование растут в геометрической прогрессии при увеличении площади блока [14].

Результаты и их обсуждение

Для оценки зависимости производительности работы разработанной системы от числа параллельных вычислений был активирован режим перебора числа тредов на файлах различного размера. При формировании исходной матрицы использовались блоки 20 и 42 бита. Полученные результаты показаны на рисунке 3.

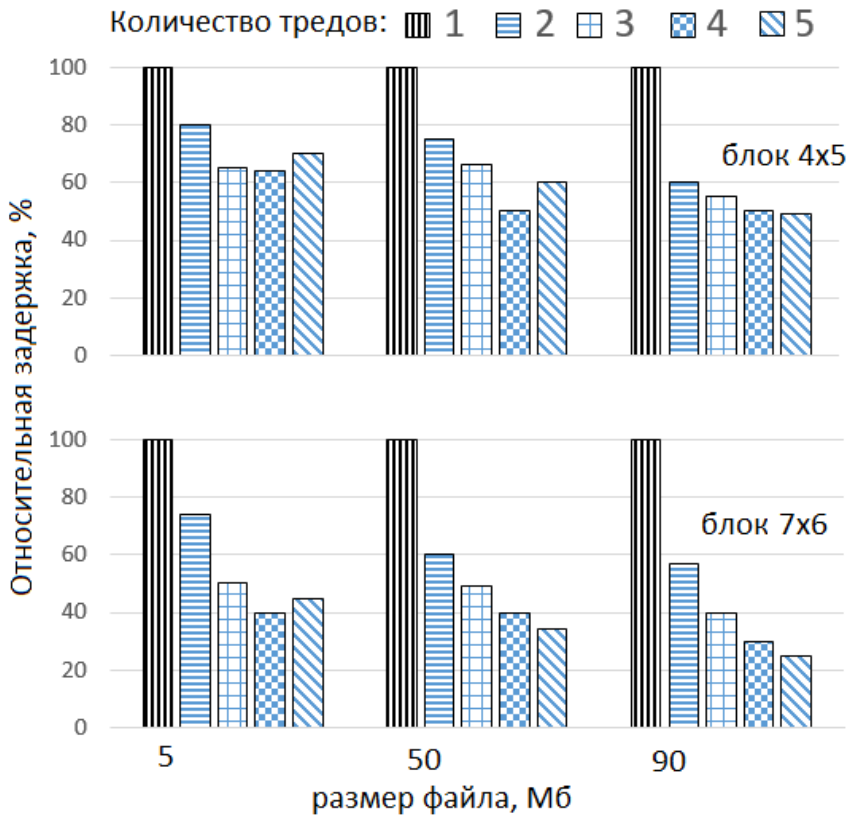

Рис. 3. Результаты исследования в многопоточном режиме
Fig. 3. The research results in multithreaded mode

Для наглядности, здесь по оси ординат указана относительная задержка, 100% соответствует максимальному времени обработки файла указанного размера, таким образом, одинаковая высота столбцов для различных данных не означает совпадение времени обработки.

Из представленных графиков следует, что на базе экспериментального оборудования целесообразно использование не более четырех потоков (процессор имеет четыре физических ядра), так как подавляющее большинство испытаний показало наибольшее быстродействие системы. Использование более пяти потоков не представляет интереса, т.к. показало снижение скорости шифрования в связи с тем, что происходит объединение задач внутри одного физического (логического) процессора и замедление его работы. Таким образом, динамика производительности зависит от архитектуры процессора и загруженности системы в целом. Также из графика следует, что зависимость прироста в скорости многопоточного преобразования зависит от размера файла. Связано это с тем, что этап инициализации и запуска тредов может занимать значительную долю от всего времени обработки, что нецелесообразно при обработке файлов менее 10 Мб. Также следует учитывать размер блока, т.к. он определяет число перезаписи элементов исходной матрицы, а в случае последовательного алгоритма время «простоя» [15]. Анализ загрузки ресурсов компьютера показал, что слабым звеном в цепи быстродействия является накопитель данных, т.к. он активно используется в момент выгрузки результатов шифрования из оперативной памяти. Вариантом решения данной проблемы является асинхронная запись обработанных сегментов исходной матрицы конфиденциальных данных на независимые устройства хранения информации [16].

Выводы

В ходе работы разработана схема организации многопоточной обработки конфиденциальных данных, сформулированы рекомендации по повышению криптостойкости метода шифрования на базе клеточных автоматов с плавающим окном. Для проведения экспериментальных исследований на основе разработанных теоретических положений синтезирован программный модуль, который с учетом особенностей аппаратного обеспечения вычислительной среды обеспечивает поддержание высокой скорости обработки потока данных. Совокупность полученных результатов подтверждают полноту и корректность предложенных решений.

Список литературы

1. Марухленко А.Л., Мирзаханов П.С. Программный комплекс для моделирования процесса передачи и обработки сетевых потоков данных // Известия Юго-Западного

государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-3. С. 175-180.

2. Программно-аппаратный комплекс «Токси+метео» для оценки последствий возможных аварий с учетом данных о текущих погодных условиях / А.А. Агапов, И.О. Хлобыстова, С.Л. Марухленко, А.Л. Марухленко, А.С. Софьин // Безопасность труда в промышленности. 2011. № 1. С. 22-25.

3. Марухленко А.Л., Плугатарев А.В., Марухленко Л.О., Ефремов М.А. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 34-40.

4. Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, The late Shon Harris. Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition. – McGraw-Hill Education, 2018. 640 с.

5. Борзов Д.Б., Чеснокова Е.О., Марухленко А.Л., Аль-Ашвал М.М.Я. Устройство поиска нижней оценки размещения в полносвязных матричных системах при двунаправленной передаче информации // патент на изобретение RUS 2421805 24.11.2008.

6. Программный модуль для оценки криптостойкости симметричных методов шифрования с использованием параллельных вычислений / В.П. Добрица, А.Л. Марухленко, Л.О. Марухленко, А.В. Плугатарев // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции. Курск, 2018. С. 33-38.

7. Анализ потенциальных уязвимостей и современных методов защиты многопользовательских ресурсов / М.О. Таныгин, А.Л. Марухленко, Л.О. Марухленко, Е.Е. Конорева // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции. Курск, 2018. С. 136-140.

8. Технология и программная реализация программного модуля для локализации потенциально опасных объектов на графической подложке с использованием нейронных сетей / М.О. Таныгин, А.Л. Марухленк., Л.О. Марухленко, А.Н. Романов // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции. Курск, 2018. С. 23-28.

9. Администрирование информационных систем / Д.О. Бобынцев, Л.А. Лисицин, А.Л. Марухленко, С.А. Кужелева. Курск, 2019. 201 с.

10. Асютиков А.А., Добрица В.П. Шифрование клеточным автоматом на разбиении по принципу плавающего окна // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции. Курск, 2018. С. 45-50.

11. Безопасность информационных систем / А.Л. Марухленко, М.О. Таныгин, М.А. Ефремов, А.Г. Спеваков; Юго-Зап. гос.ун-т. Курск, 2019. 210 с.

12. Разработка защищенных корпоративных систем на базе клиент-серверной технологии / М.А. Ефремов, Ю.А. Халин, А.Л. Марухленко, Л.О. Марухленко; Юго-Зап. гос.ун-т. Курск, 2018. 176 с.

13. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска / М.А. Ефремов, А.Л. Марухленко, А.В. Плугатарев, Л.О. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 34-40.

14. Вариант обеспечения информационной безопасности за счет повышения отказоустойчивости работы аппаратного межсетевого экрана / Л.О. Марухленко, А.Л. Марухленко, К.М. Керимбаева, А.А. Шамина // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции. Курск, 2018. С. 10-14.

15. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паролей / М.О. Таныгин, Х.Я. Алшаиа, В.А. Алтухова, А.Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 63-71.

16. Организация системы сетевого мониторинга и оценки состояния информационной безопасности объекта / А.Л. Марухленко, К.Д. Селезнёв, М.О. Таныгин, Л.О. Марухленко // Известия Юго-Западного государственного университета. 2019. 23(1): С. 118-129. https://doi.org/10.21869/2223-1560-2019-23-1-118-129.

Reference

1. Marukhlenko A.L., Mirzakhanov P.S. Programmnyi kompleks dlya modelirovaniya protsessa peredachi i obrabotki setevykh potokov dannykh [A software package for modeling the process of transmitting and processing network data streams]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing engineering, Information science. Medical instruments engineering,* 2012, no. 2-3, pp. 175-180 (In Russ.).

2. Agapov A.A., Khlobystova I.O., Marukhlenko S.L., Marukhlenko A.L., Sofin A.S. Programmno-apparatnyi kompleks «Toksi+meteo» dlya otsenki posledstvii vozmozhnykh avarii s uchetom dannykh o tekushchikh pogodnykh usloviyakh [Hardware and software complex “Toxi + meteo” for assessing the consequences of possible accidents taking into account data on current weather conditions]. *Bezopasnost' truda v promyshlennosti =Labor safety in industry*, 2011, no. 1, pp. 22-25 (In Russ.).

3. Marukhlenko A.L., Plugatarev A.V., Marukhlenko L.O., Efremov M.A. Kompleksnaya otsenka informatsionnoi bezopasnosti ob"ekta s primeneniem matematicheskoi modeli dlya rascheta pokazatelei riska [A comprehensive assessment of the information security of an object using a mathematical model for calculating risk indicators]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing engineering, Information science. Medical instruments engineering*, 2018, vol. 8. no. 4 (29), pp. 34-40 (In Russ.).

4. Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, The late Shon Harris. Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition, McGraw-Hill Education, 2018, 640 p.

5. Borzov D.B., Chesnokova E.O., Marukhlenko A.L., Al-Ashval M.M.Ya. Ustroistvo poiska nizhnei otsenki razmeshcheniya v polnosvyaznykh matrichnykh sistemakh pri dvunapravlennoi peredache informatsii. patent na izobretenie [Search device for lower estimation of placement in fully connected matrix systems with bi-directional transmission of information]. Patent for invention RUS 2421805 11.24.2008. (In Russ.).

6. Dobritsa V.P., Marukhlenko A.L., Marukhlenko L.O., Plugatarev A.V. [A software module for assessing the cryptographic strength of symmetric encryption methods using parallel computing]. *Infokommunikatsii i kosmicheskie tekhno-logii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: state, problems and solutions. The collection of scientific articles based on the materials of the II All-Russian scientific and practical conference]. Kursk, 2018, pp. 33-38 (In Russ.).

7. Tanygin M.O., Marukhlenko A.L., Marukhlenko L.O., Konoreva E.E. [Analysis of potential vulnerabilities and modern methods of protecting multi-user resources]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: state, problems and solutions. The collection of scientific articles based on the materials of the II All-Russian scientific and practical conference]. Kursk, 2018, pp. 136-140 (In Russ.).

8. Tanygin M.O., Marukhlenko A.L., Marukhlenko L.O., Romanov A.N. [Technology and software implementation of a software module for localizing potentially dangerous objects on a graphic substrate using neural networks]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: status, problems and solutions. The collection of scientific articles based on the materials of the II All-Russian scientific and practical conference]. Kursk, 2018, pp. 23-28 (In Russ.).

9. Bobyntsev D.O., Lisitsin L.A., Marukhlenko A.L., Kuzheleva S.A. Administrirovanie informatsionnykh sistem. Kursk, 2019. 201 p. (In Russ.).

10. Asyutikov A.A., Dobritsa V.P. [Encryption with a cellular machine on a partition by the principle of a floating window]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: state, problems and solutions. The collection of scientific articles based on the materials of the II All-Russian scientific and practical conference]. Kursk, 2018, pp. 45-50 (In Russ.).

11. Marukhlenko A.L., Tanygin M.O., Efremov M.A., Spevakov A.G. Bezopasnost' informatsionnykh sistem [Security of information systems]. Kursk, 2019, 210 p. (In Russ.).

12. Efremov M.A., Khalin Y.A., Marukhlenko A.L., Marukhlenko L.O. Razrabotka zashchishchennykh korporativnykh sistem na baze klient-servernoi tekhnologii [Development of secure corporate systems based on client-server technology]. Kursk, 2018. 176 p. (In Russ.).

13. Efremov M.A., Marukhlenko A.L., Plugatarev A.V., Marukhlenko L.O. Kompleksnaya otsenka informatsionnoi bezopasnosti ob''ekta s primeneniem matematicheskoi modeli dlya rascheta pokazatelei riska [A comprehensive assessment of the information security of an object using a mathematical model for calculating risk indicators]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing engineering, Information science. Medical instruments engineering.* 2018, vol. 8, no. 4 (29), pp. 34-40 (In Russ.).

14. Marukhlenko L.O., Marukhlenko A.L., Kerimbaeva K.M., Shamina A.A. [Variant of ensuring information security by increasing the fault tolerance of the hardware firewall]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya. Sbornik nauchnykh statei po materialam II Vserossiiskoi nauchno-prakticheskoi konferentsii.* [Infocommunications and space technologies: state, problems and solutions The collection of scientific articles based on the materials of the II All-Russian scientific and practical conference]. Kursk, 2018, pp. 10-14 (In Russ.).

15. Tanygin M.O., Alshaya Kh.Ya., Altukhova V.A., Marukhlenko A.L. Ustanovlenie doveritel'nogo kanala obmena dannymi mezhdu istochnikom i priemnikom informatsii s pomoshch'yu modifitsirovannogo metoda odnorazovykh parolei [Establishing a confidence channel for exchanging data between a source and a receiver of information using the modified one-time password method]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing engineering, Information science. Medical instruments engineering,* 2018, vol. 8, no. 4 (29), pp. 63-71 (In Russ.).

16. Marukhlenko A.L., Seleznev K.D., Tanygin M.O., Marukhlenko L.O. Organizatsiya sistemy setevogo monitoringa i otsenki sostoyaniya informatsionnoi bezopasnosti ob''ekta

[Organization of a network monitoring system and an assessment of the state of information security of an object]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019; 23 (1): 118-129 (In Russ.). https://doi.org/10.21869/2223-1560-2019-23-1-118-129.

Информация об авторах / Information about the Authors

Марухленко Анатолий Леонидович, кандидат технических наук, доцент кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: proxy33@mail.ru

Anatoliy L. Marukhlenko, Candidate of Engineering Sciences, Associate Professor, Information Security Department, Southwest State University, Kursk, Russian Federation e-mail: proxy33@mail.ru

Плугатарев Алексей Владимирович, магистрант кафедры информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: aplugatarev@bk.ru

Aleksey V. Plugatarev, Undergraduate**,** Information Security Department Southwest State University, Kursk, Russian Federation e-mail: aplugatarev@bk.ru

Таныгин Максим Олегович, кандидат технических наук, доцент, завкафедрой информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru

Maksim O. Tanygin, Candidate of Engineering Sciences, Associate Professor, Head of Information Security Department, Southwest State University, Kursk, Russian Federation e-mail: tanygin@yandex.ru

Марухленко Леонид Олегович, старший преподаватель, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: leonid.marukhlenko@mail.ru

Leonid O. Marukhlenko, Senior Lecturer**,** Southwest State University, Kursk, Russian Federation e-mail: leonid.marukhlenko@mail.ru

Бобынцев Денис Олегович, кандидат технических наук, старший преподаватель, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: daniel8728@yandex.ru

Denis O. Bobyntsev, Candidate of Engineering Sciences, Senior Lecturer**,** Southwest State University, Kursk, Russian Federation e-mail: daniel8728@yandex.ru