Санкт-Петербургский государственный университет
аэрокосмического приборостроения

XXV МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

Волновая электроника и инфокоммуникационные системы

ГУАП

Санкт-Петербург, Россия
2022

Санкт-Петербургский государственный университет
аэрокосмического приборостроения

XXV Международная научная конференция

ВОЛНОВАЯ ЭЛЕКТРОНИКА И ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ

Сборник статей

Часть 3

30 мая – 3 июня 2022 г.

Санкт-Петербург

Санкт-Петербург, Россия

2022

УДК 621.38
ББК 32.85
В67

В67 Волновая электроника и инфокоммуникационные системы: XXV Междунар. науч. конф. (СПб., 30 мая – 3 июня 2022 г.): сб. статей: в 3 ч. Ч. 3. СПб.: ГУАП, 2022. 279 с.
ISBN 978-5-8088-1712-8
ISBN 978-5-8088-1715-9 (Ч. 3)
DOI: 10.31799/978-5-8088-1715-9-2022-3

Материалы XXV Международной научной конференции отражают современное состояние волновой электроники и ее применение в информационных и телекоммуникационных системах.

Представляют интерес для широкого круга исследователей, преподавателей, аспирантов и специалистов в области акустооптики, акустоэлектроники.

УДК 621.38
ББК 32.85

ISBN 978-5-8088-1712-8
ISBN 978-5-8088-1715-9 (Ч. 3)
DOI: 10.31799/978-5-8088-1715-9-2022-3

© Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022

ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

УДК 621.391

В. А. Бурлакова*
специалист по УМР
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ВНУТРЕННЕЙ СТУПЕНИ КАСКАДНОЙ СХЕМЫ КОДИРОВАНИЯ ДЛЯ МНОГОУРОВНЕВОЙ ФЛЭШ-ПАМЯТИ

В статье рассмотрена каскадная схема кодирования для многоуровневой флэш-памяти, в которой в качестве внутренней ступени используются коды на основе сравнительно простых решеток, а в качестве внешней ступени используется код Рида – Соломона. Анализ каскадной схемы выполнен применительно к модели, отражающей основные физические особенности ячейки флэш-памяти с неравномерно расположенными целевыми уровнями напряжения в ячейке и дисперсией шума, зависящей от записанного значения (*input-dependent additive Gaussian noise*, ID-AGN [1–2]). Рассмотрена задача построения дискретного отображения канала записи. Указанное отображение выполняется как многоуровневое квантование сигнала на выходе ячейки записи. Конечной целью введения такого квантования является упрощение схемы, реализующей алгоритм декодирования внутреннего кода по максимуму правдоподобия. Вероятность ошибки декодирования внутреннего кода вычисляется путем численного интегрирования выражения, построенного с использованием характеристических функций логарифмов отношения правдоподобия и учитывающего структуру решетки внутреннего кода. Проанализировано влияние числа уровней квантования на вероятность ошибки декодирования внутреннего кода. Приведены численные результаты, показывающие, что снижение характеристик, вызванное квантованием, невелико по сравнению с гипотетической схемой декодирования внутреннего кода, использующей непрерывный выход канала.
Ключевые слова: каскадная схема кодирования, многоуровневая *flash*-память, дискретный канал, квантование.

V. A. Burlakova*
Education and methodology specialist
*St. Petersburg State University of Aerospace Instrumentation

INVESTIGATION OF THE CHARACTERISTICS OF THE INTERNAL STAGE OF THE CASCADE CODING SCHEME FOR MULTI-LEVEL FLASH MEMORY

The article considers a concatenatedcoding scheme for multi-level flash memory, with codes based on relatively simple lattices used in inner stage, and the Reed-Solomon code used in outer stage. The analysis is performed for a model of a flash memory cell with non-uniformly spaced target voltage levels in the cell and noise variance depending on the recorded value (input-dependent additive Gaussian noise, ID-AGN [1–2]). The problem of constructing a discrete mapping of the recording channel is considered. The specified mapping is performed as a multilevel quantization of the signal at the output of the recording cell. The goal of a such quantization is to simplify the scheme implementing the maximum likelihood decoding in inner stage. The error decoding probability of the internal code is calculated by numerical integration of an expression containing the characteristic functions of the logarithms of the likelihood ratio and taking into account the lattice structure of the internal code. The influence of the number of quantization levels

on the probability of an internal code decoding error is analyzed. Numerical results are they shows that the performance degradation caused by quantization is small compared to a decoding scheme using a non-quantized channel output.
Keywords: concatenatedcoding scheme, multilevel flash memory, discrete channel, quantization.

Введение

В ходе экспериментальных исследований [3] установлено, что в многоуровневой памяти доминирует распределение ошибок без пакетирования. Вероятность ошибки, которая может быть достигнута в канале, достаточно высока (порядка $10^{-4}...10^{-3}$ и выше). Требуемый диапазон вероятности ошибки составляет $10^{-12}...10^{-16}$ и может быть достигнут за счет применения помехоустойчивого кодирования.

Использование каскадных конструкций является одним из самых эффективных подходов к организации введения помехоустойчивого кодирования. Каскадная конструкция имеет две ступени: внешний код и внутренний код. Работы [4 – 6] показали, что каскадная конструкция эффективна для повышения надежности хранения данных во *flash*-памяти.

В этих работах анализ каскадных структур проводился применительно к упрощенной модели ячейки *flash*-памяти, т. е. с равномерно расположенными уровнями напряжения целевой ячейки, аддитивным гауссовым шумом и фиксированной дисперсией. Однако более реалистичной моделью является модель аддитивного шума, параметры которой зависят от передаваемого (записанного) значения (ID-AGN) [1].

Описание схемы каскадного кодирования для flash-памяти

Каскадный код имеет две ступени – внешнюю и внутреннею. В качестве внутренней ступени используется последовательность сигналов из четверичного алфавита.

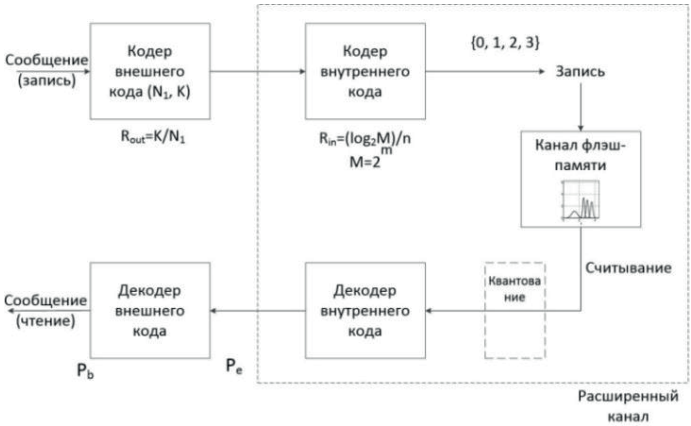


Рис. 1. Схема каскадного кодирования для flash-памяти

Эти последовательности могут быть построены с использованием целочисленных решеток (*lattice*) и кодовых решеток (*trellis*). В качестве внешнего кода использовались коды Рида – Соломона. Далее представлена схема каскадного кодирования для многоуровневой *flash*-памяти (рис. 1), где K – число информационных символов внешнего кода, N_1 –длина внешнего кода (здесь и далее подразумевается расширенный код Рида – Соломона) и равное ей число слов внутреннего кода, n – длина внутреннего кода.

Качество системы кодирования оценивается вероятностью ошибки на бит P_b. Для получения значения P_b требуется оценить вероятность ошибки декодирования слова внешнего кода. Она в свою очередь зависит от вероятности ошибки декодирования слова внутреннего кода.

Модель дискретного канала

Пусть $X = \{x_0, x_1, x_2, x_3\}$ – входной алфавит канала, $Y = \{y_0, y_1, ..., y_{L-1}\}$ – выходной алфавит канала, где L – число уровней квантования непрерывного выходного канала.

Вероятности попадания в какой-либо квант, при условии, что на входе передавалось значение x_k находятся по следующей формуле:

$$p_{y|x}(y_l \mid x_k) = \Pr\left[b_l > z > b_{l+1} \mid x_k\right] = \Pr\left[z > b_{l+1} \mid x_k\right] - \Pr\left[z > b_l \mid x_k\right],$$

где $l = 0,1,...,L-1$, $k = 0,1,2,3$, b_l и b_{l+1} – границы квантов, z – случайная величина, подвергаемая квантованию.

В случае непрерывного выхода канала через $p_{y|x}\left(y \mid x_i\right)$ обозначены функции плотностей вероятности, в случае квантованного выхода канала – переходные вероятности, которые вычисляются по следующей формуле:

$$p_{y|x}(y_l \mid x_k) = Q\left(\frac{b_{l+1} - x_k}{\sigma\left(x_k\right)}\right) - Q\left(\frac{b_l - x_k}{\sigma\left(x_k\right)}\right), \qquad (1)$$

где $l = 0,1,...,L-1$, $k = 0,1,2,3$, а b_l и b_{l+1} – границы квантов, Q – Q-функция, определенная равенством $Q(x) = (2\pi)^{-1/2}\int_x^{\infty} \exp(-u^2/2)du$.

Вероятность ошибки декодирования внутреннего кода при использовании дискретного выхода канала

Вычисление вероятности ошибки декодирования внешнего кода и внутреннего кода при использовании непрерывного выхода канала были рассмотрены в работе [1]. В данной статье приведено вычисление вероятности ошибки декодирования внутреннего кода при использовании дискретного выхода канала.

Для вероятности ошибки декодирования для кода из двух слов может быть записано выражение:

$$P_e(\mathbf{x} \to \mathbf{x}' \mid \mathbf{x}) = \frac{1}{\pi}\int_0^{\infty} \mathrm{Re}\,\frac{\prod_{i=1}^{n} c_z(\alpha - j\beta; x^{(i)}, x'^{(i)})}{\beta + j\alpha} d\alpha. \qquad (2)$$

Характеристическая функция случайной величины $z(y \mid x, x')$ будет вычисляться следующим образом:

$$c_z(\omega; x, x') = \overline{\exp(j\omega z(y \mid x, x'))}, \qquad (3)$$

где черта сверху обозначает усреднение по

$$y,\ z(y \mid x, x') = \ln \frac{p_{y|x}(y \mid x')}{p_{y|x}(y \mid x)}.$$

Вычисление правой части выражения (3) для непрерывных значений y приведено в [1], а для дискретных (квантованных) значений y можно записать, что

$$c_z\left(\omega; x, x'\right) = \overline{e^{j\omega z(y|x,x')}} = \sum_{i=0}^{L-1} p_i e^{j\omega z(y_i|x,x')}, \qquad (4)$$

где $p_i = p_{y|x}(y_i \mid x)$ – условная вероятность получения квантованного значения y_i при условии записи значения x.

Подставив с. в. $z(y \mid x, x')$ в (4), получаем:

$$c_z\left(\omega; x, x'\right) = \overline{e^{j\omega z(y|x,x')}} = \sum_{i=0}^{L-1} p_i e^{j\omega z(y_i|x,x')} = \sum_{i=0}^{L-1} p_{y|x}(y_i \mid x)^{1-j\omega} p_{y|x}\left(y_i \mid x'\right)^{j\omega}.$$

Окончательное выражение для вероятности ошибки декодирования для кода из двух слов для канала с квантованным выходом получается при подстановке этого выражения в (2).

Полученные результаты

На рис. 2 показаны графики вероятности ошибки декодирования, полученные для непрерывного выхода канала и дискретного выхода канала для решеток D_5 и E_7 при условии, что было четыре входа, а количество выходов равно L = 8, 16 и 32.

На основании графиков, приведенных на рис. 2, построим таблицу, в которой покажем, как меняется количество циклов перезаписи N при использовании канала с дискретным выходом по сравнению со случаем канала с непрерывным выходом. Расчеты выполнены для решетки – E_7, количество выходов L = 8, 16 и 32, время хранения T = 1, 12 и 120 мес. Сравнения проведены для значений вероятности ошибки декодирования внутреннего кода $P_e = 10^{-3}$ и 10^{-4}, которые обеспечивают приемлемую надежность хранения, реализуемую с использованием каскадной схемы кодирования.

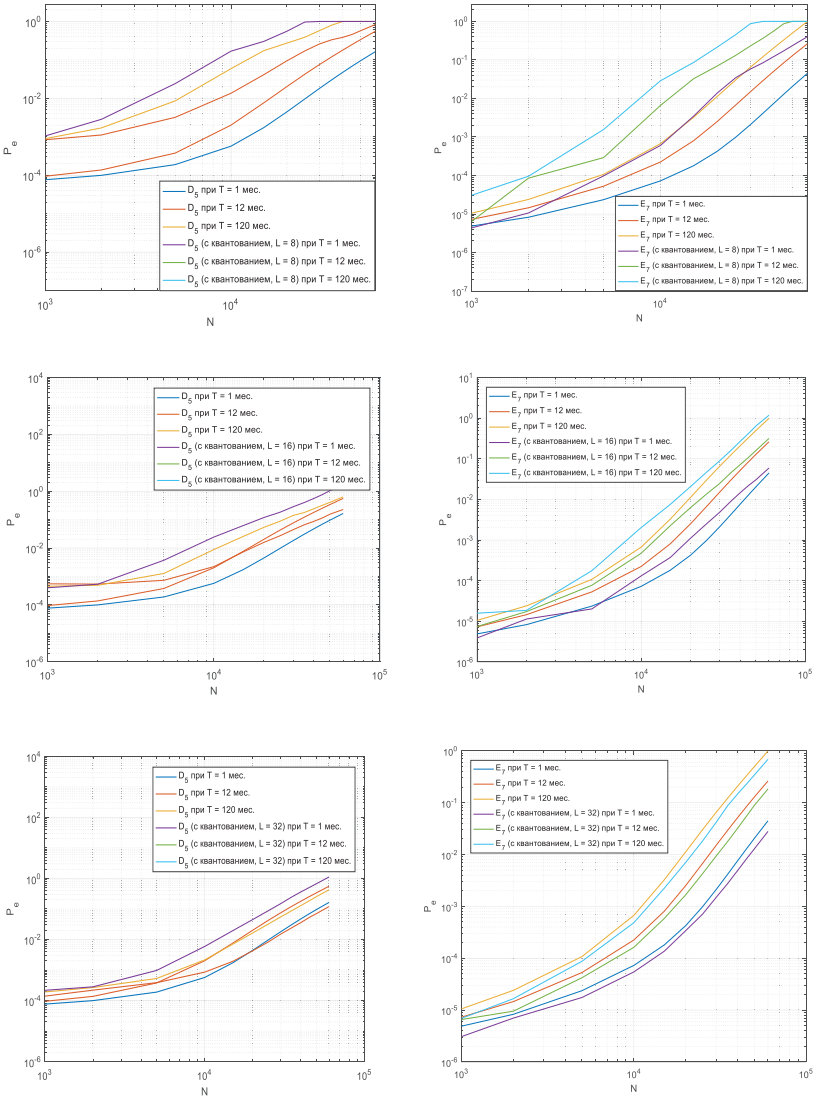


Рис. 2. Сравнение вероятности ошибки декодирования для непрерывного выхода канала и квантованного выхода канала для решеток D_5 и E_7, количество выходов L = 8, 16 и 32

Таблица 1

Степень ухудшения качества канала записи, возникающего из-за квантования сигнала на выходе ячейки памяти (относительное уменьшение числа циклов перезаписи) при $P_e = 10^{-3}, P_e = 10^{-4}$

L(число уровней квантования) / T(время хранения), P_e	8	16	32
1 мес., $P_e = 10^{-3}$	56%	22%	7,7%
12 мес., $P_e = 10^{-3}$	56,7%	20%	5,6%
120 мес., $P_e = 10^{-3}$	62,7%	27,3%	7,7%
1 мес., $P_e = 10^{-4}$	54,6%	18,2%	7,1%
12 мес., $P_e = 10^{-4}$	68,1%	21,4%	12,5%
120 мес., $P_e = 10^{-4}$	59,2%	16,7%	4%

Как следует из данных, приведенных в табл. 1, уменьшение числа циклов перезаписи при числе уровней квантования $L = 16$ невелико, а при $L = 32$ – незначительно. Это значит, что квантование с числом уровней $L = 16$ и 32 может быть использовано на практике. Квантование с числом уровней $L = 8$ приводит к существенному ухудшению характеристик и поэтому представляется неприемлемым.

Заключение

В данной работе была рассмотрена каскадная схема кодирования для многоуровневой *flash*-памяти с дискретным выходом канала, используемым при декодировании слов внутреннего кода по МП. Были представлены вычисления вероятности ошибки декодирования P_e символа внутреннего кода для двух видов решетки – D_5 и E_7. Вычисление вероятности ошибки декодирования внутреннего кода выполнено с использованием подхода, основанного на использовании характеристической функции (х. ф.) логарифма отношения правдоподобия квантованного выхода канала записи. Сформулированы выводы о допустимом числе уровней квантования, обеспечивающем приемлемое ухудшение качества канала записи.

Библиографический список

1. Трофимов А. Н., Таубин Ф. А. Каскадное кодирование на основе многомерных решеток и кодов Рида – Соломона для многоуровневой флэш-памяти // Труды СПИИРАН. 2018. Т. 57. № 2. С. 75–103.

2. Kurkoski B. M. Coded modulation using lattices and Reed-Solomon codes, with applications to flash memories. IEEE Trans. on Selected Areas in Communications. 2014. Vol. 32. No. 5. Pp. 900–908.

3. Yaakobi E. [et al.] Error correcting coding for flash memories. Flash Memory Summit. 2009. Vol. 3. Pp. 4–10.

4. Lou H.-L., Sundberg C.-E. Coded modulation to increase storage capacity of multilevel memories // Proceedings of the IEEE Globecom (Globecom'1998). 1998. Pp. 3379–3384.

5. Sun F. [et al.] Multilevel flash memory on-chip error correction based on trellis coded modulation // Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2006). 2006. Pp. 1443–1446.

6. Li S. and Zhang T. Improving multi-level NAND flash memory storage reliability using concatenated BCH-TCM coding. IEEE Trans. on VLSI Systems. 2010. Vol. 18. No. 10. Pp. 1412–1420.

УДК 004.932.2; 621.396.9635.33

В. Ю. Волков*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения
**Санкт-Петербургский государственный электротехнический университет (ЛЭТИ)

ОБНАРУЖЕНИЕ И СЕЛЕКЦИЯ КОМПАКТНЫХ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ

Рассмотрена задача обнаружения компактных объектов и различения их по форме на монохромных цифровых изображениях, присущих системам дистанционного зондирования. Использован адаптивный многопороговый подход, который основан на анализе набора бинарных срезов. На каждом срезе производится селекция объектов по площади и по коэффициенту компактности. Исследуется проблема обнаружения компактного объекта в виде диска на фоне шума. Эффективность алгоритма проверяется на реальных изображениях, содержащих компактные объекты.
Ключевые слова: адаптивная многопороговая сегментация; различение и селекция объектов; перколяция.

V. Yu. Volkov*
Dr. Sc., Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation;
**St. Petersburg State Electrotechnical University (LETI)

DETECTION AND SELECTION OF COMPACT OBJECTS IN IMAGES

The problem of detecting compact objects and distinguishing them by shape on monochrome digital images inherent in remote sensing systems is considered. An adaptive multi-threshold approach is used, which is based on the analysis of a set of binary slices. On each slice, objects are selected by area and by the compactness coefficient. The problem of detecting a compact object in the form of a disk against a background of noise is investigated. The effectiveness of the algorithm is tested on real images containing compact objects.
Keywords: adaptive multi-threshold segmentation; object discrimination and selection; percolation.

Введение

В статье исследуется обнаружение и селекция компактных объектов на монохромных цифровых изображениях с использованием адаптивного многопорогового алгоритма. Работа алгоритма основана на изменении площадей объектов с увеличением порога и на эффекте перколяции (просачивания), который вызывает расщепление единого объекта на отдельные фрагменты. Для выделения объектов на каждом морфологическом слое используются характеристики изменения площади и компактности этого объекта на соседних слоях [1].

Рассмотрена задача обнаружения компактного объекта в виде диска на фоне шума, различные решающие статистики, и рассчитаны характеристики

обнаружения. Кроме того, эффективность алгоритма проверяется на реальном изображении, содержащем компактные объекты, представляющие интерес.

Многопороговый алгоритм обнаружения с селекцией объектов

Обнаружение и селекция компактных объектов с учетом ограничений по площади и коэффициенту компактности рассмотрены в [1]. Исследуемый алгоритм многопороговой селекции использует в качестве полезной характеристики коэффициент удлинения периметра объекта $P_S = P^2/4\pi S$, где P – периметр объекта, S – его площадь [2]. Эта характеристика является геометрическим инвариантом и имеет минимальное теоретическое значение, равное единице для объекта в форме диска. Однако этот коэффициент, измеренный на зашумленных изображениях, может значительно увеличиться даже для компактного объекта из-за появления фрактальных шумовых структур на его границах, которые резко увеличивают периметр объекта. Это существенно влияет на качество селекции, особенно при малых отношениях сигнал/шум.

Многопороговый алгоритм, исследованный в [1], строит трехмерную иерархическую структуру объектов на основе набора двоичных срезов интенсивности, полученных с увеличением пороговых значений. В этой структуре интересующий объект может располагаться на нескольких бинарных слоях, в зависимости от его интенсивности и текстуры. Это состояние объекта определяется скоростью уменьшения его площади с увеличением порога. Для характеристики данного свойства вводится коэффициент K_S, равный отношению последующего значения площади объекта к полученному на предыдущем срезе. Одним из параметров алгоритма является граничное значение коэффициента устойчивости площади объекта K_P, так что $K_S \geq K_P$. Если при увеличении порога T на ΔT его площадь $S_{T+\Delta T} < K_P\, S_T$, то считается, что данный объект «погиб», а на его месте из фрагментов образуются новые объекты. Еще два параметра алгоритма связаны с селекцией и удалением объектов, имеющих площади, меньшие $S_{\min}$ и по коэффициенту компактности P_S, который ограничивается сверху значением $P_{S\max}$. Другие алгоритмы многопороговой обработки рассмотрены в работах [3, 4].

Для исследования влияния формы объекта на характеристики обнаружения рассмотрим объект в форме диска, который появляется в гауссовом шуме. В пикселях, занятых объектом, наблюдается (положительный) сдвиг в математическом ожидании распределения. Отношение сигнал/шум d определяется как сдвиг, отнесенный к среднеквадратичному значению шума.

Рис. 1 показывает входные и выходные изображения для оптимального обнаружения сдвига в каждом пикселе в соответствии с критерием Неймана – Пирсона с вероятностью ложной тревоги $F = 0{,}01$ и с отношением сигнал/шум $d = 2{,}326$. На рис. 2 показаны результаты обнаружения известными алгоритмами Отсу и Брэдли – Рота. Есть две причины, по которым нежелательно использовать накопление пикселей по площади объекта для увеличения отношения сигнал/шум. Во-первых, размер объекта часто неизвестен, а во-вторых, накопление разрушает границы объекта, которые очень информативны. В случае порога

Отсу невозможно контролировать уровень ложных срабатываний. При малом отношении сигнал/шум возникают проблемы с выделением формы объекта. Для локального адаптивного среднего порога (алгоритм Брэдли – Рота) проблема подавления фона и выделения формы объекта остается.

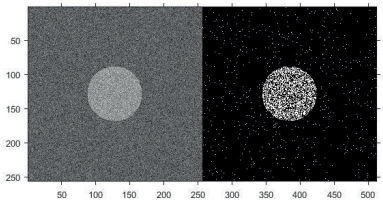


Рис. 1. Входное (слева) и выходное (справа) изображения с пороговой бинаризацией по критерию Неймана – Пирсона

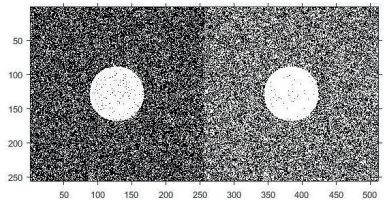


Рис. 2. Результаты бинаризации по Отсу (слева) и для адаптивного порога Брэдли – Рота (справа)

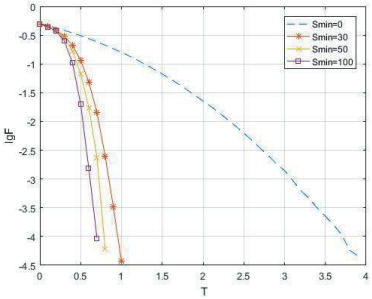


Рис. 3. Уменьшение вероятности ложной тревоги при удалении мелких объектов с $S<S_{min}$ после селекции по площади

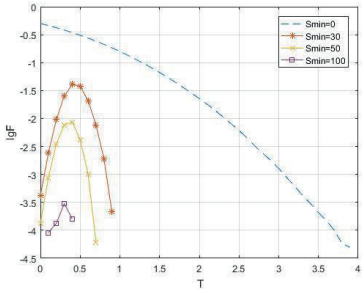


Рис. 4. Уменьшение вероятности ложной тревоги при удалении объектов с $P_S>P_{Smax}$ после селекции по компактности

Селекция объектов является эффективным средством повышения эффективности алгоритмов. Рис. 3 показывает зависимости вероятности ложной тревоги от порогового уровня в случае удаления объектов с площадью, меньшей, чем $S_{\min}$, из выходного двоичного изображения. В этом случае можно увеличить вероятность правильного обнаружения объекта за счет снижения порогового уровня. Рис. 4 иллюстрирует эффект уменьшения вероятности ложной тревоги при совместной селекции объектов по площади и компактности при $P_{S\max} = 10$. Таким образом, селекция позволяет значительно очистить выходное изображение от остатков фона. Решающими статистиками, позволяющими обнаружить и выделить компактные объекты могут быть минимальные коэффициенты P_S, со-

ответствующие им оптимальные пороги T_{opt}, а также значения площадей выделенных объектов.

Алгоритм формирует набор объектов, которые индексируются по их пороговым значениям. Объект интереса можно выделить по максимальному пороговому значению. Рис. 5 содержит выходное изображение для всех выбранных объектов (слева) и извлеченный диск с использованием максимального порогового значения (справа).

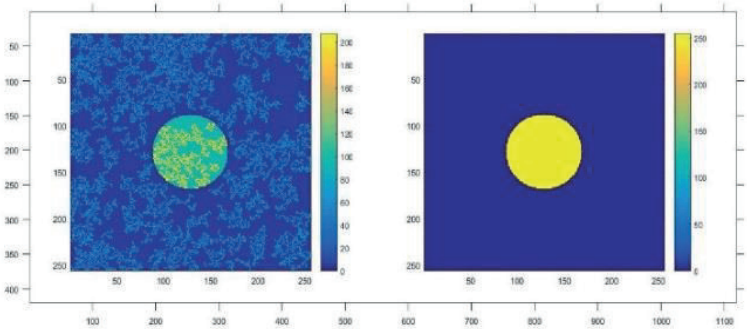


Рис. 5. Все отселектированные объекты с d = 10 (слева) и в диск, выделенный с использованием максимального порогового значения (справа)

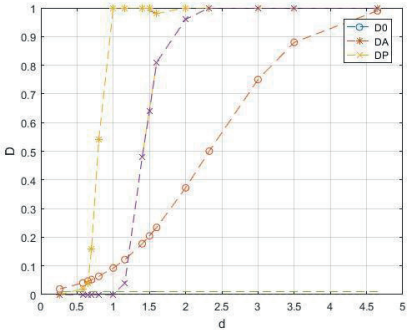


Рис. 6. Характеристики обнаружения диска в шуме при K_P = 0,5; S_{min} = 50; P_{Smax} = 20 (DA – для селекции объекта по максимальной площади; DP – для селекции по минимуму P_S; D0 – характеристика обнаружителя Неймана – Пирсона)

Характеристики обнаружения получены путем моделирования с числом итераций M = 100 и представлены на рис. 6. Параметры селекции K_P, $S_{\min}$ и $P_{S\max}$ были выбраны таким образом, чтобы вероятность ложной тревоги была меньше F = 0,01 (см. рис. 4). Пунктирная линия $D0$ соответствует детектору Неймана – Пирсона для той же вероятности ложной тревоги, Вероятность правильного обнаружения вычисляется по формуле $D0 = \Phi(d - t_{NP})$, где t_{NP} = 2.326 – порого-

вое значение для $F = 0{,}01$, с использованием интеграла вероятности Ф в форме Лапласа.

Как следует из анализа, алгоритм многопороговой селекции обеспечивает выигрыш в качестве обнаружения компактных объектов по сравнению с известными процедурами. Алгоритм имеет три параметра для управления процессом, которые легко понять физически. Он нечувствителен к изменениям масштаба изображения, если не учитывать селекцию по площади. Форма интересующего объекта также сохраняется, что важно в задачах различения компактных объектов по форме.

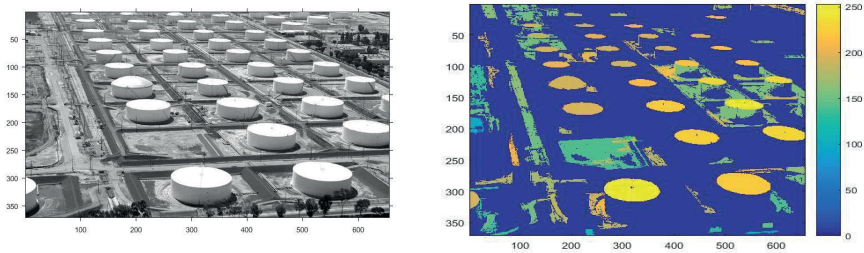


Рис. 7. Реальное изображение с компактными объектами (слева) и результаты их обнаружения и селекции (справа)

Пример многопороговой обработки реального изображения на рис. 7 иллюстрирует эффективность использования коэффициента компактности P_S для обнаружения компактных объектов по форме. Каждый изолированный объект выделяется отдельно и может быть локализован и измерен.

Заключение

Рассмотрена проблема обнаружения и выделения компактных объектов на монохромных изображениях, получаемых системами дистанционного наблюдения. Исследован адаптивный многопороговый алгоритм с селекцией объектов по площади и по коэффициенту удлинения периметра. Получены характеристики обнаружения диска в гауссовском шуме. Установлено, что для компактных объектов получаются более высокие пороги обнаружения, чем для фоновых объектов, что позволяет использовать эти статистики для обнаружения. Эффективность алгоритма проверена на реальном изображении, содержащем компактные объекты.

Библиографический список

1. Volkov V. Yu. Detection and extraction of objects in digital images / V. Yu. Volkov. M. I. Bogachev. 2020 9th Mediterranean Conf. on Embedded Computing, MECO 2020, 9134228.

2. Gonzales R. C. Digital Image Processing / R. C. Gonzales. R. E. Woods. 4ed. Pearson, 2018.

3. Cheng G. A survey on object detection in optical remote sensing images / G. Cheng. J. Han. ISPRS Journal of Photogrammetry and Remote Sensing. V. 117. P. 11–28, 2016.

4. Shivahare B. D. Multilevel thresholding based image segmentation using whale optimization algorithm / B. D. Shivahare, S. K. Gupta. Int. J. of Innovative Technology and Exploring Engineering (IJITEE). V. 8. Issue-12. October 2019.

УДК 004.056

В. Г. Ерышов*
кандидат технических наук, доцент
Д. В. Ильина*
старший преподаватель
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МАРКОВСКАЯ МОДЕЛЬ ПРОЦЕССА КОМПЬЮТЕРНОЙ РАЗВЕДКИ, ОСУЩЕСТВЛЯЮЩЕЙ НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП И ПОЛУЧЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ИЗ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНИЗАЦИЙ

В статье рассматривается математическая модель процесса компьютерной разведки, осуществляющей несанкционированный доступ и получение конфиденциальной информации из информационных систем организаций, разработанная на основе теории Марковских случайных процессов.
Ключевые слова: математическая модель, компьютерная разведка, несанкционированный доступ, защита информации, конфиденциальная информация, информационная система, Марковский случайный процесс.

V. G. Eryshov*
PhD, Tech., Associate Professor
D. V. Ilina*
Senior Lecturer
*St. Petersburg State University of Aerospace Instrumentation

MARKOV MODEL OF THE COMPUTER INTELLIGENCE PROCESS THAT PROVIDES UNAUTHORIZED ACCESS AND OBTAINING CONFIDENTIAL INFORMATION FROM INFORMATION SYSTEMS OF ORGANIZATIONS

The article discusses a mathematical model of the computer intelligence process that provides unauthorized access and obtaining confidential information from the information systems of organizations, developed on the basis of the theory of Markov random processes.
Keywords: mathematical model, computer intelligence, unauthorized access, information protection, confidential information, information system, Markov random process.

Введение

В представленной статье рассмотрена задача моделирования процесса компьютерной разведки (КР), определены вероятностно-временные зависимости данного процесса, которые позволяют исследовать его возможности.

На современном этапе развития и применения новейших информационных технологий, сетей связи и информационных систем (ИС), разработки нового программного обеспечения (ПО), а также постоянного ведения компьютерной разведки (КР), в организациях все более обостряется задача обеспечения

защиты информации (ЗИ) и ИС от кибернарушителей, а также органов КР специальных служб иностранных государств.

Объектами КР являются: защищаемая конфиденциальная информация (КИ), телекоммуникационное оборудование, ИС – как основные источники КИ, обрабатываемой и циркулирующей в них.

Компьютерная разведка (киберразведка) – это осуществление несанкционированного доступа (НСД) к КИ, ИС и дальнейшего несанкционированного воздействия (НСВ) на них: кража, модификация, удаленное управление, уничтожение КИ или ИС. Для этого применяется специальное вредоносное ПО [1].

В связи с этим для служб информационной безопасности (СИБ) организаций все более актуальной становится задача обеспечения защиты КИ и ИС организаций от НСД и НСВ.

С целью выполнения требований по ЗИ ИС организаций, а также для построения адекватной существующим угрозам ИБ комплексной системы ЗИ (СЗИ) организации одной из важнейших задач является задача исследования процесса получения КР КИ из ИС организации. Для этого необходимо провести теоретические исследования по оценке возможностей КР. Наиболее эффективным методом при таких исследованиях выступает моделирование, заключающееся в построении математической модели и изучении исследуемых объектов и их процессов.

В связи с этим возникает необходимость разработки математической модели процесса КР для выявления вероятностно-временных зависимостей его событий и состояний.

Под математической моделью в статье будем понимать математическое описание процесса КР и вероятностно-временных зависимостей его подпроцессов. Для разработки такой модели могут быть использован математический аппарат теории Марковских случайных процессов [2].

Марковский процесс – это такой случайный процесс, происходящий в исследуемой системе, если для любого момента времени его вероятностные характеристики процесса в будущем зависят только от его состояния в данный момент и не зависят от того, когда и как система пришла в это состояние [2].

Процесс КР можно представить ориентированным графом состояний и описать в терминах теории Марковских случайных процессов с дискретными состояниями и непрерывным временем (рис. 1).

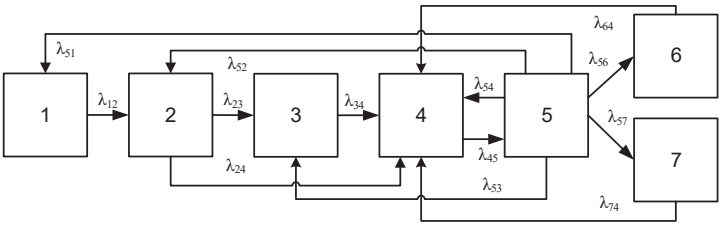


Рис. 1. Ориентированный граф состояний процесса КР

Под Марковским случайным процессом будем понимать процесс, у которого в любой момент времени t множество его состояний S – счетно и конечно, а переходы из одного состояния в другое происходят в любой момент времени t исследуемого периода.

В разрабатываемой математической модели при описании исследуемого процесса КР предполагается, что все его переходы из состояния в состояние происходят под воздействием пуассоновских потоков событий.

Исходными данными для построения таких моделей являются потоки событий, полученные на основе экспертных оценок в области кибербезопасности, различных международных экспертных организаций и т. д. Для получения вероятностных и временных характеристик процесса КР, для построенного ориентированного графа состояний (рис. 2) в модели была составлена и решена система обыкновенных дифференциальных уравнений Колмогорова [3].

Переходы из состояния в состояние в исследуемом процессе происходят под воздействием кусочно-стационарных пуассоновских потоков событий [2]. Описание данных состояний представлены в табл. 1.

Таблица 1

Описание состояний процесса КР ИС организаций

№ п/п	Наименование состояния	№ вх. сост.	№ вых. сост.
S_1	Осуществление НСД КР к защищаемым ресурсам ИС организации	λ_{61}	λ_{12}
S_2	Осуществление перехвата КР КИ из ИС организации	λ_{12}	λ_{23}
S_3	Осуществление сбора КР КИ, циркулирующей в ИС организации	λ_{23}, λ_{43}	λ_{34}
S_4	Осуществление анализа полученной КР КИ из ИС организации	λ_{34}, λ_{54}, λ_{64}	λ_{41}, λ_{43}, λ_{45}, λ_{46}
S_5	Выбор органами управления КР типа воздействия на ИС (КИ) организации	λ_{45}	λ_{54}
S_6	Использование КР специального ПО для осуществления НСВ на ИС, ее элементы и циркулирующей в ней КИ	λ_{46}	λ_{64}
S_7	Осуществление КР скрытого информационного воздействия на ИС, ее элементы и циркулирующей в ней КИ	λ_{57}	λ_{74}

Таблица состояний исследуемого процесса осуществления КР, описывает его основные укрупненные этапы. Каждая операция в математической модели характеризует материальное действие, требующее использования ресурсов системы КР, или логическое, требующее лишь взаимосвязи событий.

Для построенного ориентированного графа исследуемого процесса (рис. 1) была составлена система обыкновенных дифференциальных уравнений Колмогорова [3].

Для решения системы дифференциальных уравнений было использовано математическое ПО для инженерных расчетов *Mathcad,* которое позволило получить расчетные значения вероятностей нахождения событий исследуемого процесса в зависимости от модельного времени (времени функционирования системы) – вероятностно-временные зависимости.

Результатами моделирования исследуемого процесса КР явились его вероятностно-временные зависимости, представленные на рис. 2.

$$\frac{dp_1(t)}{dt} = p_5(t)\lambda_{51}(t) - p_1(t)\lambda_{12}(t),$$

$$\frac{dp_2(t)}{dt} = p_1(t)\lambda_{12}(t) + p_5(t)\lambda_{52}(t) - p_2(t)\{\lambda_{23}(t) + \lambda_{24}(t)\},$$

$$\frac{dp_3(t)}{dt} = p_2(t)\lambda_{23}(t) + p_5(t)\lambda_{53}(t) - p_3(t)\lambda_{34}(t),$$

$$\frac{dp_4(t)}{dt} = p_2(t)\lambda_{24}(t) + p_3(t)\lambda_{34}(t) + p_5(t)\lambda_{54}(t) + p_6(t)\lambda_{64}(t) +$$

$$+ p_7(t)\lambda_{74}(t) - p_4(t)\lambda_{45}(t),$$

$$\frac{dp_5(t)}{dt} = p_4(t)\lambda_{45}(t) - p_5(t)\{\lambda_{51}(t) + \lambda_{52}(t) + \lambda_{53}(t) + \lambda_{54}(t) + \lambda_{56}(t) + \lambda_{57}(t)\},$$

$$\frac{dp_6(t)}{dt} = p_5(t)\lambda_{56}(t) - p_6(t)\lambda_{64}(t),$$

$$\frac{dp_7(t)}{dt} = p_5(t)\lambda_{57}(t) - p_7(t)\lambda_{74}(t).$$

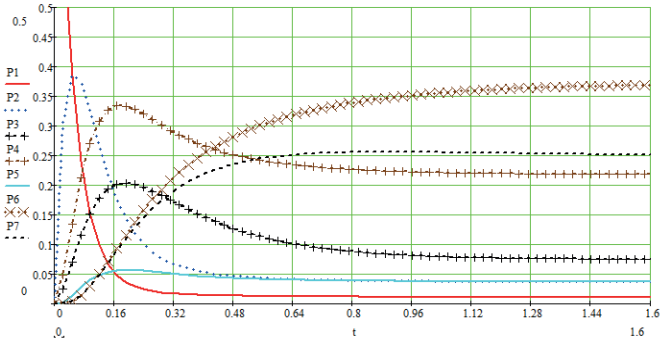


Рис. 2. Вероятностно-временные зависимости процесса КР

Анализ полученных результатов показал, что в представленном примере наибольшей финальной вероятностью события процесса КР является вероятность: $P_6 = 0{,}37$. Это значит, что процесс КР находится в наиболее вероятном событии: «Использование КР специального ПО для осуществления НСВ на ИС.

В качестве заключения можно отметить, что разработанная математическая модель КР позволяет получать и анализировать вероятностные и временные зависимости и характеристики процесса КР, исследовать его возможности по осуществлению НСД и НСВ к ресурсам и самим ИС.

Библиографический список

1. Меньшаков Ю. К. Теоретические основы технических разведок. М.: ИПЦ «Маска», 2017. 640 с.

2. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения. М.: Наука, Гл. ред. Физ.-мат. Лит., 1991. 384 с.

3. Ерышов В. Г. Модель процесса добывания конфиденциальной информации компьютерной разведкой из информационных систем организаций // Сборник избранных статей по материалам научных конференций «Международная научная конференция "Безопасность: Информация, Техника, Управление». СПб.: ГНИИ «Нацразвитие», декабрь 2021. С. 64. С. 26–29.

УДК 621.391

М. Н. Исаева*
ассистент
А. А. Овчинников*
кандидат технических наук, доцент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОБ ОДНОМ МЕТОДЕ ПОСТРОЕНИЯ КОДОВОЙ СИСТЕМЫ НА ОСНОВЕ КВАЗИЦИКЛИЧЕСКИХ КОДОВ

В данной статье рассматривается построение кодовой системы на основе квазициклических кодов. Проведен анализ корректирующей способности использующихся в системе кодов. Сформированы направления развития предложенной системы.
Ключевые слова: постквантовая криптография, криптография с открытым ключом, кодовая криптосистема, квазициклические коды

M. N. Isaeva*
Assistant
A. A. Ovchinnikov*
PhD, Tech., Associate Professor
*St. Petersburg State University of Aerospace Instrumentation

ABOUT ONE METHOD OF CONSTRUCTING A CODE-BASED CRYPTOSYSTEM BASED ON QUASI-CYCLIC CODES

This article discusses the construction of a code system based on quasi-cyclic codes. The analysis of the correcting ability of the codes used in the system is carried out. The directions of development of the proposed system are formed.
Keywords: post-quantum cryptography, public-key cryptography, code cryptosystem, quasi-cyclic codes

Введение

С учетом перспективной возможности создания квантовых компьютеров, большое значение сегодня приобретают постквантовые криптосистемы. В настоящее время действует конкурс NIST (*National Institute of Standards and Technology*) *Post-quantum competition* [1], в котором предлагаются квантово-устойчивые криптосистемы. Критерием построения таких систем является компромисс между обеспечением стойкости и размером открытого ключа. В данной статье рассматривается способ задания кодовой криптосистемы на основе квазициклических кодов, исправляющих ошибки.

Кодовые криптосистемы с открытым ключом

В 1978 году Р. Мак-Элисом была предложена первая кодовая криптосистема, в которой использовались коды Гоппы [2]. Стойкость данной криптосистемы основана на задаче исправления ошибок заданной кратности. Основным

недостатком этой системы является размер открытого ключа, например, при параметрах системы $n = 1024$ и $k = 524$ обеспечивается стойкость примерно 2^{50}, а размер открытого ключа около 65,5 Кбайт, а для параметров $n = 4096$ и $k = 2056$ стойкость равна примерно 2^{170}, но при этом открытый ключ будет более 1 Мб.

В последние годы рассматривались модификации системы Мак-Элиса на основе других кодов, нежели коды Гоппы, а также различные способы уменьшения размера ключа. В [3] предлагается вариант криптосистемы на основе квазициклических низкоплотностных кодов.

Квазициклическим (*quasi-cyclic* – QC) [3] называется линейный код, у которого циклический сдвиг любого кодового слова на некоторое фиксированное число позиций так же является кодовым словом. QC-код может быть задан с помощью проверочной (или порождающей) матрицы следующего вида:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{11} & \cdots & \mathbf{H}_{1\rho} \\ \vdots & \ddots & \vdots \\ \mathbf{H}_{\gamma 1} & \cdots & \mathbf{H}_{\gamma\rho} \end{bmatrix}, \qquad (1)$$

где $\mathbf{H}_{ij}$ – циркулянтная матрица размера $m \times m$, в которой все строки – циклический сдвиг первой строки. В случае, если открытый ключ задает QC-код, для заданного ключа достаточно хранить только первую строку циркулянта, что приводит к значительному сокращению размера ключа [3].

Кодовые системы на основе полного декодирования

Другим направлением развития системы Мак-Элиса является использование более трудной для злоумышленника математической задачи. Например, задача полного декодирования (исправление лидеров всех смежных классов) является NP-трудной [4].

В [5] предложен подход построения криптосистемы на основе задачи полного декодирования. Один из вариантов системы на основе такого подхода предложен в [6] с использованием низкоплотностных кодов, исправляющих пакеты ошибок длиной b. Под пакетом ошибок понимается двоичный вектор, у которого между первым и последним ненулевыми элементами находится не более b позиций. Ниже представлено описание такой криптосистемы:

1. Генерируется порождающая матрица $\mathbf{G}$ размера $k \times n$.
2. Генерируется случайная невырожденная матрица $\mathbf{M}_2$ размера $n \times n$.
3. Задается $\tilde{E}$ – множество пакетов ошибок длиной не более x и матрица $\mathbf{M}_1$, структура которой представлена на рис. 1 (для любого $\tilde{e} \in \tilde{E}$ вектор $\tilde{e} \cdot \mathbf{M}_1 \in E$, где E – множество пакетов ошибок длиной не более b).
4. Вычисляется матрица $\mathbf{M} = \mathbf{M}_1 \times \mathbf{M}_2$ размера $n \times n$.
5. Вычисляется матрица $\mathbf{G}' = \mathbf{G} \times \mathbf{M}_2$ размера $k \times n$.

Открытый ключ: $(\mathbf{G}', \mathbf{M})$ и $\tilde{E}$. Закрытый ключ: $(\mathbf{M}_1, \mathbf{M}_2, \mathbf{G})$.

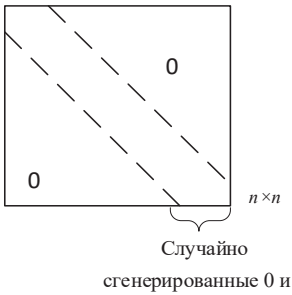


Рис. 1. Структура матрицы M_1

Шифрование: $\mathbf{m}$ – сообщение длиной k, берется случайный вектор ошибки $\tilde{\mathbf{e}}$ и вычисляется $\mathbf{e}' = \tilde{\mathbf{e}} \cdot \mathbf{M}$, шифртекст вычисляется следующим образом: $\mathbf{c} = \mathbf{m} \cdot \mathbf{G}' + \mathbf{e}'$.

Дешифрование: вычисляется $\mathbf{c}' = \mathbf{c} \cdot \mathbf{M}_2^{-1}$. Затем $\mathbf{c}'$ декодируется в $\mathbf{m}'$, используя алгоритм декодирования для кода $\mathbf{G}$.

В рассмотренной системе открытый ключ не обладает структурой, позволяющей уменьшить размер ключа. В данной статье предлагается вариант этой системы на основе квазициклических кодов.

Квазициклическая система на основе полного декодирования

Рассмотрим вариант системы, описанной в предыдущем разделе, на основе блочно-циркулянтной структуры. Параметры системы: γ, ρ задают количество блоков в матрицах, m – размер блоков.

1. Генерируется порождающая матрица $\mathbf{G}$, состоящая из $\gamma \times \rho$ блоков – циркулянтов размером $m \times m$. Для кода $\mathbf{G}$ известна полиномиальная процедура исправления пакетов ошибок длиной b.
2. Генерируется случайная матрица $\mathbf{M}_2$ размером $\rho \times \rho$, состоящая из блоков – циркулянтов размером $m \times m$.
3. Задается матрица $\mathbf{M}_1$, по диагонали которой располагаются ненулевые блоки циркулянтов (рис. 2).
4. Вычисляется матрица $\mathbf{M} = \mathbf{M}_1 \times \mathbf{M}_2$, которая также будет являться циркулянтной матрицей из $\rho \times \rho$ блоков.
5. Вычисляется матрица $\mathbf{G}' = \mathbf{G} \times \mathbf{M}_2$, которая также будет являться циркулянтной матрицей из $\rho \times \rho$ блоков.

Открытый ключ: $(\mathbf{G}', \mathbf{M})$. Закрытый ключ: $(\mathbf{M}_1, \mathbf{M}_2, \mathbf{G})$.

Шифрование: $\mathbf{m}$ – сообщение длиной k бит, берется случайный вектор ошибки $\mathbf{e}$, представляющий собой пакет длиной x. Шифртекст вычисляется следующим образом: $\mathbf{c} = \mathbf{m} \cdot \mathbf{G}' + \mathbf{e} \cdot \mathbf{M}$.

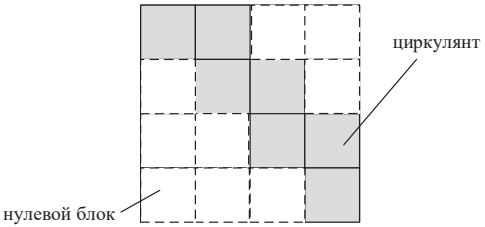


Рис. 2. Общая схема матрицы M_1 для блочно-циркулянтной структуры

Дешифрование: вычисляется $\mathbf{z} = \mathbf{c} \cdot \mathbf{M}_2^{-1} = \mathbf{m} \cdot \mathbf{G} + \mathbf{e} \cdot \mathbf{M}_1 = \mathbf{m} \cdot \mathbf{G} + \mathbf{e}'$. Так как вектор $\mathbf{e}' = \mathbf{e} \cdot \mathbf{M}_1$ представляет собой пакет длиной *b,* вектор *z* может быть продекодирован в коде **G**.

Для оценки параметров данной системы необходимо выбрать класс квазициклических кодов, исправляющих пакеты ошибок. Максимальная длина исправляемого пакета для линейного кода может быть эффективно определена с помощью процедуры, описанной в [7].

Рассмотрим блочно-циркулянтные матрицы для различного числа блоков. Максимальные длины исправляемых пакетов *b* приведены в табл. 1 для веса строки циркулянта, равного *t*.

Таблица 1

Корректирующая способность QC-кодов

γ	ρ	*m*	*t*	*b*
2	4	127	0,1m	119
2	4	127	0,3m	63
2	4	127	0,4m	119
2	4	127	0,5m	63
2	4	127	0,7m	120

γ	ρ	*m*	*t*	*b*
4	8	127	0,1m	126
4	8	127	0,3m	63
4	8	127	0,4m	126
4	8	127	0,5m	63
4	8	127	0,7m	126

Как видно из таблицы, существует высокая вероятность сгенерировать случайный квазициклический код, исправляющий пакеты длиной, незначительно меньшей размера блока *m*. Однако, с учетом структуры квазициклической матрицы $\mathbf{M}_1$, чтобы обеспечить длину пакета *b* не больше размера блока матрицы $\mathbf{M}_1$, на расположение пакета длиной *x* в векторе **e** необходимо добавить ограничение: пакет ошибок не должен затрагивать соседние циркулянты матрицы $\mathbf{M}_1$.

Очевидно, что размер занимаемой памяти, необходимой для хранения порождающей матрицы зависит от ее параметров – количества блоков и размера этих блоков. Для блочно-перестановочной конструкции это будет $\gamma \times \rho \times m \times m$, для блочно-циркулянтной: $\gamma \times \rho \times m$, так как нам необходимо хранить только

первую строку матрицы. В табл. 2 представлено сравнение размера порождающей матрицы.

Однако, накладываемые ограничения требуют тщательного подбора параметров и оценки стойкости. Предпочтительнее было бы использование структуры матрицы $\mathbf{M}_1$, изображенной на рис. 2, однако, это требует построения квазициклических кодов соответствующей корректирующей способности.

Таблица 2

Сравнение занимаемого места для хранения порождающей матрицы

n	k	γ	ρ	m	Размер для блочно-перестановочной конструкции	Размер для блочно-циркулянтной структуры
508	254	2	4	127	16129 Байт	127 Байт
1028	514	2	4	257	66049 Байт	257 Байт
1016	508	4	8	127	64516 Байт	508 Байт
2056	1028	4	8	257	264196 Байт	1028 Байт

Одним из возможных направлений для достижения этого может являться замена некоторых циркулянтов матрицы в (1) нулевыми блоками, что может рассматриваться как направление дальнейших исследований.

Заключение

В статье рассмотрен вариант кодовой криптосистемы на основе задачи полного декодирования с использованием квазициклической структуры матрицы. Приведены оценки корректирующей способности квазициклических кодов при исправлении пакетов ошибок. Для более точной оценки стойкости и улучшения параметров системы необходимы дальнейшие исследования в области корректирующей способности квазициклических кодов.

Библиографический список

1. NIST Post-Quantum Cryptography Standardization https://csrc.nist.gov/projects/post-quantum-cryptography (дата обращения: 30.03.2022).

2. McEliece R. J. A Public-Key Criptosystem Based on Algebraic Coding Theory / R. J. McEliece // DSN progress report 42–44. Jet Propulsion Laboratory, Pasadena, California, 1978. P. 114–116.

3. Baldi M. QC-LDPC Code-Based Cryptography / M. Baldi. Springer, 2014. 120 p.

4. Berlekamp E. On the inherent intractability of certain coding problems (corresp.) / E. Berlekamp, R. McEliece, H. van Tilborg // IEEE Transactions on Information Theory. May 1978. Vol. 24. P. 384–386.

5. Krouk E. A New Public-Key Cryptosystem / E. Krouk // Sixth Joint Swedish-Russian International Workshop on Information Theory. Moelle, Sweden, 1993. P. 285–286.

6. Krouk E. Code-Based Public-Key Cryptosystem Based on Bursts-Correcting Codes / E. Krouk, A. Ovchinnikov // The Thirteen Advanced International Conference on Telecommunications. 2017. P. 93–95.

7. Veresova A. M. About One Algorithm for Correcting Bursts Using Block-Permutation LDPC-Codes / A. M. Veresova, A. A. Ovchinnikov // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). Saint-Petersbug, Russia, 2019. P. 1–4.

УДК 004.056

В. С. Коломойцев*
кандидат технических наук, доцент
Е. Ю. Баглаенко*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

СПОСОБЫ РАСПРОСТРАНЕНИЯ СЕТЕВЫХ ЧЕРВЕЙ И ПОСЛЕДСТВИЯ ДЛЯ СИСТЕМ, ЗАРАЖЕННЫХ ИМИ

Работа посвящена исследованию методов распространения сетевых червей, а также возможных последствий заражения систем этим вредоносным программным обеспечением. В работе проведена классификация вредоносного программного обеспечения и рассмотрена схема распространения сетевых червей, таких как *MyDoom* и *Nimda*. Наибольшую опасность сетевые черви представляют в первые 10 часов своей работы, а их главная уязвимость проявляется в механизмах идентификации устройства на заражение.
Ключевые слова: вредоносное программное обеспечение, компьютерные вирусы, сетевые черви, сетевые угрозы, распространение сетевых червей, сетевая безопасность, информационная безопасность, информационная атака.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
E. Y. Baglaenko*
Student
*St. Petersburg University of Aerospace Instrumentation

METHODS OF SPREADING NETWORK WORMS AND THE CONSEQUENCES FOR SYSTEMS INFECTED WITH THEM

The work is devoted to the study of methods of spreading network worms, as well as the possible consequences of infecting systems with this malicious software. The paper considers the classification of malicious software, as well as the distribution scheme of network worms such as MyDoom and Nimda. It is shown that network worms pose the greatest danger in the first 10 hours of their work. At the same time, their main vulnerability is manifested in the mechanisms of identification of the device for infection.
Keywords: malicious software, computer viruses, network worms, network threats, spread of network worms, network security, information security, information attack

Введение

В эпоху глобализации обмен информацией между людьми как никогда важен. При этом злоумышленники могут предпринимать попытки получения несанкционированного доступа к этой информации, с целью ее повреждения или злонамеренно зашифровать ее, например, для шантажа жертвы. Для этих целей могут использоваться различные средства, наиболее популярными из них являются вирусы.

Компьютерным вирусом называется вид вредоносных программ, внедряющихся в код других программ, загрузочные секторы и различные объекты выполнения, а также способный распространять свои копии по различным каналам связи [1].

Несмотря на то, что данное определение является довольно точным, однако оно не позволяет сформировать определенный закон (правило), согласно которому можно будет отличить «вирус» от «хорошего» файла [2]. Признаками, указанными в определении, также обладают и программы, не являющиеся вредоносными. Более того злоумышленник будет стараться уменьшить ее вредоносность, снижая потребление ресурсов персонального компьютера или выдавая ее за «хорошую» (полезную для пользователя).

Сетевые вирусы и способы их распространения

Существует большое количество разновидностей вредоносных программ, и далеко не все из них можно четко классифицировать и отнести к какому-либо типу, поскольку они могут обладать свойствами, присущими разным группам [2].

Компьютерные вирусы можно разделить на следующие классы основных признаков: заражаемая операционная система; особенности работы алгоритмов программы; деструктивные способности; среда обитания [2]. По среде обитания вирусы можно разделить на: файловые; макро; загрузочные; сетевые.

Вирусы могут распространяться в нескольких средах, тем самым образую сочетания, например, файлово-сетевой вирус, заражающий файлы и отправляющий их копии по электронной почте [1].

Сетевые вирусы отличаются от остальных тем, что способны автономно, т. е. без участия человека, передавать свои копии на удаленный или локальный сервер. Благодаря этому свойству, такие вирусы крайне «заразны», а их эпидемии тяжело остановить. Рассмотрим подробнее такой класс вирусов.

Существует множество независимых способов распространения, наиболее примечательным из которых является импорт данных из адресной книги *Outlook Express* или подобного почтового клиента, просмотр на зараженном компьютере локальных файлов на наличие сетевых адресов, сканирование IP-адресов в данной подсети и генерирование случайного IP-адреса. Для того чтобы не парализовать сеть своей высокой активностью и иметь дальнейшие пути распространения, вирус использует пропускную способность подконтрольных ему информационных каналов лишь на некоторую часть [3].

Указанный вид распространения принадлежит так называемым почтовым вирусам. Заражение происходит за счет действий пользователя, просматривающего почту или ошибок в операционных системах или почтовых программах [3]. Данный способ является довольно привлекательным для разработчиков сетевых вирусов из-за обширного числа возможностей внедрения в почтовые сообщения.

Кроме этого, электронное сообщение также может передаваться в виде HTML-документа. При таком способе передачи сообщения допускается произ-

вольное форматирование текста и добавление ссылок на интернет-ресурсы, изображения или активные компоненты, например, элементы управления *ActiveX* или *Java*-апплеты. Такой формат представляет немалую угрозу для получателя, ведь ссылка может перенаправлять на вредоносный компонент расположенный на Web-сайтах злоумышленников или троянских Web-сайтах.

К сожалению, антивирусы, рассчитанные на проверку дисков и файлов, зачастую не способны обнаружить вредоносные программы в почтовых сообщениях, так как сами сообщения хранятся в базах данных почтовых программ, которые в свою очередь имеют разный формат. Однако современные антивирусы способны нейтрализовать угрозу на почтовых серверах или персональных компьютерах еще до того, как те попадут в почтовую программу [2].

В настоящий момент, в интернет-пространстве существуют большое количество децентрализованных сетей для обмена файлами, которые называются файлообменными или пиринговыми. Сетевые же вирусы, которые распространяются по таким сетям, называются вирусами пиринговых сетей. Такой вирус является вредоносной программой, которая специально предназначена для распространения в системах обмена файлами между пользовательскими компьютерами, например *Windows Messenger* или µ*Torrent*.

Можно заключить, что сетевые вирусы могут довольно быстро распространяться, так как пользователи постоянно обмениваются электронной почтой или файлами, и если пользователь не знает о наличии вредоносной программы на своем компьютере, то он может поневоле стать распространителем вируса, что приведет к вирусным «эпидемиям», наносящим большой вред компьютерным сетям.

На рис. 1 представлена схема распространения сетевых червей. График в первые часы быстро растет, и в течение этой «вспышки» вирус проявляет себя активнее всего, перегружая сети и наполняя их своими копиями.

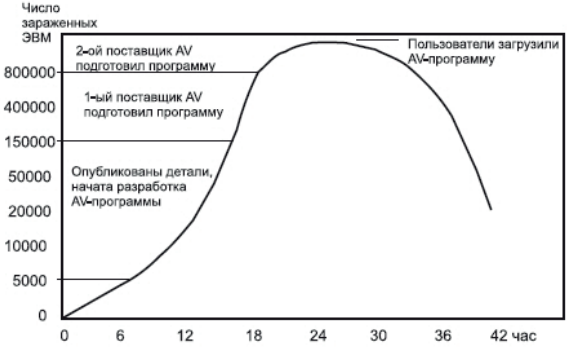


Рис. 1. Схема распространения сетевых червей

После такого роста наступает чуть более плавный спад активности червя. Это происходит из-за закрытия уязвимостей, которые использует вирус для

своего распространения, а также из-за того, что червь постепенно начинает встречать уже зараженные компьютеры [3].

Простейшим способом идентификации не зараженного устройства является «рукопожатие». Потенциальной системе для заражения посылается определенное ключевое слово, выглядящее как безвредный сетевой запрос. Если в системе уже находится червь, то он перехватывает пакет данных, возвращая отправителю другое ключевое слово, которое отличается от стандартного ответа незараженной машины [3].

Опасность сетевых червей

Ввиду обилия сетей в современном мире черви становятся все более опасными и могут наносить существенный материальный вред [4]. Основной угрозой сетевых червей является не только высокая нагрузка на сети и снижение Интернет-трафика, но и также полезная нагрузка, переносимая вирусом. Распространенной нагрузкой может являться порча или кража файлов зараженного компьютера, в некоторых случаях изменение или закрытие доступа к Web-сайтам, а также возможно организовать ботнет из носителей вируса, который будет использоваться для проведения DDOS-атак, спам-атак или майнинга криптовалюты [5].

В общем случае, нагрузка зависит от целей и возможностей злоумышленников, так, например, червь-вымогатель *Petya* шифровал файлы пользователей и перезаписывал, после чего также шифровал, главные загрузочные данные, код и данные необходимый для запуска операционной системы. Пострадавшим предлагалось выплатить определенную сумму, после которой вирус якобы расшифровал и вернул данные, чего естественно не происходило.

Таким образом, есть множество видов червей, но их можно классифицировать по нескольким критериям:

1. По вектору атаки: многовекторные; одновекторные (почтовые; пиринговые; использующие различные эксплойты для операционных систем; и др.).

2. По структуре: резидентные; нерезидентные.

Многовекторные типы червей являются наиболее опасными и заразными. Многовекторные черви – черви, использующие для проникновения в систему несколько механизмов (векторов атаки), например, пиринговые сети и почтовые программы. Ярким представителем вирусов такого типа является червь *Nimda*.

Nimda – сложный многовекторный червь, с компонентом массовой рассылки. Также он является первым червем, использующим зараженные компьютеры для сканирования уязвимостей Web-сайтов, что позволяет ему легко завладеть слабозащищенными Интернет-ресурсами. Своей эффективностью вирус обязан пяти векторам распространения: по электронной почте, через просмотр вредоносных Web-сайтов, через открытые сетевые ресурсы, а также через использования слабых мест *Microsoft IIS* 4.0/5.0. Такой набор возможностей инфицирования позволил вирусу заразить более 3 млрд компьютеров спустя 22 минуты после активации. *Nimda* являлся нерезидентным червем и оставался в

системе после перезагрузки компьютера. Избавиться от нерезидентных червей можно только при помощи антивирусной программы.

Рассмотренные векторы распространения больше не работают ввиду закрытия уязвимостей разработчиками операционных систем или антивирусных программ. Тем не менее, требуется проводить их исследование, так как одной из важнейших частей любого вектора атаки является человек, работающий с системой (социальная инженерия), а принципы его работы меняются гораздо реже, чем программное обеспечение вируса. Это происходит потому, что количество неопытных пользователей снижается гораздо медленнее, чем количество уязвимостей в той или иной системе.

Заключение

В статье рассмотрены основные способы распространения сетевых вирусов, а также последствия заражения систем сетевыми червями. Проведена классификация и выделены наиболее опасные программы, способные парализовать большие части сетей. Показано, что сетевой червь проявляет наибольшую активность в первые 10–12 часов своей работы, после чего его активность начинает снижаться, из-за того, что незараженные машины начинают встречаться реже.

Новые методы распространения вирусов появляются с каждой новой программой или способом обмена данными, но основная задача любого метода состоит в том, чтобы «обмануть» как программу, через которую реализуется атака, так и потенциальную жертву. Стоит внимательно относится к данным, которые пользователь предоставляет тем или иным программам, ведь обычный музыкальный проигрыватель получает доступ к файловой системе и при подключении к Интернету может без ведома пользователя отправлять его данные на удаленный сервер.

Библиографический список

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2011. 416 с.: ил. (Профессиональное образование).

2. Климентьев К. Е. Компьютерные вирусы и антивирусы: взгляд программиста. М.: ДМК Пресс, 2013. 656 с.

3. Остапенко О. А., Соколова Е. С., Разинкин К. А., Щекунских Р. А. К вопросу описания процесса распространения сетевого червя // Информационная безопасность. 2014. Т. 17. № 2. С. 328–329.

4. Сорокина Ю. К. Сетевые черви // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. 2014. С. 173–175.

5. Смирнова Е. В., Абачараева Э. Р. Современные угрозы вирусных атак на компьютерные сети и критерии их оценивания // Технологии инженерных и информационных систем. 2020. № 3. С. 3–12.

6. Дьяков Н. В. Применение методов социальной инженерии в социальных сетях // Общество 2020. № 2 (17). С. 126–128.

УДК 004.056

В. С. Коломойцев*
кандидат технических наук, доцент
В. О. Верхонина*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСОБЕННОСТИ ПОСТРОЕНИЯ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ ДЛЯ МЕССЕНДЖЕРОВ

В статье рассматриваются подходы к построению защищенной передачи данных в мессенджерах, и проводится их сравнение с точки зрения использования в системе. Также проводится сравнение сквозного и транспортного типов шифрования, в результате которого выявляются существующие достоинства и недостатки. Проведенная работа помогает структурировать принципы работы защищенной передачи сообщений.
Ключевые слова: мессенджер, система мгновенного обмена сообщениями, информационная безопасность, канал передачи данных, протокол Диффи – Хеллмана, обмен ключами.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
V. O. Verkhonina*
Student
*St. Petersburg University of Aerospace Instrumentation

FEATURES OF BUILDING A SECURE COMMUNICATION CHANNEL FOR MESSENGERS

The article discusses approaches to building secure data transmission in instant messengers and compares them from the point of view of their use in the system. A comparison is also made of end-to-end and transport types of encryption, as a result of which the existing advantages and disadvantages are revealed. The work done helps to structure the principles of secure messaging in instant messengers.
***Keywords*:** messenger, instant messaging system, data link, information security, Diffie-Hellman protocol, key exchange.

Введение

Существует множество программных приложений и автоматизированных систем, обрабатывающих огромное количество информации. На текущий день в связи с возросшей заинтересованностью мгновенным обменом сообщений, онлайн-звонков и онлайн-конференций стали популярны мессенджеры.

Мессенджер – это программное приложение для смартфона или персонального компьютера, которое обеспечивает обмен мультимедийными данными в режиме реального времени через Интернет. Такое средство, обрабатывающее и хранящее большой массив конфиденциальной информации, с точки зрения информационной безопасности, требует хорошей защищенности личных данных пользователей. Несмотря на огромные усилия по созданию различных

технологий защиты данных, находятся все более новые способы нарушения конфиденциальности информации.

Мессенджеры и файлообменники зачастую объединены в одно приложение по причине того, что мессенджер – это главный центр хранения всей персональной информации каждого человека, включающей в себя личные переписки, персональные данные, фото и видео. Говоря о мессенджерах, вне зависимости от множества различных систем по мгновенному обмену данными, они в большинстве своем используют схожие подходы построения и базовые механизмы защиты: построение защищенного канала обмена данными между абонентами, методы целостности при передаче данных, криптографические методы предоставления конфиденциальности, генерация секретных ключей и их согласование между абонентами.

Как правило, в мессенджерах используются собственные протоколы передачи данных, при этом шифрование обычно происходит на прикладном уровне, а уже затем зашифрованные данные передаются в транспортный протокол. Чаще всего используется SSL/TLS, ставший стандартом для всех защищенных веб-коммуникаций. Для защиты самих данных используется «*end-to-end*» (сквозное) шифрование или транспортное шифрование. Согласно сквозному шифрованию, данные шифруются на устройстве отправителя, а расшифровываются на устройстве получателя, криптографические ключи хранятся и генерируются на конечных устройствах пользователей, а не на серверах системы. Поэтому, никто кроме адресата не может прочитать содержимое зашифрованных сообщений. Тем временем, для транспортного шифрования свойственно наличие между абонентами промежуточного звена – сервера, который, получив передаваемое сообщение, расшифровывает его. Несмотря на то, что в транспортном шифровании защищенная передача сообщений основана на доверии к серверу, для широкой функциональности мессенджеров удобнее использовать именно его за счет того, что оно в отличие от сквозного шифрования дает возможность серверу обеспечить хранение истории переписки и подключение дополнительных абонентов к диалогу.

Таким образом, с точки зрения архитектуры все существующие решения можно разделить на два типа, с симметричными и асимметричными каналами связи. Для систем первого типа обмен данными между участниками диалога реализуем при условии, что все они подключены к единому каналу передачи данных одновременно. Для систем второго типа обмен данными возможен, если хотя бы одна из них имеет доступ к каналу. Второй подход требует наличия службы доставки – устройства, которое постоянно находится в канале связи, хранит сообщения и отправляет их пользователю при его появлении в сети.

Защищенная передача сообщений с симметричным каналом

Для того чтобы начать общение, двум пользователям A и B необходимо аутентифицироваться и сгенерировать общий секрет. Формирование общего секрета реализуется с помощью протокола Диффи – Хеллмана с параметрами p и g в группе Z_p, где p – некое простое число, а g – образующий элемент подгруппы группы Z_p. Далее участники A и B генерируют секретные ключи

x_A, x_B и обмениваются открытыми ключами g^{x_A} и g^{x_B}, при этом секретом является величина $g^{x_A x_B}$. Как правило, общий ключ используется для генерации секретных ключей.

По видимым в канале связи открытым ключам g^{x_A} и g^{x_B} злоумышленнику сложно определить общий ключ $g^{x_A x_B}$, однако у него есть возможность провести атаку «человек посередине». Чтобы избежать этой уязвимости, аутентификацию пользователей необходимо провести с применением схемы электронной подписи:

$$A \to B : sign(g^{x_A}, k_A), K_A; \;\; B \to A : sign(g^{x_B}, k_B), K_B,$$

где k_A и K_A – соответственно секретный и открытый ключи пользователя A; k_B и K_B – соответственно секретный и открытый ключи пользователя B; $sign$ – схема вычисления электронной подписи.

В современных системах открытые ключи g^{x_A} и g^{x_B} подписываются и публикуются соответствующими пользователями заранее. Для установления диалога нужно взять уже известные величины $sign(g^{x_A}, k_A), K_A$ с указанием собеседнику, какие ключи он должен использовать для соединения. Тогда сложно будет доказать факт установления разговора. Следующий шаг взаимодействия собеседников A и B – генерация ключей шифрования. Эти ключи формируются из общеизвестного секрета с использованием однонаправленной функции – как пример, хеш-функции, которая позволяет расширить значение общего секрета до необходимого размера, получив ключи шифрования. Для этих ключей существуют обязательные требования о времени их использования: их необходимо обновлять как можно чаще, использованные ключи необходимо сразу же стирать с устройства, и согласно протоколу Диффи – Хеллмана постоянно генерировать новые общие секреты.

Следующим этапом является непосредственно сама передача зашифрованного сообщения. Например, в большинстве мессенджеров шифрование реализовано с использованием блочного шифра, работающего в режиме CTR (*Counter mode*). Режим CTR гарантирует конфиденциальность пересылаемых данных, а для проверки подлинности источника данных используются ключевые хеш-функции, как вариант, по результату которой владелец секретного ключа может проверить, не нарушена ли целостность полученного сообщения.

Таким образом, конфиденциальность сообщений обеспечивается их шифрованием с помощью алгоритмов блочного шифрования, а контроль целостности сообщений и аутентификация источника данных – за счет использования ключевой хеш-функции.

Для симметричного канал характерно то, что внутри системы выстраиваются отношения, где никто никому не доверяет, а работа всей системы, зависит только от самих пользователей. У рассмотренного подхода есть минусы – например, наличие высокой нагрузки на устройство пользователя из-за посто-

янной необходимости вычислять новые ключи, шифровать и хранить сообщения до появления получателя в сети. Также присутствует недостаток в том, что приходится либо доверять инфраструктуре открытых ключей, либо устраивать личную встречу для обмена значениями $sign(g^{x_i}, k_i), K_i$.

На данный момент большинство мессенджеров имеют функцию сквозного шифрования, которая реализуется на основе показанного подхода.

Защищенная передача сообщений с асимметричным каналом

При работе с асимметричным каналом пользователь *A* создает аккаунт на специальном сервисе аутентификации, получает от него уникальный идентификатор и выдает сервису свои открытые ключи, подписанные личной электронной подписью. Чтобы начать общение/обмен данными, пользователь *A* запрашивает у сервиса открытый ключ пользователя *B* и высчитывает общий секрет. В первом отправленном сообщении, пользователь *A* указывает свой подписанный открытый ключ и открытый ключ пользователя *B*, который использовался в вычислении общего секрета. Далее сообщение высылается сервису доставки, который передаст его собеседнику.

Затем пользователь *B* проверяет подпись, в полученном им сообщении от пользователя *A* и вычисляет с их помощью общий секрет. Далее с помощью общего секрета, получает исходное сообщение. Чтобы отправить новое сообщение, пользователь *B* генерирует новый открытый ключ, используя старый ключ абонента, *A* и вычисляет новый общий секрет по протоколу Диффи – Хеллмана для шифрования нового сообщения. Абонент *B* вместе с сообщением передает пользователю *A* новый открытый ключ. Каждая отправка нового сообщения проходит путь вычисления открытого ключа, формирования нового секрета и шифрования сообщения.

Главная проблема системы с асимметричным каналом связи – это постоянная необходимость в доверии к сервису аутентификации, который может оказаться злоумышленником, выдающим себя за другого пользователя. Открытые ключи абоненты получают от сервиса аутентификации и, следовательно, нет возможности проверить их подлинность. Также из-за возможности сервиса в генерации пары открытых/секретных ключей и отправлению только этих пар по запросам абонентов, он может выступить «человеком посередине», получая и вскрывая все общение между участниками диалога.

В качестве примера системы с безусловным доверием, можно привести приложения для организации видео-звонков и видео конференций – *Zoom*. Благодаря тому, что сервер сам формирует ключи клиентов, он обеспечивает защиту от внешнего вредителя. А самому серверу, неинтересно, какой именно информацией обмениваются абоненты. Упомянутое ранее транспортное шифрование реализовано на основе показанного подхода.

Заключение

На основании проведенного исследования подходов защищенной передачи информации стоить заметить, что у каждого из подходов присутствуют свои

недостатки. Однако на сегодняшний день в сфере электронной связи большую популярность имеет подход с асимметричным каналом передачи информации. При этом пользователи должны глубоко понимать, что подобные системы, несмотря на то что они более удобны в применении, имеют доступ к их личной информации. К тому же в криптографии предполагается, что если что-то может пойти «не так», то рано или поздно это случится. Например, если сервису аутентификации теоретически доступна возможность читать переписку пользователей, то, скорее всего, он может начать это делать. В связи, с чем подобные системы нельзя считать достаточно надежными.

Библиографический список

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / Б. Шнайер. М.: Триумф, 2003. 30 с.

2. Богданов Д, Ноздрунов В. Мессенджеры и безопасность // Открытые системы. СУБД. 2020. № 04. 15 с.

3. Chris Alexander, Ian Avrum Goldberg. Improved User Authentication in Off-The-Record Messaging // Proceedings of the 2007 ACM workshop on Privacy in electronic society. New York: Association for Computing Machinery, 2007. February. P. 41–47.

4. Бирюков А. А. Информационная безопасность: защита и нападение. М: ДМК Пресс, 2012. 474 с.

5. Титов Е. Ю. Обеспечение информационной безопасности в мессенджерах // Проблемы науки. 2019. № 12 (48). С. 34.

6. Вишневская Ю. А. Анализ способов и методов незаконного распространения личных данных пользователей мессенджеров, социальных сетей и поисковых систем / Ю. А. Вишневская, М. В. Коваленко // Наука без границ. 2020. № 7 (47). С. 28–36.

УДК 519.6

В. С. Коломойцев*
кандидат технических наук, доцент
С. Р. Гринченко*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

СРАВНЕНИЕ АЛГОРИТМОВ ГЕНЕРАЦИИ ПРОСТЫХ ЧИСЕЛ И ПРЕДЛОЖЕНИЯ ПО ИХ УЛУЧШЕНИЮ

Работа посвящена исследованию алгоритмов генерации больших псевдослучайных простых чисел. В работе рассмотрены три генератора, используемых миром – генератор OpenSSL, генератор ГОСТ 34.10-2018 и генератор Люка. Также предложен улучшенный генератор, использующий принцип генератора Люка, но показывающий лучшие результаты. Проведены сравнительные тесты исследуемых алгоритмов по памяти, по времени и по качеству генерируемых простых чисел.
Ключевые слова: большие простые числа, криптография, распределение простых чисел, протокол OpenSSL, ГОСТ 34.10-2018, тест Люка.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
S. R. Grinchenko*
Student
*St. Petersburg University of Aerospace Instrumentation

COMPARISON OF ALGORITHMS FOR GENERATING PRIME NUMBERS AND SUGGESTIONS FOR IMPROVEMENT

The work is devoted to the study of algorithms for generating large pseudorandom primes. The paper considers three generators used by the world – the OpenSSL generator, the GOST 34.10-2018 generator and the Lucas generator. An improved generator is also proposed, using the principle of the Lucas generator, but showing better results. Comparative tests of the studied algorithms were carried out in memory, in time and in the quality of primes.
Keywords: large primes, cryptography, distribution of primes, OpenSSL protocol, GOST 34.10-2018, Lucas test.

Введение

Большинство ассиметричных алгоритмов шифрования данных основываются на простых числах. Для функционирования алгоритмов требуется генератор случайных простых чисел заданного диапазона разрядностей. Причем любой криптографически стойкий генератор простых чисел должен соответствовать двум требованиям [1]:

1. Распределение получаемых простых чисел должно быть близко к равномерному.

2. Процесс генерации конкретного случайного простого числа нельзя воспроизвести.

В данной статье будут замеряться характеристики трех генераторов, а именно:

1. Генератора *OpenSSL* [2].
2. Генератора ГОСТ 34.10-2018 [3].
3. Генератора Люка [4].

Также будет предложен новый генератор, основанный на принципах трех исследуемых. Его характеристики будут измерены и сравнены с характеристиками трех вышеперечисленных генераторов.

Предлагаемый генератор простых чисел

Покажем алгоритм, позволяющий быстро генерировать большие, вероятностно простые числа. Больше всего данный алгоритм схож с генератором Люка, но в его основе будет лежать не тест Люка, а вариант простых чисел Софи Жермен [5].

В основе алгоритма лежит период чисел, а также идея, что «простые числа одинакового заряда отталкиваются, а разного – притягиваются». В качестве заряда выступает результат деления на 3. Если остаток от деления на 3 равен 1, то число будем называть «отрицательно заряженным». Если остаток от деления на 3 равен 2 – «положительно заряженным». Особенность заключается в том, что, при перемножении разнозаряженных чисел с последующим умножением на 2 и прибавлением единицы, с высокой долей вероятности получается простое число. Данный феномен основан на совпадениях полупериодов чисел.

Поэтапно алгоритм генерации простого числа выглядит следующим образом:

1. На вход подается список простых чисел, среди которых не должно быть числа 3, но обязательно должно быть число 2. Чем длиннее этот список, тем ближе будет распределение получаемых простых чисел к равномерному.

2. Полученный список разбивается на 2 подсписка:

– отрицательно заряженные *O*, т. е. такие, у которых остаток от деления на 3 == 1.

– положительно заряженные *P*, т. е. такие, у которых остаток от деления на 3 == 2.

3. Сгенерировать число $n = O_x * P_y * 2 + 1$, где x и y – случайные числа.

4. $n_2 = n$

5. Если остаток от деления *n* на 3 == 1, то $n = n * P_y * 2 + 1$, y генерируется заново;

если остаток от деления *n* на 3 == 2, то $n = n * O_x * 2 + 1$, *x* генерируется заново;

если остаток от деления n на 3 == 0, то $n = n_2$ (крайне редкий случай).

6. Если разрядность *n* меньше *k*, то перейти к шагу 4,

если разрядность *n* больше *k*, то $n = n_2$ и перейти к шагу 5

если разрядность *n* == *k*, то *n* с очень высокой вероятностью – простое число.

7. Проверить n тестом простоты,

если тест показал, что n – составное, перейти к шагу 3,

если тест показал, что n – простое, вернуть n.

Причем, подавать на вход можно любые простые числа, кроме 3. Подавая определенные наборы чисел, можно легко и тонко настраивать свойства выходных чисел. В качестве простого примера: если известно, что сгенерировать нужно огромное число, например 8192 бита, можно подать на вход предварительно сгенерированные этим же алгоритмом просты числа чуть меньше, порядка 4096 бит. Тогда процесс генерации будет чрезвычайно быстрым. Однако, двойку подавать на вход следует всегда, чтобы алгоритм мог увеличивать число на один разряд и не застревал на 6 шаге.

Проведем несколько сравнительных тестов предлагаемого генератора и трех генераторов, перечисленных выше.

Время и память

Тест № 1

Поочередно сгенерируем 10000 простых чисел, разрядностью 512 бита. На вход генератору Люка и предложенному генератору подадим одинаковый список из 2000 случайных простых чисел, в диапазоне от 2 до 2^{50}, взятых из открытых источников [6]. Всего тест состоит из 101 прогона. Первый прогон холостой и его данные не записываются. Следующие 100 результатов обрабатывались как:

1. Среднее арифметическое времени t: T_s.

2. Усредненное арифметическое время t – удаляются 5% самых лучших и 5% самых худших результатов, далее считается среднее арифметическое: T_{us}.

3. Медианное время t: T_m.

4. Затрачиваемая память N – среднее арифметическое результатов затрат памяти.

Таблица 1

Показатели времени и памяти, затрачиваемых алгоритмами на прохождение теста № 1

	T_s, сек	T_{us}, сек	T_m, сек	N, Kbyte
Генератор *OpenSSL*	30,02	29,98	30,2	0,777
Генератор ГОСТ 34.10-2018	11,63	11,83	11,77	0,39
Генератор Люка	26,83	26,68	26,86	140
Предложенный генератор	17,11	16,97	17,15	168

Как видно из табл. 1, показатели генератора ГОСТ 34.10-2018 значительно превосходят все остальные алгоритмы. Однако, генератор ГОСТ 34.10-2018 способен генерировать простые числа разрядностью до 1025 бит. Следовательно, из следующего теста он выбывает.

Тест № 2

Повторяет шаги теста № 1, но теперь генерируются числа разрядностью 2048 бит. Для генератора Люка и предложенного генератора, входными параметрами будут те простые числа, которые получились в результате теста № 1.

Таблица 2

Показатели времени и памяти, затрачиваемых алгоритмами на прохождение теста № 2

	T_s, сек	T_{us}, сек	T_m, сек	N, Kbyte
Генератор *OpenSSL*	105,37	103,32	108,4	3
Генератор Люка	38,33	38,07	38,33	140
Предложенный генератор	22,12	22,04	22,22	712

Как видно из табл. 2, тест № 2 утвердил выигрыш генератора *OpenSSL* у генератора Люка и предложенного генератора в вопросе памяти. Однако показатели времени генератора *OpenSSL* значительно уступают показателям двух других генераторов.

Качество генерируемых простых чисел

Тест № 3

Качественный тест представляет из себя сбор и анализ статистики. В начале генерируются 10 000 случайных простых чисел разрядностью 100 бит. Далее происходит следующий анализ:

1. Подсчитывается количество дубликатов.
2. Подсчитывается количество вызовов теста простоты.
3. Подсчитывается количество псевдопростых чисел.

Таблица 3

Качественные характеристики простых чисел, сгенерированных алгоритмами

	Дубликаты	Тестов	Псевдопростых
Генератор *OpenSSL*	0	234 581	0
Генератор ГОСТ 34.10-2018	0	–	0
Генератор Люка	0	–	0
Предложенный генератор	0	10 026	0

Результаты из табл. 3 показывают, что все 4 генератора не имеют проблем с дубликатами и псевдопростыми числами в исследуемом диапазоне чисел.

Тест № 4

В данном тесте генерируется 1000000 простых 10 битных чисел. Далее будут построены графики распределения на множестве всех 10 битных простых чисел.

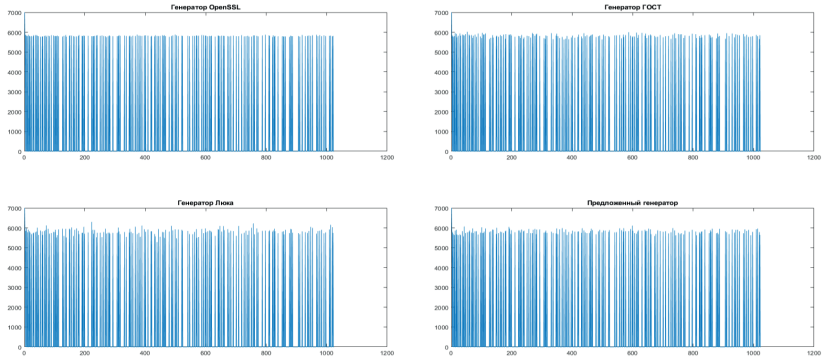


Рис. 1. Графики распределения сгенерированных псевдослучайных простых чисел

График генератора *OpenSSL* показывает, что у алгоритма распределение получаемых простых чисел очень близко к равномерному, в отличии от результатов генераторов ГОСТ 34.10-2018 и Люка.

График предложенного генератора показывает удовлетворительную близость распределение получаемых простых чисел к равномерному.

Проанализировав 4 генератора простых случайных чисел, можно сделать вывод – у каждого есть своя область применения:

1. Генератор *OpenSSL* медленный, но самый близкий к выполнению первого требования криптографически стойких генератор случайных простых чисел. Также его схема работы наиболее соответствует второму требованию, потому что детерминирована только генератором случайных чисел. Следовательно, генератор *OpenSSL* можно применять там, где важна не скорость генерации, а стохастичность.

2. Генератор ГОСТ 34.10-2018 отлично подойдет тогда, когда требуется быстро сгенерировать много небольших, гарантированно простых чисел.

3. Генератор Люка по всем параметрам близок к генератору ГОСТ 34.10-2018, кроме распределения. Однако, он способен генерировать большие простые числа, а не только малой и средней величины. Следовательно, его стоит применять там, где нужно сгенерировать гарантированно простые большие числа.

4. Представленный генератор предлагает скорость взамен гарантированности простоты. Этот генератор имеет смысл использовать тогда, когда требуется сгенерировать много очень больших простых чисел, не располагая при этом большим запасом времени.

Заключение

В работе предложен алгоритм генерации большие простые числа. Также продемонстрированы позитивные и негативные особенности алгоритмов гене-

рации простых чисел *OpenSSL*, ГОСТ, Люка и проведено их взаимное сравнение с предложенным алгоритмом. Показано, что каждый из исследуемых алгоритмов может быть использован для генерации простых чисел при накладываемых ограничениях на время процедуры генерации простого числа и затрачиваемой на нее памяти.

Библиографический список

1. Нестеренко Ю. В. Как строить большие простые числа // Введение в криптографию. 2001. С. 288.

2. Исходный код генерации ключей RSA OpenSSL, URL: https://github.com/openssl/openssl/blob/master/ssl/ssl_rsa.c (дата обращения: 30.03.2022).

3. ГОСТ 34.10-2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: межгосударственный стандарт // Разработан Центром защиты информации и специальной связи ФСБ России с участием открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»). М.: Стандартинформ, 2018.

4. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии // МЦНМО. 2003. С. 15–18.

5. Простые числа Софи Жермен. URL: https://planetmath.org/SophieGermainPrime (дата обращения: 30.03.2022).

6. Список первых 100000 простых чисел. URL: http://oeis.org/A000040/a000040.txt (дата обращения: 30.03.2022).

УДК 004.056.52

В. С. Коломойцев*
кандидат технических наук, доцент
Г. А. Грузденков*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МЕТОД МНОГОУРОВНЕВОГО ДОСТУПА К ДОКУМЕНТАМ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Работа посвящена описанию способа разделенного доступа к документам. В работе рассматривается структура docx-формата документов, и на ее основе предлагается способ внесения разметки в документ, с целью достижения разграничения областей работы пользователей в нем. Также, на базе архитектуры клиент-сервер, построена возможная система многопользовательского доступа к размеченному документу. После проектирования системы видно, что предлагаемый подход обеспечивает высокую вариативность разделения пользователей, безопасную работу множества пользователей с одним и тем же документом, а также широкие возможности для дальнейшего интегрирования в нее различных других подсистем.
Ключевые слова: защита информации; средства защиты информации; система электронного документооборота; информационная безопасность.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
G. A. Gruzdenkov*
Student
*St. Petersburg State University of Aerospace Instrumentation

THE WAY OF MULTI-LEVEL ACCESS TO THE DOCUMENTS IN THE ENTERPRISE CONTENT MANAGEMENT SYSTEMS

The work is devoted to describing the way of divided access to the document. The paper considers the structure of docx document format, and on its basis proposes a way to make markup in the document, in order to achieve delimitation of user work areas. Also, on the basis of client-server architecture, a possible system of multi-user access to the marked-up document is built. After designing the system, it can be seen that the proposed approach provides high variability of separation of users, secure work of many users with the same document, as well as ample opportunities for further integration of various other subsystems into it.
Keywords: Information security; computer systems; enterprise content management system; information security.

Введение

Современные системы электронного документооборота состоят из большого множества компонентов и систем, в том числе отвечающих за защиту документов при передаче по сети, а также при хранении документа. Однако, такие способы защиты, как правило, не позволяют гибко настраивать систему защиты при возникновении потребности разделять документ в соответствии с иерархией в компании. Это приводит к случаям, когда у всех пользователей, которые

работают с документом, имеется один и тот же уровень доступа ко всей информации, содержащейся в нем. Это может негативно сказаться, например, когда в документе содержится информация различного уровня конфиденциальности. Это приводит к тому, что необходимо присваивать документу максимально необходимый уровень конфиденциальности, что усложняет работу с ним другим сотрудникам, у которых уровень доступа ниже требуемого, хотя часть информации, содержащейся в нем, разрешена им для ознакомления. Также, данный факт, может привести к тому, что в случае утечки документа и успешного его расшифрования, злоумышленник получит доступ ко всему его содержимому.

В связи с этим, одним из решений указанных проблем может стать разработка метода разделения документа в зависимости от прав (ранга) пользователя в компании.

Метод разделения документа

В общем виде предлагается сначала размечать документ некоторыми идентификаторами пользователей, а затем осуществлять всю дальнейшую работу не как с одним документом, а как с множеством размеченных страниц, выдаваемых сотруднику в зависимости от наличия у него соответствующих «ранговых» ключей. Такой подход позволяет ограничить пользователям доступ к информации, которая, не нужна им для выполнения своих служебных функций.

Существует огромное множество различных форматов документов. Формат “.docx” является доминирующим в мире, благодаря простоте работы с ним, а также мощному инструментарию, предоставляемому компанией *Microsoft*.

Документ формата docx представляет собой zip-архив, в котором содержаться:

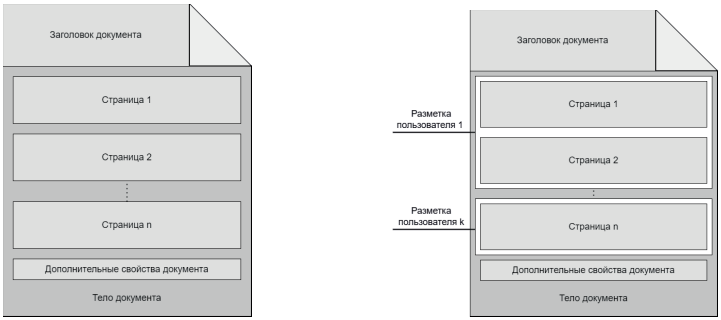
1. Некоторое количество xml документов, содержащих структуру основного документа, информацию необходимую для дополнительных атрибутов текста, информацию о типах контента в основном документе и т.п.
2. Различный дополнительный контент: рисунки, таблицы, ссылки и т.п.

Основная информация о тексте содержится в документе под названием «document.xml». Его внутренняя структура представлена на рис. 1, *а*.

Как видно из рисунка страницы занимают отдельные «узлы» xml-формата. Это означает, что возможно объединение страниц под некоторыми «узлами» таким образом, что страницы фактически становятся дочерними элементами некоторой «вершины», а в роли этой родительской «вершины» как раз и выступает разметка пользователя. Структура такого (размеченного) документа представлена на рис. 1, *б*.

При использовании такого подхода достигается наименьшее вмешательство во внутреннюю структуру документа, а значит, риск повредить информацию в документе также минимален. Простота вносимой разметки позволяет при помощи некоторых алгоритмов гибко редактировать данные в документе. Размеченный таким образом документ, будет выглядеть для конечного пользова-

теля как совершенно обычный документ docx-формата, а значит, никаких специфических условий и требований работы с ним не потребуется.



а) б)

Рис. 1. Структура .docx документа в формате xml (а); внедренная разметка в document.xml (б)

Система многопользовательской работы с размеченным документом

Допустим, что имеется несколько пользователей, которым необходимо работать с одним и тем же документом. Пользователи имеют различный допуск к информации, содержащийся в разных частях этого документа. Разделим такой документ на некоторые области и закрепим за ними пользователей. В итоге получится, что пользователь работает не со всем документом целиком, а только с той его частью, к которой имеет допуск.

Такая схема разделения должна отвечать следующим главным требованиям:

1. Пользователь должен иметь доступ к работе только над той частью документа (информации), к которой имеет соответствующие разрешения.
2. Операции, в результате которых добавляются новые и удаляются старые страницы, не должны приводить к нарушению «границ» работы пользователя.
3. Внедренная разметка не должна нарушать нормальную работу пользователя с документом.

Для соответствия этим требованиям предлагается система с клиент-серверной архитектурой, в которой все изменения, полученные от пользователей, хранятся на сервере (в «мастер-документе»). Пусть «мастер-документ» будет размечен методом, предложенным выше. Вся работа пользователей будет осуществляться с новыми документами, содержание которых, взято из соответствующей пользователю размеченной области. Иными словами, сервер будет направлять пользователям новые документы, составленные из страниц «мастер-документа». Схема такого способа представлена на рис. 2.

Когда пользователи закончат работу со своей частью, им необходимо будет сохранить внесенные изменения в «мастер-документ». В таком случае, от

клиента отправляется запрос на изменение пользовательской части. Сервер, при успешной обработке, запрашивает выданный им документ пользователя и встраивает его содержание в соответствующую область разметки. Стоит отметить, что работа с областями документа, а не с данными напрямую, позволяет сколь угодно уменьшать или увеличивать количество страниц со стороны пользователей, все изменения будут синхронизированы в «мастер-документе», а разметка не будет нарушена.

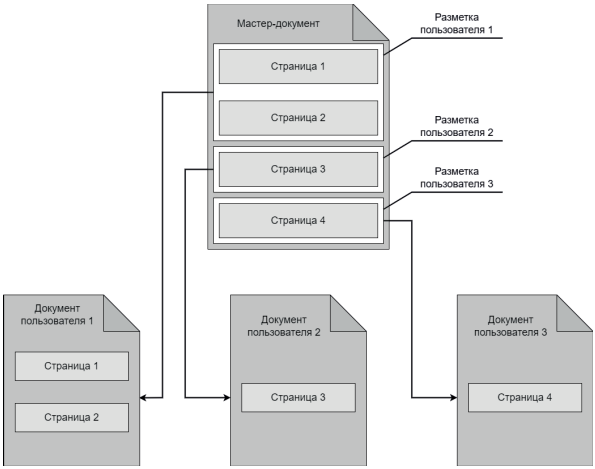


Рис. 2. Схема разделенного доступа к документу (выдача)

Пример отправления пользователями своих документов представлен на рис. 3.

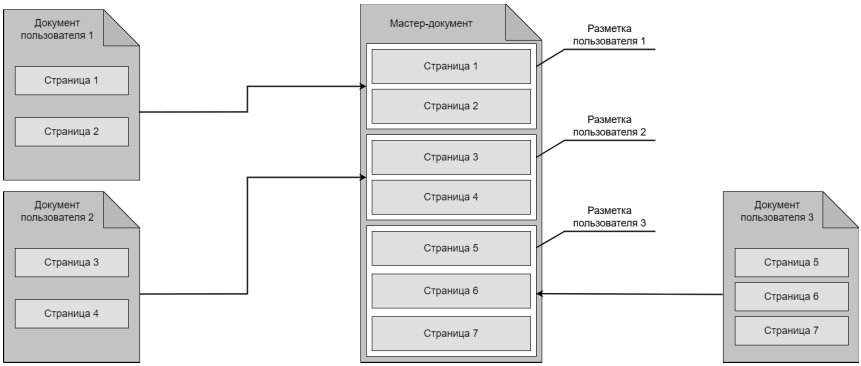


Рис. 3. Схема разделенного доступа к документу (получение)

При просмотре примеров, может сложиться впечатление, что пользователи размечены как отдельные сотрудники, но стоит понимать, что такая разметка условна. В действительности, благодаря гибкости такого подхода, например, руководитель может иметь доступ ко всему документу целиком, обладая правами суперпользователя, а скажем, бухгалтер, только к той части (к тем разметкам пользователей), которая относиться к его непосредственной деятельности (уровню доступа).

Заключение

В работе приведено описание структуры документов популярного формата docx, а также предложен метод внедрения разметки в такие документы, используя простые в реализации алгоритмы работы с xml-форматом. Метод позволяет разделить содержимое документа для сокрытия информации от лиц, не допущенных для работы с ней.

Также, на основе предложенного метода внедрения разметки, рассмотрена схема разделенного доступа к документу на базе архитектуры клиент-сервер. Такая схема позволяет безопасно разделять содержание документа на множество пользователей с различными правами, без потери удобства работы с документом. Представленный метод доставки до конечного пользователя его фрагмента позволяет снизить нагрузку на канал связи (по причине того, что отправляется только необходимая часть документа, а не весь целиком). Однако это может потребовать дополнительных вычислительных ресурсов как на стороне клиента, так и со стороны сервера.

Библиографический список

1. Blyth A., Cunliffe D., Sutherland I. Security analysis of xml, xml usage and xml parsing // COMPUTERS & SECURITY. Elsevier Science Publishing Company, Inc., 2003. 6. Vol. 22. P. 494.

2. Марияш П. И., Маслов А. А. Анализ СЭД: российский и зарубежный опыт внедрения СЭД // XI Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Информационные технологии в науке, бизнесе и образовании». М.: Московский государственный лингвистический университет, 2020. С. 444–450.

3. Ширяев В. В., Турчановская А. В. Извлечение текстовых данных из документов формата pdf, docx (doc) с помощью сторонних библиотек // Труды семинара по геометрии и математическому моделированию. Барнаул, 2019. 5. С. 158–160.

4. Шавловский А. Б. Исследование файлов текстовых форматов на примере форматов rtf, doc, docx // Молодежный научно-технический вестник. Москва. 2015. 10. С. 68.

5. Виниченко З. С. Проблемы внедрения и использования СЭД в организации (на примере СЭД Docsvision) и предложения по их решению // IV Международная научно-практическая конференция «Управление

документацией: прошлое, насояшее, будущее». Москва, 21–22 марта 2019 г. М.: ООО «ТЕРМИКА.РУ», 2019. С. 641–651.

6. Бровкина А. С. Программа архиватор 7-zip // Форум молодых ученых. ООО "Институт управления и социально-экономического развития", 2017. 1. С. 123–124.

7. Стружков Д. Н., Савинов Д. И. СЭД как основа ведения документооборота и методы ее криптозащиты // Научно-технический прогресс как фактор развития современного общества, Таганрог, 26 января 2019 г. Таганрог: ООО "ОМЕГА САЙНС", 2019. С. 208–210.

УДК 006.065

В. С. Коломойцев*
кандидат технических наук, доцент
Н. В. Ерышов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МЕТОД ОЦЕНКИ РИСКОВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ГОСТ Р 59339-2021

В работе предложен метод оценки рисков защиты информации по ГОСТ Р 59339-2021. Метод основывается на перечнях защищаемых объектов, угроз и системных процессов. Приведен пример работы метода на основе некоторых входных данных об объекте защиты, угрозах. Рекомендации, полученные после использования метода, позволяют повысить обоснованность принимаемых решений в процессе построения высокоэффективных систем защиты информации, благодаря большому количеству системных процессов, описанных в тексте ГОСТ Р. Предложенный метод имеет недостатки: высокая зависимость состава множеств от защищаемых объектов и угроз, которым они подвержены; для корректной интерпретации необходим последующий анализ полученных рекомендаций.
Ключевые слова: защита информации; системный анализ; методы защиты информации; информационная безопасность.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
N. V. Eryshov*
Student
*St. Petersburg State University of Aerospace Instrumentation

METHOD FOR ASSESING THE RISKS OF INFORMATION SECURITY BY GOST R 59339-2021

The method proposed in the work is based on GOST R and is used to assess information security risks. The method is based on lists of protected objects, threats, and system processes. This is an example of how the method works based on some input data about the protection object, threats. Recommendations received after using the method make it possible to increase the validity of decisions made in the process of building highly efficient information protection systems, due to the large number of system processes described in the text of GOST R. The proposed method has disadvantages: a high dependence of the composition of sets on protected objects and the threats to which they are exposed; for correct interpretation, subsequent analysis of the recommendations received is required.
Keywords: information security; system analysis; information security methods; Information Security.

Введение

В современном мире процесс системного анализа необходим во многих сферах деятельности человека. Системный анализ – это совокупность методов и принципов исследования сложных объектов, путем представления их в качестве систем и различного анализа этих систем [5]. В зависимости от то-

го, как хорошо будет проанализирован каждый процесс в системе, можно будет сделать вывод об уязвимостях тех или иных процессов, о надежности защиты информации, которую они используют. Для организации и систематизирования общих процессов в абсолютно разных организациях были разработаны различные стандарты. Так 30 ноября 2021 года был введен в эксплуатацию ГОСТ Р 59339-2021 «Защита информации в процессе управления рисками для системы» (далее, ГОСТ) [1]. Настоящий стандарт конкретизирует основные положения системного анализа для процесса управления рисками применительно к вопросам защиты информации. Нормативно-технический документ регламентирует комплекс норм, требований и правил к объекту стандартизации. Таким образом, возможно построить эффективную систему защиты информации, основываясь на рекомендациях ГОСТ [1].

Метод оценки рисков защиты информации по ГОСТ Р 59339-2021

Разработаем метод оценки рисков защиты информации в процессе управления рисками для системы, на основе текста ГОСТ и данных об потенциальных угрозах информационной безопасности и объектов защиты, которые можно получить в открытых источниках [1]. Для того чтобы разработать актуальную модель защиты информации, необходимо установить: объекты защиты и угрозы, применимые к данным объектам защиты.

На основании полученных и проанализированных данных можно выбрать необходимые системные процессы из текста ГОСТ и использовать возможные способы уменьшения рисков, указанные в Приложении Г к ГОСТ [1]. В Приложении Г указаны системный процесс, вероятностные показатели риска и возможные способы их уменьшения. Таким образом, получим готовые к применению инструкции по уменьшению рисков информационной безопасности в процессе управления рисками для системы.

В общем виде алгоритм работы метода выглядит следующим образом:

1. Анализируются отчеты по информационной безопасности организации. Выявляется, какие защищаемые объекты наиболее подвержены атакам.
2. Далее исследуются наиболее популярные угрозы, применимые к рассматриваемым объектам защиты. Сопоставляются объекты защиты и угрозы (отношение – один объект защиты ко многим угрозам). Неправильно составленные отношения объектов защиты к угрозам информационной безопасности могут привести к ошибочным выводам в дальнейшем.
3. После того, как всем объектам защиты были присвоены возможные угрозы, необходимо сопоставить угрозы и системные процессы из текста ГОСТ (одна угроза ко многим системным процессам) [1]. Связь один ко многим обусловлена тем, что к успешной реализации угрозы приводит не один системный процесс. Например, совокупность неправильной реализации, сопровождения, контроля системных процессов из разных областей приводит к реализации всего одной угрозы.

Пример применения метода оценки рисков защиты информации по ГОСТ Р 59339-2021

Рассмотрим пример использования метода оценки рисков защиты информации по ГОСТ Р 59339-2021 [1]. Имеется три множества: Множество объектов (*A*); Множество угроз (*K*); Множество системных процессов (Θ).

Объект защиты $\alpha \in A$. Любой α подвержен угрозам $\kappa \in K$. В свою очередь любая κ ссылается на один или несколько $\theta \in \Theta$, где θ – системный процесс.

Основываясь на отчетах по информационной безопасности различных компаний, был сформирован список наиболее популярных объектов защиты информации, а также список угроз информационной безопасности [2], [3], [4].

Во множество объектов *A* входят: 1) продукция, закупаемая для организации; 2) персонал организации; 3) сетевое оборудование организации; 4) облачные хранилища; 5) персональные данные; 6) коммерческая тайна; 7) государственная тайна.

Множество угроз *K* содержит [2], [3], [4]: 1) угроза нарушения цепочки поставок; 2) утечка персональных данных контрагентов; 3) утечка персональных данных сотрудников организации; 4) угроза нарушения работоспособности сетевого оборудования в результате несанкционированного доступа изнутри организации; 5) угроза утечки защищаемой информации в результате нарушения работы сетевого оборудования изнутри организации; 6) угроза утечки защищаемой информации в результате несанкционированного доступа к облачным хранилищам изнутри организации; 7) угроза появления аппаратных или программных сбоев; 8) угроза хакерской атаки из вне для кражи защищаемой информации; 9) кража оборудования; 10) халатность сотрудников; 11) подкуп должностных лиц.

Имея данные к анализу, составим таблицу соответствия объекта защиты и угроз, применимых к ней. Результат сопоставления представлен в табл. 1.

Таблица 1

Сопоставление объекта защиты и угроз

Номер объекта защиты (α)	Номер угрозы (κ)
1	1, 9, 10
2	2, 3, 10, 11
3	4, 5, 6, 7, 8, 10
4	3, 7, 8
5	2, 3, 11, 10
6	2, 3, 5, 6, 8, 10, 11
7	5, 6, 8, 10, 11

После сопоставления объекта защиты и угроз, применимых к ним, сопоставим угрозы и системные процессы, имеющиеся в тексте ГОСТ [1].

В тексте ГОСТ имеются методические указания по прогнозированию рисков [1]. Они состоят из: общих положений, анализируемых объектов для прогнозирования рисков, целей прогнозирования рисков, используемых методов и моделей, порядка прогнозирования, обработки и использования результатов, а также полного перечня системных процессов Θ. Перечень находится в Таблице Г.1, приложение Г к ГОСТ [1]. Всего он состоит из 28 пунктов. Пронумеруем все системные процессы и сопоставим их с угрозами. Результат сопоставления представлен в табл. 2.

Таблица 2

Сопоставление угрозы и системного процесса

Номер угрозы (κ)	Номер системного процесса (θ)
1	1, 6, 8, 12, 17
2	4, 5, 13, 16, 24, 25, 27
3	4, 5, 13, 10, 21
4	5, 12, 15, 18
5	3, 6, 7, 10, 12, 15, 21
6	3, 5, 9, 11, 21, 27
7	3, 5, 9, 15, 17, 18, 21, 24
8	5, 6, 7, 9, 11, 16, 20, 24, 26, 27, 28
9	1,3,5,16
10	5,16,19,20,26,27
11	4,5,8,9,13,16,19,26

Исследуем результаты работы метода, например, для объекта защиты под номером 4 (облачное хранилище). Для него были выявлены угрозы под номерами 3, 7, 8. В свою очередь угрозы под этими номерами ссылаются на системные процессы под номерами 4, 5, 6, 7, 9, 11, 10, 13, 15, 16, 17, 18, 20, 21, 24, 26, 27.

Облачные хранилища используются для хранения на них информации, в том числе и персональных данных [6]. Как видно из табл. 1 для облачного хранилища возможны: угроза утечки персональных данных сотрудников организации, угроза появления программах или аппаратных сбоев и угроза хакерской атаки извне для кражи защищаемой информации [7]. Так как вся информация содержится в цифровом виде, то возможны нарушения работы системного оборудования. Таким образом, злоумышленник, с некоторой вероятностью может получить несанкционированный доступ к информации, хранящейся в этом облачном хранилище.

Обратимся к тексту ГОСТ и, используя табл. 2 (соответствия К и Θ), рассмотрим некоторые полученные системные процессы [1]:

1. Процесс управления человеческими ресурсами системы. Для обеспечения защиты можно: ограничить круг лиц, имеющий право доступа к находящейся в облачных хранилищах информации; использовать сложные пароли для

получения доступа к конкретным областям информации, которые выдаются допущенным сотрудникам и иные.

2. Процесс сопровождения системы. Для обеспечения защиты можно: оптимизировать период времени между системными диагностиками; уменьшить время системной диагностики и уменьшить область диагностики; ввести в эксплуатацию системы, уменьшающие время восстановления системы после нарушения.

3. Процесс управления решениями. Для обеспечения защиты можно: выбрать период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления решениями; уменьшить частоту возникновения источника угроз.

4. Процесс управления информацией системы. Для обеспечения защиты можно: обеспечить необходимую актуальность обновляемой информации; обеспечить необходимой безошибочностью действия должностных лиц; обеспечить полное оперативное отражение в системе новых объектов и явлений.

5. Процесс гарантии качества для системы. Для обеспечения защиты можно: повысить уверенность в ожидаемой готовности системы к выполнению требований, предъявляемых к ней.

Стоит отметить, что полученные результаты сами по себе не раскрывают полную модель защиты информации и требуют последующего анализа для каждой конкретной системы и организации [7].

Заключение

В работе предложен метод оценки рисков защиты информации по ГОСТ Р 59339-2021. Метод позволяет оценить процесс защиты информации в процессе управления рисками для системы, основываясь на данных о защищаемых объектах, угрозах и системных процессах. Приведен пример работы метода на основе некоторых входных данных по объектам защиты, угрозам и системным процессам. Рекомендации, полученные после использования метода, позволяют повысить обоснованность принимаемых решений в процессе построения высокоэффективных систем защиты информации, благодаря большому количеству системных процессов, описанных в тексте ГОСТ Р 59339-2021. Также с увеличением количества защищаемых объектов и угроз, возрастает эффективность применения данного метода. Показано, что предложенный метод имеет недостатки: зависимость от защищаемых объектов и угроз, которым они подвержены; для корректной интерпретации необходим последующий анализа полученных рекомендаций.

Библиографический список

1. ГОСТ Р 59339-2021 Защита информации в процессе управления рисками для системы: нац. стандарт Рос. Федерации / Разраб. ФГУ ФИЦ ИУ РАН, ФАУ ГНИИИ ПТЗИ ФСТЭК России, ФБУ «НТЦ Энергобезопасность», ООО НИИПМС. Введ. 2021-11-30. Офиц. изд. Москва: Стандартинформ, 2021. 46 с.

2. Актуальные тренды кибербезопасности в 2021 году. URL: https://www.securityvision.ru/blog/aktualnye-trendy-kiberbezopasnosti-v-2021-godu// (дата обращения: 22.03.2022).

3. Актуальные киберугрозы: II квартал 2021 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/#id2 (дата обращения: 14.03.2022).

4. Угрозы информационной безопасности. URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 19.03.2022).

5. Моисеев Н. Н. Математические задачи системного анализа: учеб. пособие для вузов по спец. «Прикл. математика». М.: Наука, 1981. 487 с.

6. Защита данных при использовании облачных сервисов. URL: https://cyberleninka.ru/article/n/zaschita-dannyh-pri-ispolzovanii-oblachnyh-servisov/viewer (дата обращения: 20.03.2022).

7. Угрозы информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ (дата обращения: 22.03.2022).

УДК 004.057.4

В. С. Коломойцев*
кандидат технических наук, доцент
Е. А. Калинина*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРОТОКОЛЫ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ СООБЩЕНИЙ

Статья посвящена исследованию современных протоколов, используемых в системах мгновенного обмена сообщений для обеспечения защиты информации при передаче. В статье приведен обзор свойств данных протоколов и представлено описание особенностей их реализации. Показано, что в большинстве случаев повышение уровня защищенности при передаче данных ведет к пропорциональному повышению объема затрачиваемых вычислительных ресурсов и снижению быстродействия протокола.
Ключевые слова: информационная безопасность, сетевая безопасность, системы обмена сообщениями, обмен мгновенными сообщениями, криптографические протоколы, асимметричное шифрование, обмен ключами.

V. S. Kolomoitcev*
PhD, Tech., Associate Professor
E. A. Kalinina*
Student
*Saint Petersburg State University of Aerospace Instrumentation

PROTOCOLS OF SECURE MESSAGE TRANSMISSION

The article is devoted to the study of modern protocols used in instant messaging systems to ensure the protection of information during transmission. The article provides an overview of the properties of these protocols and describes the features of their implementation. It is shown that in most cases, an increase in the level of security during data transmission leads to a proportional increase in the amount of computing resources consumed and a decrease in the speed of the protocol.
Keywords: information security, network security, messaging systems, instant messaging, cryptographic protocols, asymmetric encryption, key exchange

Введение

В настоящее время системы обмена сообщениями используются повсеместно: как частными пользователями, так и большими компаниями. Наибольшую популярность приобретают системы мгновенного обмена сообщениями, позволяющие пользователям быстро общаться между собой с помощью коротких текстовых предложений. Как правило, для подключения к системе каждый пользователь должен обладать программой-клиентом, которая взаимодействует с общим сервером, передающим сообщения между пользователями. Поскольку системы мгновенного обмена сообщениями могут использоваться для обсуждения конфиденциальной информации, встает вопрос об обеспечении безопасности передачи данных между собеседниками. Система обмена сообщениями, по-

зиционирующая себя как защищенная, должна не допускать попадания содержимого переписки к третьим лицам и обеспечивать: конфиденциальность передаваемой информации, идентификацию участников переписки, аутентификацию и целостность получаемых данных. За обеспечение безопасности при передаче данных отвечает протокол, на котором основана система обмена сообщениями. Рассмотрим и проанализируем на предмет защищенности некоторые наиболее популярные протоколы и технологии, используемые в системах обмена сообщениями.

Протоколы и технологии систем обмена сообщений

Изначально большинство систем обмена сообщениями использовало для защиты алгоритмы симметричного шифрования с постоянными ключами. Такой подход опасен тем, что, если злоумышленник перехватит ключ шифрования, он сможет прочесть все ранее переданные сообщения.

Одним из первых протоколов, решающих проблему «упреждающей секретности» (*Perfect Forward Secrecy*) стал криптографический протокол *Off-the-Record Messaging* (OTR). Перед началом общения собеседники выполняют не аутентифицированный обмен ключами по протоколу Диффи – Хеллмана для настройки зашифрованного канала, а затем выполняют взаимную аутентификацию внутри этого канала и устанавливают общий секретный ключ.

Для шифрования сообщения пользователи используют алгоритм AES в режиме счетчика. Полученный шифротекст аутентифицируется с помощью HMAC и отправляется собеседнику, который в свою очередь с помощью общего секрета генерирует ключи для AES и HMAC, дешифрует сообщение и проверяет его целостность [1]. В OTR пользователи генерируют новый секретный ключ при отправке каждого нового сообщения – это обеспечивает невозможность чтения старых сообщений при перехвате нового ключа.

Процесс генерации нового ключа для каждого сообщения требует значительных вычислительных ресурсов, что сказывается на скорости общения между пользователями.

В качестве альтернативного OTR метода передачи сообщений рассмотрим протокол XMPP: *Extensible Messaging and Presence Protocol* (XMPP) – это протокол, разработанный на основе языка разметки XML. Сеть XMPP использует клиент–серверную архитектуру: пользователи не общаются напрямую друг с другом, а передают сообщения через сервер. Каждый пользователь имеет свой уникальный идентификатор, состоящий из имени пользователя и доменного имени сервера, на котором находится этот пользователь [2].

Безопасность в XMPP обеспечивается использованием протокола TLS и фреймворка SASL. SASL позволяет клиенту и серверу производить взаимную аутентификацию, с использованием заранее выбранных механизмов, например пароля и хэш-функции MD5 [3]. С помощью протокола TLS реализуются шифрование, аутентификация передаваемых сообщений и проверка их целостности. Перед началом передачи сообщений между клиентом и сервером происходит согласовывание способа шифрования данных и производится обмен ключами с

помощью алгоритма RSA или протокола Диффи – Хеллмана. После настройки соединения между сервером и пользователями для передачи сообщений используются методы симметричного шифрования (для повышения быстродействия).

Еще одним криптографическим протоколом, используемым в системах мгновенного обмена сообщениями, является протокол *Signal*. Данный протокол обеспечивает сквозное шифрование, а также расширенные свойства безопасности – «совершенную упреждающую секретность» (*Perfect Forward Secrecy*) и «секретность в будущем» (*Future Secrecy*).

Для аутентификации и получения общего секрета пользователи производят первоначальный обмен ключами с помощью протокола X3DH (*extended triple Diffie-Hellman*), а затем отправляют собеседнику свои одноразовые открытые ключи. Эти ключи используются собеседником для генерации новой ключевой пары «храповика» Диффи – Хеллмана и обновления ключей цепочки сообщений [4]. При получении нового сообщения пользователь с помощью текущего ключа цепочки сообщений вычисляет ключ для дешифрования принятых данных [4]. Таким образом, каждое сообщение, отправленное пользователем, шифруется с использованием нового ключа сообщения, что помогает обеспечить «упреждающую секретность». Однако это может сказываться на быстродействии системы из-за больших потребностей в вычислительных ресурсах.

Протоколы OTR, XMPP, и *Signal* используют клиент-серверную архитектуру, обладающую существенным недостатком: при возникновении проблем с сервером передача данных между пользователями становится невозможной. Протокол защищенной передачи сообщений *Bitmessage* использует одноранговую архитектуру, что позволяет сохранять способность передачи данных даже при отключении одного или нескольких узлов.

Первым делом собеседники проводят аутентификацию, в процессе которой обмениваются результатами хэширования открытых ключей (используются SHA-512 или RIPEMD-160), которые также являются адресами пользователей в *Bitmessage.* Для отправки сообщения пользователю необходимо предварительно выполнить «доказательство выполнения работы» (*Proof-of-work*) в виде обнаружения частичной коллизии хэша сообщения. Сложность проверки работоспособности пропорциональна размеру сообщения и должна быть установлена таким образом, чтобы компьютер затрачивал в среднем 4 минуты на отправку сообщения [5].

Механизм передачи сообщений в *Bitmessage* аналогичен системе транзакций и передачи блоков Bitcoin, поэтому при подключении к сети все пользователи будут получать все сообщения и пытаться расшифровать каждое сообщение с помощью своих закрытых ключей, чтобы узнать, предназначается ли сообщение им. Такой вариант является крайне ресурсозатратным и может быть неудобен при необходимости быстро обмениваться информацией.

Для избегания необходимости дешифровать каждое сообщение с помощью своих закрытых ключей, создатели других децентрализованных протоко-

лов предложили добавлять к сообщению информацию о его отправителе. Именно такой способ решения проблемы используется в протоколе *Briar*, в котором информация об отправителе прикрепляется к сообщениям в виде тегов. Передача данных в *Briar* осуществляется через браузер TOR, а при отсутствии интернет-соединения – через *Bluetooth* или Wi-Fi. Способ аутентификации собеседника также отличается от способов, используемых в других протоколах: пользователи сначала сканируют QR-коды друг друга, содержащие открытый ключ, а затем генерируют общий секрет по протоколу Диффи – Хеллмана.

Безопасность передаваемой информации в *Briar* обеспечивается с помощью протокола транспортного уровня BTP (*Bramble Transport Protocol*). Собеседники шифруют сообщения и с помощью общего секрета генерируют идентичные последовательности тегов, затем отправитель прикрепляет тег к каждому сообщению, которое он отправляет. Получатель в свою очередь распознает тег, удаляет его из своей последовательности и использует соответствующий ключ для аутентификации и дешифрования данных [6]. Каждый пользователь хранит пару ключей: один для генерации тегов и один для аутентификации и шифрования данных. Для обеспечения «упреждающей секретности» оба ключа используются только один раз и обновляются для каждого нового сообщения.

С течением времени протоколы все чаще стали разрабатываться для обеспечения нужд конкретных систем обмена сообщениями. Так, например, криптографический протокол *Proteus* был разработан специально для системы обмена сообщениями *Wire*. Для обеспечения безопасности передачи данных *Proteus* использует имплементацию алгоритма Двойного храповика с добавлением пре-ключей (*prekeys*) [4]. Перед началом общения каждый пользователь генерирует пару открытого и закрытого ключей, а также набор пре-ключей, которые будут храниться на его устройстве. Затем, используя пре-ключ и открытый ключ собеседника, участники с помощью протокола Диффи – Хеллмана на эллиптических кривых генерируют общий секрет [7]. Непосредственно передача сообщений происходит по алгоритму Двойного храповика аналогично протоколу *Signal.*

Так как *Proteus* использует клиент-серверную архитектуру, зашифрованные пакеты данных сначала попадают на сервер, который оповещает пользователя, если тот пытается отправить собеседнику сообщение, зашифрованное на чужом открытом ключе.

Ситуация, когда сообщения дешифруются на сервере, предоставляет злоумышленнику еще одну возможность заполучить передаваемые данные. Для решения этой проблемы протокол *MTProto* применяет сквозное шифрование: при его использовании прочесть сообщения могут только отправитель и получатель. Для передачи данных протокол использует клиент-серверную структуру сети: при авторизации пользователь и сервер осуществляют обмен ключами по протоколу Диффи – Хеллмана и генерируют общий секрет, впоследствии используемый в качестве ключа авторизации. С целью обеспечения защищенности старых сообщений от прочтения, пользователи генерируют новый общий секрет по истечении недели или после того, как старый был использован более

100 раз [9]. Перед отправкой текст сообщения объединяется вместе с идентификатором сообщения, его порядковым номером и некоторыми избыточными данными с сервера (*salt*). Полученный пакет данных шифруется с использованием алгоритма шифрования AES-256 в режиме IGE (*Infinite Garble Extension*) и в свою очередь объединяется с ключом сообщения, полученным путем взятия хеш-функции SHA-256 от исходного сообщения и 32-х бит ключа авторизации.

Заключение

В статье дано определение защищенной передачи данных, описаны протоколы, используемые для обеспечения защищенной передачи в системах обмена сообщениями, их характеристики и способы реализации.

В зависимости от поставленных задач, при реализации собственных систем обмена сообщениями разработчики могут использовать протокол, отвечающий необходимым требованиям. Например, если в приоритете повышенная конфиденциальность рекомендуется использовать протоколы *OTR*, *Signal* или *Briar*, однако стоит учесть, что необходимость шифровать каждое сообщение на новом ключе требует значительных затрат вычислительных ресурсов и снижает быстродействие протокола. В протоколе *MTProto* также используется регулярная смена ключей, однако ключ меняется через каждые 100 сообщений, что позволяет ему выигрывать в быстродействии.

Библиографический список

1. Di Raimondo M., Gennaro R., Krawczyk H. Secure off-the-record messaging // WPES'05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. 2005. С. 81–89.

2. An Overview of XMPP. URL: https://xmpp.org/about/technology-overview/ (дата обращения: 25.03.2022).

3. Simple Authentication and Security Layer (SASL). URL: https://www.isode.com/products/sasl.html (дата обращения: 25.03.2022).

4. Cohn-Gordon K., Cremers C., Dowling B., Garratt L., Stebila D. A Formal Security Analysis of the Signal Messaging Protocol (Extended Version) // Journal of Cryptology. 2019. № 33. С. 2–4.

5. Warren J. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System. 2012. С. 2.

6. Bramble Transport Protocol, version 4. URL: https://code.briarproject.org/briar/ briar-spec/blob/master/protocols/BTP.md (дата обращения: 26.03.2022).

7. Wire Whitepapers. Security. URL: https://wire.com/en/resources/whitepapers/security/ (дата обращения: 26.03.2022).

8. MTProto 2.0 End-to-End Encryption, Secret Chats. URL: https://core.telegram.org/api/end-to-end (дата обращения: 27.03.2022).

УДК 004.773

О. Ю. Куров*
студент
М. Н. Исаева*
ассистент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ В ЗАГОЛОВКАХ TCP ПАКЕТОВ

В статье рассматривается метод реализации скрытой передачи информации с помощью полей заголовков протоколов IP-пакета и сегмента TCP. Это возможно, так как некоторые поля не принимают непосредственного участия и могут быть изменены без потери передающих способностей.
Ключевые слова: передача данных, TCP заголовки, пакеты данных.

O. Y. Kurov*
Student
M. N. Isaeva*
Assistant
* St. Petersburg State University of Aerospace Instrumentation

HIDDEN DATA TRANSMISSION IN TCP HEADERS

This article discusses a method for implementing covert information transfer using the protocol header fields of an IP packet and a TCP segment. This is possible because some fields are not directly involved and can be changed without loss of transmission capabilities.
Keywords: data transmission, TCP headers, data packets.

Введение

В рамках концепции безопасности было предложено несколько идей для защиты данных при передаче по сети Интернет: сокрытие содержимого сообщения, которое было названо криптографией и сокрытие существования такого сообщения, которое было названо стеганографией [1]. В этой статье рассмотрено, что такое сетевая стеганография, набор протоколов TCP/IP, методы, использующие заголовок протокола TCP для стеганографии, реализация стеганографии в TCP/IP, предлагаемая система, практическая реализация, результаты и выводы.

Набор протоколов TCP/IP

Абсолютное большинство компьютерных сетей работает на основе стека TCP/IP, включающего в себя набор стандартизированных протоколов, обеспечивающих передачу данных по сети, а также обмен служебными и управляющими сообщениями для организации взаимодействия между сетевым оборудованием. Название этого набора произошло от двух основных протоколов: IP *(Internet Protocol* – межсетевой протокол) и TCP (*Transmission Control*

Protocol – протокол управления передачей). Протокол TCP – это протокол, ориентированный на гарантированную передачу данных. В процессе обмена информацией, данный механизм устанавливает соединения и подтверждает, что сообщения были доставлены.

Протокол IPv4 состоит из тринадцати обязательных полей и поля для вспомогательных опций. На рис. 1 представлена структура IPv4 заголовка.

<table>
<tr><td>4 бита
номер версии</td><td>4 бита
длина заголовка</td><td>8 бит
тип сервиса</td><td>16 бит
общая длина</td></tr>
<tr><td colspan="2">16 бит идентификатор пакета</td><td>3 бита флаги</td><td>13 бит смещение фрагмента</td></tr>
<tr><td>8 бит время жизни</td><td colspan="2">8 бит протокол верхнего уровня</td><td>16 бит контрольная сумма</td></tr>
<tr><td colspan="4">32 бита IP адрес источника</td></tr>
<tr><td colspan="4">32 бита IP адрес приемника</td></tr>
<tr><td colspan="4">параметры и выравнивание</td></tr>
</table>

Рис. 1. Структура IPv4 заголовка

Описание полей IPv4 заголовка: версия протокола – текущая версия используемого протокола IP; размер заголовка – размер заголовка IP; тип обслуживания – используются для разделения трафиков на классы обслуживания; указатель перегрузки – предупреждение о перегрузке сети; размер пакета – полный размер пакета; идентификатор – идентификационный номер; флаги – флаги контроля фрагментации; смещение фрагмента – указывает смещение для поля данных; время жизни пакета – определяет максимальное количество маршрутизаторов на пути пакета; протокол верхнего уровня – указывает на тип инкапсулированного протокола; контрольная сумма – контрольная сумма для проверки целостности; адрес источника – IP-адрес отправителя; адрес получателя – IP-адрес получателя.

Структура TCP заголовка [3] представлена на рис. 2.

<table>
<tr><td colspan="2">16 бит порт источника</td><td colspan="2">16 бит порт получателя</td></tr>
<tr><td colspan="4">32 бита номер последовательности</td></tr>
<tr><td colspan="4">32 бита номер подтверждения</td></tr>
<tr><td>6 бит длина заголовка</td><td>6 бит резерв</td><td>6 бит флаги</td><td>16 бит размер окна</td></tr>
<tr><td colspan="2">16 бит контрольная сумма</td><td colspan="2">16 бит указатель важности</td></tr>
<tr><td colspan="4">32 бита поле опций</td></tr>
</table>

Рис. 2. Структура TCP заголовка

Описание полей TCP заголовка: порт источника – порт приложения клиента, на который отправляются пакеты; порт назначения – идентификатор порта получателя, на который отправляются пакеты; порядковый номер – порядковый номер пакета; номер подтверждения – порядковый номер байта, который отправитель может получит; длина заголовка – размер TCP заголовка; резерв – резервное поле; флаги – поле, содержащее 6 битовых флагов: URG (указатель важности), ACK (номер подтверждения), PSH (отправка накопленных данных из буфера), RST (сброс соединения), SYN (установка соединения), FIN (завершение сессии);

размер окна – количество байт, которые можно принять; контрольная сумма – 2-байтное дополнение к сумме всех 2-байтных слов заголовка и данных; указатель важности – порядковый номер байта, которым заканчиваются важные данные; поле опций – применяется в случаях расширения протокола.

Подходы к сокрытию данных в полях заголовков IP/TCP пакетов

Для встраивания данных в заголовок IP-пакета теоретически можно использовать следующие места [2]:

1. Биты указателя перегрузки в поле «Тип сервиса», так как многие хосты не поддерживают работу с ним и не используют его.
2. «Поле идентификатора». Важным требованием для использования этого поля является то, что все передаваемые пакеты не должны быть фрагментированы. Необходимо разделять их «вручную» и идентифицировать как отдельные и законченные сообщения.

Для встраивания данных в заголовок TCP пакета можно использовать следующие поля:

1. Поле «Номер последовательности». При обмене сообщениями в установленном соединении каждый пакет имеет номер последовательности на единицу больше предыдущего, необходимо, чтобы соединение не устанавливалось в привычном понимании.
2. Поле «Указатель важности». Данное поле обрабатывается только при установке соответствующего флага и никак не влияет на процесс передачи данных.
3. Поле «Опции». Это поле содержит данные, которые не используются на приемной стороне (метка времени).

Поле «Опции» и «Номер последовательности» имеют размер, превышающий размер поле «Указатель важности» в два раза, что позволяет передать большее количество информации за то же количество пакетов. Помимо этого, лучше использовать поле «Опции», так как использование поля «Номер последовательности» накладывает ограничения на создание TCP сессии [4].

Реализация метода встраивания сообщения на основе TCP/IP заголовков

Программное средство разработано на языке программирования *Python*. Оно решает следующие задачи: криптографическое преобразование данных за счет сложения сообщения с ключом; запись зашифрованных данных в служебные поля сетевых протоколов: создание структуры *Packet*, автоматическое формирование заголовка средствами ядра *Linux*, замена значений полей «Номер последовательности»[5] (сообщение) и «Идентификационный номер»[6] (ключ), пересчет контрольной суммы, передача пакета с помощью *raw* – сокетов; восстановление принятых по сетям связи общего пользования данных из служебных полей сетевых протоколов стека TCP/IP для последующего криптографического преобразования. На рис. 3 показан алгоритм модулей передачи и приема данных на стороне источника и приемника.

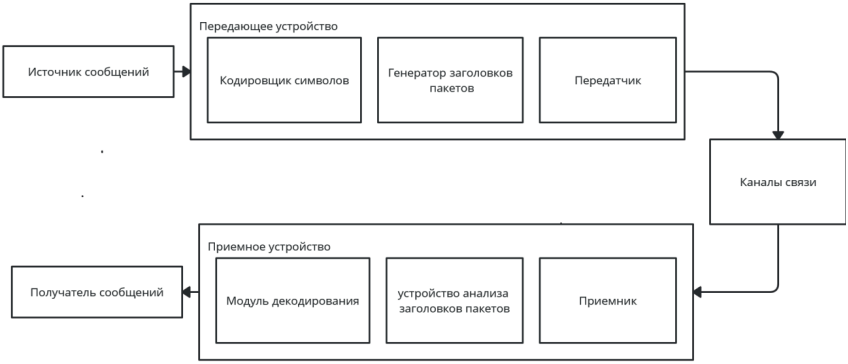


Рис. 3. Алгоритмы модулей передачи и приема данных

Практическая реализация

На стороне отправителя открытый текст разбивается на блоки данных по 5 символов. Каждый символ заменяется на его код из словаря. После этого генерируется ключ, который прибавляется к значениям символов из блока. После этого ключ от зашифрованных данных помещается в поле идентификатора заголовка IP-пакета, а сами данные помещаются в поле номер последовательности SYN TCP пакета. Данные передаются на заранее определенный TCP порт. На рис. 4 представлен поток пакетов данных, пришедших на приемную сторону. Отображение пакетов данных проводилось с помощью программы *Wireshark*.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.101	51.250.31.49	TCP	54	9090 → 9090 [SYN] Seq=0 Win=28944 Len=0
2	0.051085680	51.250.31.49	192.168.0.101	TCP	60	9090 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.051351094	192.168.0.101	51.250.31.49	TCP	54	9090 → 9091 [SYN] Seq=0 Win=28944 Len=0
4	0.119876100	51.250.31.49	192.168.0.101	TCP	60	9091 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.120168722	192.168.0.101	51.250.31.49	TCP	54	9090 → 9092 [SYN] Seq=0 Win=28944 Len=0
6	0.180762759	51.250.31.49	192.168.0.101	TCP	60	9092 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.181054309	192.168.0.101	51.250.31.49	TCP	54	9090 → 9093 [SYN] Seq=0 Win=28944 Len=0
8	0.242439115	51.250.31.49	192.168.0.101	TCP	60	9093 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.242687880	192.168.0.101	51.250.31.49	TCP	54	9090 → 9094 [SYN] Seq=0 Win=28944 Len=0
10	0.314064670	51.250.31.49	192.168.0.101	TCP	60	9094 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.314333718	192.168.0.101	51.250.31.49	TCP	54	9090 → 9095 [SYN] Seq=0 Win=28944 Len=0
12	0.379924142	51.250.31.49	192.168.0.101	TCP	60	9095 → 9090 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Рис. 4. Поток пакетов данных

На рис. 5 и 6 представлен пакет данных, у которого в передаваемых значениях идентификатора заголовка IP-пакета содержится ключ, а сами данные содержатся в поле «Номер последовательности».

```
▾ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 51.250.31.49
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xf46f (62575)
  ▸ Flags: 0x0000
    Fragment offset: 0
```

Рис. 5. Ключ от пакета

```
Transmission Control Protocol, Src Port: 9090, Dst Port: 909
    Source Port: 9090
    Destination Port: 9090
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 3197272163
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
```

Рис. 6. Зашифрованные данные пакета

Заключение

В этой статье были описаны процедура сокрытия данных с использованием полей TCP/IP и основные требования к такому носителю. С помощью нескольких незначительных операций с содержимым поля можно построить скрытый канал для обмена информацией. Серьезной проблемой является фиксированный размер полей, который ограничивает размер сообщений. Поэтому для отправки больших данных, а отправитель должен увеличить количество подключений. Помимо вышеперечисленных методов скрытия передачи можно использовать скрытые каналы связи, что значительно усилит защищенность информации.

Библиографический список

1. Szczypiorski K. Steganography in TCP/IP networks //State of the Art and a Proposal of a New System–HICCUPS, Institute of Telecommunications' seminar, Warsaw University of Technology, Poland. 2003.

2. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия Южного федерального университета. Технические науки. 2012. Т. 137. №. 12 (137). С. 167. 176. Postel, J.: STD7: Transmission control protocol // IETF (1981). 24 с.

3. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection //Soft Computing. 2011. Т. 15. №. 3. С. 505–515.

4. Kadhim J. M., Abed A. E. Steganography using TCP/IP's sequence number // Al – Nahrain Journal of Science. 2017. Т. 20. №. 4. С. 102–108.

5. Kundur D., Ahsan K. Practical Internet steganography: data hiding in IP // Proc. Texas wksp. security of information systems. 2003.

6. Волкогонов В. Н., Гетьман Е. М., Салита А. С. Методы и способы создания стеганографических вложений в сетевых пакетах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). 2021. С. 178–183.

УДК 004.07

П. С. Летуновская*
магистрант
Б. С. Шром*
магистрант
Е. Д. Пойманова*
кандидат технических наук
Т. М. Татарникова*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МАШИННОЕ ОБУЧЕНИЕ В ВОПРОСЕ РАСПРЕДЕЛЕНИЯ ФАЙЛОВ ПО УРОВНЯМ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

В статье предложена архитектура многоуровневой системы хранения данных и рассмотрена возможность применения методов машинного обучения в вопросах распределения файлов по уровням системы хранения данных.
***Ключевые слова*:** системы хранения данных, машинное обучение, распределение.

P. S. Letunovskaya*
Postgraduate Student
B. S. Shrom*
Postgraduate Student
E. D. Poymanova*
PhD, Tech.
T. M. Tatarnikova*
Dr. Sc., Tech, Professor
*St. Petersburg State University of Aerospace Instrumentation

MACHINE LEARNING IN THE DISTRIBUTION OF FILES BY LEVELS OF THE DATA STORAGE SYSTEM

The article proposes the architecture of a multi-level data storage system and the possibility of using machine learning methods in the distribution of files across the levels of the data storage system is considered.
Keywords: storage systems, machine learning, distribution.

Введение

На сегодняшний день Российская Федерация озабочена формированием собственной IT-инфраструктуры. Принимаются меры по поддержке отечественных производителей электроники и программного обеспечения, включая рынок отечественных систем хранения данных. Такие системы имеют в своем составе как программную, так и аппаратную части. Спрос на эти системы создается за счет принятия законов, обязывающих операторов связи использовать

именно отечественную продукцию, при этом отечественный рынок пока не в силах покрыть внутренние потребности [1].

Схема предлагаемой системы хранения данных

Система хранения данных (СХД) – это комплекс программно-аппаратных средств, предназначенный для управления и хранения больших объемов информации.

Предлагается создание многоуровневой системы хранения данных, схема которой приведена на рис. 1 [2].

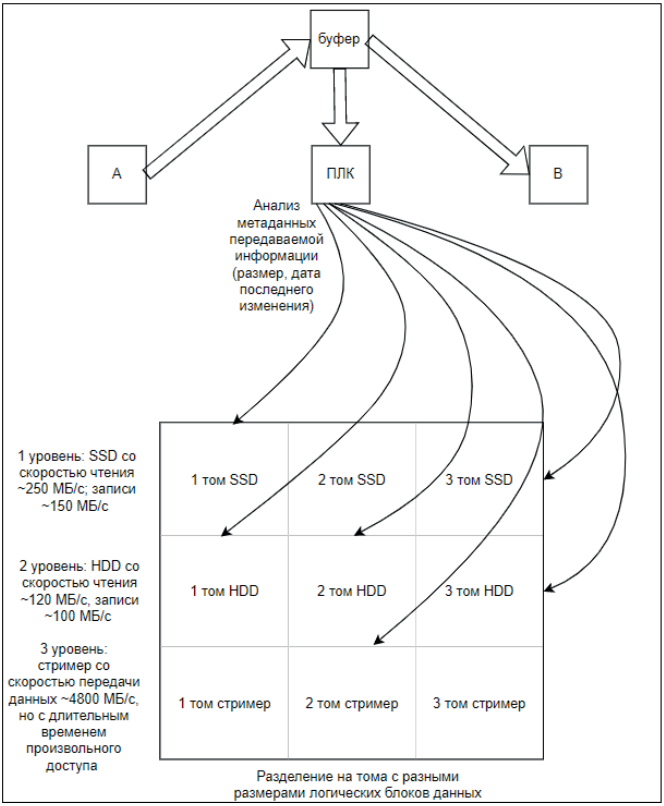


Рис. 1. Многоуровневая система хранения данных

В предлагаемой схеме СХД (рис. 1) предусмотрен механизм распределения данных по уровням и томам при их первоначальной записи в СХД. Предполагается, что при первоначальной записи информации будут собраны метаданные файлов, в зависимости от которых будет приниматься решение о распо-

ложении файлов в СХД. Анализ метаданных предлагается проводить программируемым логическим контроллером (ПЛК).

Возможна ситуация, когда объем трафика в единицу времени будет больше, чем скорость обработки и записи данных в СХД, следовательно, для записи данных без потерь необходим буфер, в который будет поступать необработанная ПЛК информация. Таким образом, весь объем поступающей информации будет сначала записываться в буфер, затем поступать на вход ПЛК для дальнейшего распределения по томам и уровням СХД.

СХД состоит из нескольких уровней запоминающих устройств. На первом уровне располагается запоминающее устройство с наибольшей скоростью чтения/записи, но с наибольшей стоимостью хранения единицы информации, а на последнем – устройство с наименьшей скоростью чтения/записи, но и с наименьшей стоимостью хранения единицы информации.

При этом каждый уровень разбивается на тома с различными размерами логических блоков – секторов, что при определенных условиях должно положительно сказаться на скорости чтения и записи и обеспечить более полное заполнение носителя полезной информацией.

Рассматриваемые метаданные передаваемой информации

Метаданные – структурированные сведения о данных, т. е. информация, использующаяся для описания какого-либо документа или файла.

Каждый файл имеет свои метаданные. Они помогают систематизировать контент, облегчить поиск данных, установить ограничения на распространение информации, указывая на автора.

С помощью метаданных можно определить, когда был создан файл, когда файл последний раз редактировался, его размер, и другие характеристики. Именно эти свойства помогут в принятии решения о записи файла в нужный уровень и том СХД. В табл. 1 приведены примеры для определения нужного для записи уровня СХД.

Таблица 1

Примеры метаданных и распределение файлов по уровням СХД

№ п/п	Метаданные	Пример, сек	Δ, сек	Запись в уровень №
1	Время последнего изменения	1426184823	220 924 809	3
	Текущее время	1647109632		
2	Время последнего изменения	1520849226	126 260 406	2
	Текущее время	1647109632		
3	Время последнего изменения	1615571526	31 538 106	1
	Текущее время	1647109632		

Примечание: используется формат времени *Unix*.

Для определения нужного уровня вычисляется, какое количество времени прошло с момента создания файла до текущего момента времени. Так как воз-

можных уровней всего 3, вся рассматриваемая временная шкала делится на 3 равных отрезка. Соответственно, на третий уровень СХД, состоящего из стримера, будут записываться файлы, которые давно не редактировались, а, следовательно, их можно отнести к архивным файлам. На первый уровень СХД, состоящего из SSD, будут записываться новейшие файлы (оперативные данные). Все остальные, не подходящие по временным рамкам ни под третий, ни под первый уровни, будут записываться на HDD второго уровня.

Для выбора тома определяется остаток от деления размера файла на размер сектора (минимально занятый участок информации для конкретного тома). Том, для которого этот остаток от деления наименьший, будет выбран для записи. Примеры выбора тома приведены в табл. 2.

Таблица 2

Примеры метаданных и распределение файлов по томам СХД

№ п/п	Метаданные	Размер, байт	Остаток от деления	Запись в том №
1	Размер файла	578106	–	3
	Размер сектора тома 1	120	66	
	Размер сектора тома 2	681	618	
	Размер сектора тома 3	300	6	
2	Размер файла	81045	–	2
	Размер сектора тома 1	120	45	
	Размер сектора тома 2	681	6	
	Размер сектора тома 3	300	45	
3	Размер файла	148 080	–	1
	Размер сектора тома 1	120	0	
	Размер сектора тома 2	681	303	
	Размер сектора тома 3	300	180	

Назовем предложенный выше метод определения уровня и тома СХД алгоритмическим. Далее рассмотрим методы машинного обучения.

Методы машинного обучения

Рассмотренный ранее алгоритмический метод прост и легко реализуем. Однако при увеличении количества рассматриваемых параметров (других метаданных) будет затруднительно формализовать алгоритм выбора уровня и тома в СХД. В связи с этим предлагается рассмотреть машинное обучение как метод решения задач такого вида.

Данная задача, по сути, является задачей классификации и применение методов машинного обучения, в частности нейронных сетей, позволит ускорить процесс распределения входящей информации, а также найти ранее неизвестные зависимости от других метаданных [3].

Для описанного ранее алгоритмического метода предлагается разработать нейронную сеть, решающую задачу распределения файлов. Для этого на вход

нейронной сети будут подаваться размеры секторов, а также размер файла и разница между временем создания файла и текущим моментом времени. На выходе такой нейронной сети предполагается получить информацию об уровне и томе.

На сегодняшний момент для запуска нейронных сетей создают специальные тензорные ядра [4] и другие технологии, которые во много раз ускоряют работу нейронной сети, что может положительно сказаться на скорости записи в СХД. Также можно учитывать такие неочевидные параметры, как заполненность различных уровней и томов, пользователь-создатель файла и другие.

Заключение

В настоящей статье предложена модель многоуровневой системы хранения данных, а также механизмы по распределению данных внутри системы с помощью алгоритмических методов и методов машинного обучения.

Библиографический список

1. Федеральный закон от 06.07.2016 г. № 374-ФЗ. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности.

2. Татарникова Т. М., Пойманова Е. Д. Модель многоуровневой организации системы хранения данных // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 2. С. 271–279.

3. Миронов А. М. Машинное обучение: учеб. пособие // Московский государственный университет имени М. В. Ломоносова, Механико-математический факультет, Кафедра математической теории интеллектуальных систем. Ч. 1. М.: МАКС Пресс, 2018.

4. Тензорные ядра NVIDIA H100. https://www.nvidia.com/ru-ru/data-center/tensor-cores/ (дата обращения: 12.03.2022).

УДК 004.056.4

А. А. Овчинников*
кандидат технических наук, доцент
А. М. Вересова*
аспирант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

СРАВНЕНИЕ ВЕРОЯТНОСТИ ОШИБКИ ДЕКОДИРОВАНИЯ КОДОВ РИДА – СОЛОМОНА И НИЗКОПЛОТНОСТНЫХ КОДОВ В КАНАЛЕ ГИЛБЕРТА – ЭЛЛИОТА

В статье рассматривается применение кодов Рида – Соломона и низкоплотностных кодов в канале Гилберта – Эллиота с различными характеристиками. Проводится оценка вероятности ошибки декодирования при различных параметрах канала с использованием имитационного моделирования.
***Ключевые слова*:** декодирование, каналы с памятью, канал Гилберта – Эллиота, низкоплотностные коды, коды Рида – Соломона.

A. A. Ovchinnikov*
PhD, Tech., Associate Professor
A. M. Veresova*
PhD Student
*St. Petersburg State University of Aerospace Instrumentation

COMPARISON OF THE PROBABILITY OF REED – SOLOMON AND LDPC CODES DECODING ERROR IN THE GILBERT – ELLIOTT CHANNEL

The article considers the application of Reed–Solomon codes and low-density parity-check codes in the Gilbert – Elliott channel with different characteristics. The probability of decoding error is estimated for various channel parameters using simulation.
Keywords: decoding, channels with memory, Gilbert – Elliott channel, low-density parity-check codes, Reed – Solomon codes.

В реальных системах передачи информации помехи, как правило, носят неравномерный характер: ошибки группируются при ухудшении условий передачи и возникают редко при хороших условиях. Такие каналы называются каналами с памятью, так как текущее состояние канала зависит от предыдущих. Классическим способом борьбы с помехами в таких каналах является использование кодов Рида – Соломона. Однако в настоящее время наиболее популярны низкоплотностные коды, которые, благодаря своей псевдослучайной природе, обладают высоким потенциалом при использовании в каналах с памятью, но их применение для исправления группирующихся ошибок малоисследовано.

Для анализа каналов с памятью удобно использовать модель канала с конечным числом состояний. Наиболее распространенный случай – канал с двумя состояниями, плохим (*bad*, *B*) и хорошим (*good*, *G*), описываемый марковской

цепью, изображенной на рис. 1. Плохое состояние характеризуется высокой вероятностью возникновения помех (обозначим ее p_B), а хорошее – низкой (p_G). В зависимости от вероятностей ошибок можно выделить несколько частных случаев, описываемых данной моделью:

– Марковский канал: $p_G = 0,\ p_G = 1$;
– Канал Гилберта: $p_G = 0,\ p_B = 0{,}5$;
– Канал Гилберта – Эллиота: $0 \le p_G \ll p_B \le 1$.

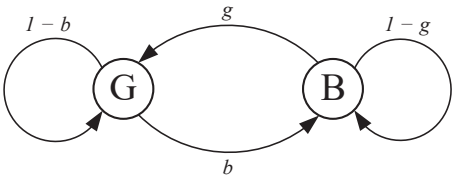


Рис. 1. Модель канала с двумя состояниями

Таким образом, модель Гилберта – Эллиота описывает общий случай канала с двумя состояниями. Для того, чтобы канал обладал памятью, необходимо задать переходные вероятности b и g, обеспечивающие зависимость текущего состояния от предыдущего. В частности, считается, что канал обладает памятью, если $b + g \ne 1$ [1]. Как правило, рассматриваются ситуации, когда $g > b$, т. е. канал чаще находится в хорошем состоянии.

Традиционно при исправлении пакетов ошибок используется процедура интерливинга, которая позволяет распределять ошибки равномерно во времени, и применять классические процедуры декодирования. Однако из теории кодирования известно, что учет памяти канала позволяет повысить достижимую скорость передачи [2; 3]. Таким образом, исследование алгоритмов для надежной передачи информации в соответствующих каналах, а в частности – алгоритмов декодирования пакетов ошибок, является актуальной задачей.

Для учета памяти канала могут быть использованы специальные коды, например, коды Рида – Соломона (*Reed – Solomon*, RS) [4]. RS-код является недвоичным кодом, значения кодовых символов которого принадлежат полю GF(2^m), т. е. (n, k, d) RS-код является кодом длиной $n = 2^m - 1$ с минимальным расстоянием $d = n - k + 1$, что является максимально достижимым расстоянием кода. Такой код может исправлять $t = \lfloor d/2 \rfloor = \lfloor (n-k+1)/2 \rfloor$ независимых ошибок. Но если каждому двоичному вектору длиной m поставить в соответствие элемент поля GF(2^m), то код Рида – Соломона может быть представлен в виде двоичного кода длиной $n' = m \cdot (2^m - 1)$. Такое отображение RS-кода позволяет исправлять многократные пакеты ошибок: например, будет исправлен любой одиночный пакет длиной до $m \cdot (t-1) + 1$, так как он покрывается не более, чем t блоками – символами GF(2^m).

Также для передачи по каналам с памятью зачастую используются коды с малой плотностью проверок на четность (*low-density parity-check*, LDPC) [5; 6]. Благодаря разреженной структуре проверочной матрицы, такие коды нечувствительны к образованию пакетов ошибок. Наиболее распространенный подход к построению LDPC-кодов заключается в использовании блочно-перестановочной конструкции проверочной матрицы. Блоки в такой конструкции представляют собой циркулянты – циклические перестановки единичной матрицы. При использовании такой структуры вес столбцов и строк матрицы (γ и ρ соответственно) постоянен, т. е. код является регулярным. Тогда при использовании блока размером $m \times m$ код будет иметь длину $n = \rho m$ и размерность $k = \gamma m$.

Для декодирования низкоплотностных кодов используются итеративные посимвольные декодеры, которые описываются в терминах пересылки сообщений по ребрам графа Таннера. Классическим методом декодирования считается алгоритм распространения доверия (*Belief-Propagation*, *BP*), критерием оптимальности которого является максимум апостериорной вероятности. Данный алгоритм разработан для исправления независимых ошибок. Как было замечено, разреженная структура кода позволяет использовать классические алгоритмы при исправлении пакетных ошибок, однако это малоэффективно.

В работе [7] было предложено при декодировании LDPC-кодов в канале Гилберта – Эллиота использовать подход с пересылкой сообщений для оценки состояний канала путем построения объединенного графа канала и низкоплотностного кода – графа GE-LDPC. В работе [8] предложен алгоритм для декодирования одиночных пакетов ошибок, однако он не исправляет множественные пакеты и ошибки за пределами пакета.

Для проведения экспериментов рассмотрим случайный блочно-перестановочный LDPC-код с параметрами $\gamma = 4$, $\rho = 8$ и размером блока $m = 127$. Длина такого кода $n = 8 \cdot 127 = 1016$, скорость $R = k / n = 1 / 2$. Для его декодирования будем использовать классический алгоритм распространения доверия и алгоритм с оценкой состояний канала, описанный в [7]. Также рассмотрим (127, 63, 7) код Рида – Соломона, т. е. код длиной $n = 127$ с элементами из поля $GF(2^7)$. Количество исправляемых ошибок для данного кода $t = 32$. В двоичном представлении этот код имеет длину $n' = 889$ и способен исправить все ошибки или пакеты ошибок в пределах 32 блоков, соответствующих символам поля.

Рассмотрим канал Гилберта – Эллиота с фиксированными параметрами $b = 0{,}001$, $g = 0{,}1$ и $p_B = 0{,}5$. При таких параметрах на длине кодового слова $n = 1000$ возникает в среднем один пакет ошибок длиной 10: время нахождения в плохом состоянии является случайной величиной с геометрическим распределением и математическим ожиданием $1 / g = 10$. На рис. 2 представлен график зависимости вероятности ошибки декодирования от вероятности ошибки в хорошем состоянии для различных декодеров.

При $p_G = 0$ ошибок в хорошем состоянии не происходит, т. е. канал соответствует каналу Гилберта. В таком канале наилучшая вероятность ошибки обеспечивается при использовании кода Рида – Соломона: он исправляет все

возникающие ошибки. Следующий по количеству исправленных ошибок в канале Гилберта – алгоритм BP для LDPC-кода. С увеличением вероятности ошибки в хорошем состоянии все кривые стремятся к вероятности ошибки при некодированной передаче, однако в интервале $p_G \in [0{,}02; 0{,}08]$ декодер GE-BP с оценкой состояний показывает заметно меньшую вероятность ошибки. Остальные декодеры уже при значении $p_G = 0{,}05$ оказываются неспособными восстановить кодовое слово.

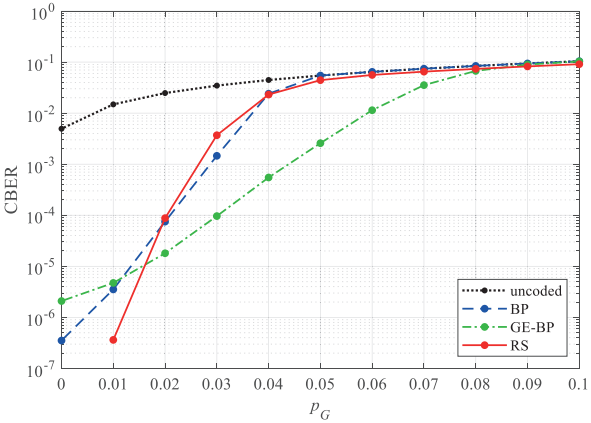


Рис. 2. Вероятность ошибки на бит кодового слова при b = 0,001 и g = 0,1

На рис. 3 приведены аналогичные результаты для канала с $g = 0{,}05$, т. е. с более длинными пакетами ошибок.

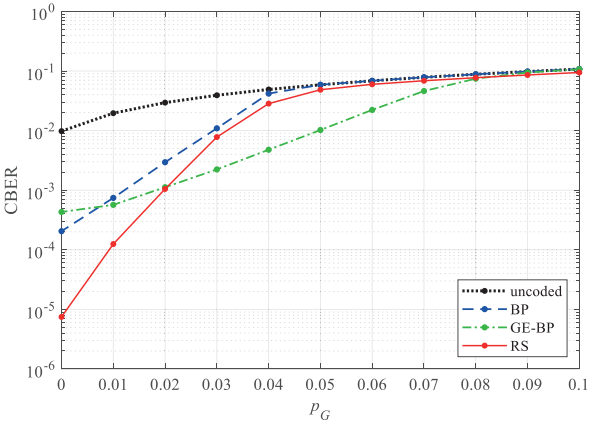


Рис. 3. Вероятность ошибки на бит кодового слова при b = 0,001 и g = 0,05

Таким образом, использование кодов Рида – Соломона обеспечивает наименьшую вероятность ошибки для рассмотренных параметров канала Гилберта, однако для канала Гилберта – Эллиота, где возможны ошибки в хорошем состоянии, более высокую эффективность показывает алгоритм GE-BP для LDPC-кодов, включающий оценку состояний канала. Классический алгоритм распространения доверия показывает низкую эффективность в рассмотренных случаях.

Библиографический список

1. Mushkin M. Capacity and coding for the gilbert-elliott channels / M. Mushkin, I. Bar-David // IEEE Transactions on Information Theory. 1989. Vol. 35. № 6. P. 1277–1290.

2. Кудряшов Б. Д. Теория информации: учебник для вузов. СПб.: Питер, 2009. 320 с.

3. Wolfowitz J. Memory Increases Capacity // Information and Control. 1967. Vol. 11. № 4. P. 423–428.

4. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М: Техносфера, 2005. 320 с.

5. Gallager R. G. Low Density Parity Check Codes. Cambridge, MA: MIT Press, 1963. 90 p.

6. Ryan,W. E. Channel Codes: Classical and Modern / W. E. Ryan, S. Lin. New York: Cambridge University Press, 2009. 710 p.

7. Eckford A. W. Analysis of Low-Density Parity-Check Codes for the Gilbert–Elliott Channel / A. W. Eckford, F. R. Kschischang, S. Pasupathy // IEEE Transactions on Information Theory. 2005. Vol. 51. № 11. P. 3872–3889.

8. Veresova A. M. About One Algorithm For Correcting Bursts Using Block-Permutation LDPC-Codes / A. M. Veresova, A. A. Ovchinnikov // 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). St. Petersburg, Russia, 2019. P. 1–4.

УДК 629.735.33

А. А. Овчинников*
кандидат технических наук, доцент
А. А. Фоминых*
магистрант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ДВУХСТУПЕНЧАТОЕ ДЕКОДИРОВАНИЕ НА ОСНОВЕ ИТЕРАТИВНОГО И СФЕРИЧЕСКОГО ПОДХОДОВ

Рассмотрены подходы к многоступенчатому декодированию линейных кодов. Предложен гибридный алгоритм декодирования, в котором реализован подход к комбинированию различных алгоритмов декодирования для использования одной и той же избыточности кода. Основное внимание уделено оценке возможности использования такого декодера для декодирования кода БЧХ в канале с АБГШ.
***Ключевые слова*:** многоступенчатое декодирование, декодирование в сфере

A. A. Ovchinnikov*
PhD, Tech., Associate Professor
A. A. Fominykh*
Postgraduate Student
*St. Petersburg State University of Aerospace Instrumentation

A TWO-STAGE DECODING BASED ON ITERATIVE BOUNDED DISTANCE APPROACH

The paper considers approaches to multistage decoding of linear codes. Proposed hybrid decoding algorithm implements an approach to combine different decoding algorithms to use the same code redundancy. The main attention is paid to evaluating the possibility of using such a decoder for decoding a BCH code in an AWGN channel.
Keywords: two-stage decoding, bounded decoding.

Введение

В современном мире информация представляет собой один из важнейших ресурсов. При передаче, хранении и обработке информации могут возникать ошибки, для исправления которых теория помехоустойчивого кодирования предлагает использовать методы кодирования, вносящие избыточность, которая используется алгоритмом декодирования для исправления ошибок. Важными параметрами при декодировании являются сложность декодирования и обеспечиваемая корректирующая способность. Эти параметры находятся в противоречии, но существуют схемы кодирования и декодирования, которые позволяют обеспечить компромисс. В данной работе рассматривается двухступенчатый подход к декодированию, позволяющий уменьшать число ошибок за счет незначительного увеличения сложности схемы.

Двухступенчатый алгоритм декодирования

Среди алгоритмов декодирования можно выделить два основных класса: декодеры с ограниченным расстоянием (*bounded distance decoding*) и итеративные посимвольные декодеры [1]. Декодеры с ограниченным расстоянием позволяют исправлять любую комбинацию ошибок кратности до t, где t определяется минимальным расстоянием d или конструктивным расстоянием. Итеративные посимвольные декодеры принимают решение не о кодовом слове в целом, а по каждому символу в отдельности, что позволяет в случае большого числа ошибок в канале достигать меньшей вероятности ошибки на бит, даже есть решение о кодовом слове в целом было неверным [2].

При рассмотрении не отдельных алгоритмов декодирования, а их комбинации, можно сформулировать подход, в котором на приемной стороне одна и та же избыточность используется несколькими декодерами. Примерами такой схемы передачи является, например, случайный линейный код, который сначала декодируется итеративным посимвольным декодером, а затем алгоритмом декодирования по информационным совокупностям [3]. В данном случае рассматривается сочетание итеративного посимвольного декодирования и декодирования в сфере. Вторым примером является декодирование кодов с малой плотностью проверок на четность [4]: для кодирования используется код с малой плотностью проверок на четность, декодирования осуществляется сначала итеративным посимвольным декодером, а затем алгоритмов мажоритарного декодирования. Мажоритарные декодеры также являются итеративными посимвольными, но позволяют гарантировать исправление фиксированного числа ошибок равного $\gamma/2$, где γ – вес столбца проверочной матрицы [5]. Третьим примером является кодирование с помощью циклического кода и последовательное декодирование с помощью итеративного посимвольного декодера и алгебраического декодера.

Гибридное декодирование БЧХ кодов

Циклические коды представляют собой подкласс линейных кодов, для которого циклический сдвиг любого кодового слова также является кодовым словом. Основополагающим примером циклических кодов являются коды Боуза-Чоудхури-Хоквингема (БЧХ) [6].

Рис. 1. Гибридная схема декодирования

Для БЧХ кодов известны эффективные алгебраические процедуры декодирования, такие как алгоритм Евклида, алгоритм Берлекэмпа-Месси [1], га-

рантирующие исправления числа ошибок вплоть до конструктивного расстояния, и способные сигнализировать о превышении числа ошибок отказом от декодирования. Наиболее известными итеративным посимвольными алгоритмами декодирования являются: алгоритм распространения доверия (*belief propagation*, BP) и алгоритм инвертирования битов (*bit flipping*, BF). В работе предлагается схема декодирования, представленная на рис. 1.

Результаты моделирования

В экспериментах будет использовано два БЧХ кода с параметрами $n = 31$, $k = 15$, $t = 3$ и $n = 63$, $k = 33$, $t = 6$. Моделируется передача 100000 слов. Для построения матрицы БЧХ более подходящей для итеративного декодирования использовалась следующая процедура: (1) строится начальный код БЧХ для заданных параметров (n, k), (2) выписываются слова дуального кода, (3) из слов меньшего веса строятся N матриц, для каждой из которых вычисляется число циклов длины 4. При построении получены матрицы с различным числом циклов длины 4, указанным в табл. 1.

Таблица 1

Количество циклов длины 4 в построенных матрицах кода БЧХ

Код	Количество циклов длины 4							
(31, 15)	386	402	470	474	558	563	576	658
(63, 33)	1527	2511	3367	3113	3470	3588	3419	3722

Рассмотрим применение нескольких схем декодирования в канале с АБГШ для кодов, описанных по вышеуказанной процедуре. Результаты декодирования алгоритмом распространения доверия с 5 итерациями для матриц БЧХ кодов с параметрами (31, 15) и (63, 33) с разным числом циклов, построение которых было описано выше. На рисунках также приведена кривая некодированной передачи (*Uncoded*). Вероятность ошибки оценивается на кодовое слово (*codeword error rate*, CER). По рис. 2, *а* и 2, *б* можно заметить аналогичное поведение для двух рассматриваемых параметров кодов, что вероятность ошибки для матриц, имеющих меньше циклов оказывается меньше, что подтверждает чувствительность итеративных алгоритмов декодирования к количеству циклов.

Далее введем в рассмотрение четыре схемы декодирования, которые будут промоделированы для матриц с наименьшим числом циклов. Будут рассмотрены следующие схемы декодирования: (1) Алгебраический декодер (*Hard*); (2) Алгоритм распространения доверия (*Soft*); (3) Комбинация алгоритма распространения доверия с алгебраическим декодером (*Soft* + *Hard*); (4) Двухэтапная схема декодирования, с включением последовательной схемы алгоритма распространения доверия в связке с алгебраическим декодером, если первый алгебраический декодер сигнализировал об отказе от декодирования (*Hard* + *Soft* + *Hard*).

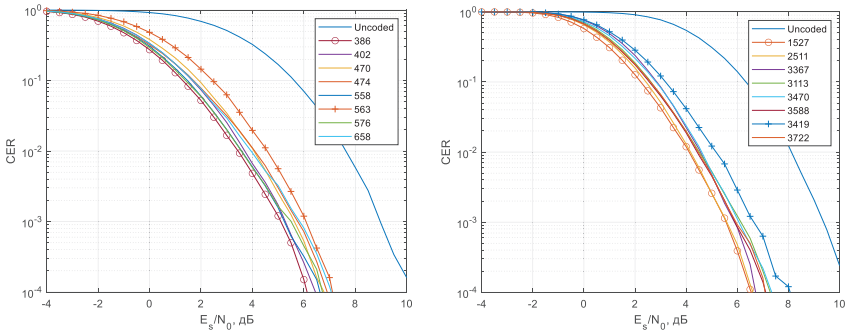


Рис. 2. Вероятность ошибки для матриц (31, 15) (а, слева) и (63, 33) (б, справа) БЧХ кодов с разным числом циклов

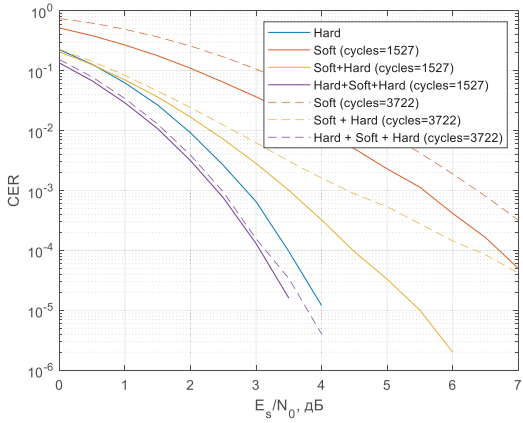


Рис. 3. Сравнение вероятности ошибки для разных схем декодирования

Результаты моделирования четырех схем декодирования для БЧХ кода с параметрами (63, 33) с наименьшим и наибольшим числом циклов, для алгоритма распространения доверия используется 10 итераций (рис. 3). По результатам моделирования заметно, что вероятность ошибки итеративного алгоритма неудовлетворительная, из-за плотности матриц, однако использование комбинации из итеративного декодера и алгебраического декодера позволяет значительно уменьшить вероятность ошибки. В случае гибридного декодирования с предварительным включением алгебраического декодера, схема показывает небольшой выигрыш по сравнению с одним алгебраическим декодером.

Заключение

В работе предложен гибридный алгоритм декодирования, в котором реализован подход к комбинированию различных алгоритмов декодирования для использования одной и той же избыточности кода. Основное внимание уделено оценке возможности использования такого декодера для кода БЧХ в канале с АБГШ. Показано, что целесообразность такой схемы имеется только в случае, когда алгебраический декодер сигнализировал об отказе от декодирования. С одной стороны это позволяет понизить вероятность ошибки, с другой стороны первый алгебраический декодер используется как индикатор необходимости включения второй связки декодеров.

Библиографический список

1. MacWilliams F. J., Sloane N. J. A. The theory of error correcting codes. Elsevier, T. 16, 1977.

2. Ryan W., Lin S. Channel codes: classical and modern. Cambridge university press, 2009.

3. Фоминых А. А., Овчинников А. А. Обзор алгоритмов декодирования линейных блоковых кодов на основе информационных совокупностей // Обработка, передача и защита информации в компьютерных системах: Первая Всероссийская научная конференция, Санкт-Петербург, 14–22 апреля 2020 года. Санкт-Петербург: СПб. ГУАП, 2020. С. 220–223.

4. Gallager R. G. Low-density parity-check codes // IRE Transactions on Information Theory, Vol. 8. No. 1. 1962. С. 21–28.

5. Massey J. L. Threshold decoding. Cambridge, MA: MIT Press. 1963.

6. Hocquenghem A. Codes correcteurs d'erreurs. Chiffers, 1959. Т. 2. С. 147–156.

УДК 004.891

Е. В. Пастухова*
кандидат технических наук, доцент
Ю. С. Романова*
кандидат технических наук, доцент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ИССЛЕДОВАНИЯ В ЭПОХУ BIG DATA

В статье обсуждается использование искусственного интеллекта (ИИ) для принятия решений в целом и конкретные вопросы, касающиеся взаимодействия и интеграции методов ИИ для поддержки или замены лиц, принимающих решения. Для продвижения исследований по использованию ИИ для принятия решений в эпоху больших данных авторами предлагаются перспективные направления для исследователей ИИ с точки зрения концептуальной и теоретической разработки, взаимодействия технологии ИИ с человеком и внедрения ИИ.
***Ключевые слова*:** искусственный интеллект, принятие решений, *Big Data*, экспертные системы, машинное обучение.

E. V. Pastukhova*
PhD, Tech., Associate Professor
Y. S. Romanova*
PhD, Tech., Associate Professor
*St. Petersburg State University of Aerospace Instrumentation

ARTIFICIAL INTELLIGENCE: RESEARCHES IN THE OF AGE OF BIG DATA

The article discusses the use of artificial intelligence (AI) for decision making in general and specific issues regarding the interoperability and integration of AI methods to support or replace decision makers. To advance research on the use of AI for decision making in the era of big data, the authors propose promising directions for AI researchers in terms of conceptual and theoretical development, the interaction of AI technology with humans, and the implementation of AI.
***Keywords*:** Artificial Intelligence, making decisions, Big Data, Expert Systems, Machine Learning.

Введение

Рост искусственного интеллекта в последние годы вызвал многочисленные противоречивые замечания. Например, генеральный директор IBM (2012-2020) Джинни Рометти утверждала, что технологии ИИ являются «технологиями для усиления человеческого интеллекта... По большому счету, мы видим мир партнерства между человеком и машиной, и это фактически делает нас лучше» [1].

Стивен Хокинг, с другой стороны, заметил, что «развитие полного искусственного интеллекта может означать конец человеческой расы» [2], а Билл Гейтс также заявил, что люди должны беспокоиться об угрозе, которую представляет искусственный интеллект [3].

Эти очень разные мнения ведущих экспертов требуют дальнейшего изучения того, как люди могут сосуществовать с ИИ, как минимизировать негативное влияние и использовать преимущества данных технологий.

Общепринятого определения ИИ не существует. Обычно ИИ называется способностью машины учиться на опыте, подстраиваться под новые вводы и выполнять задачи, похожие на задачи человека.

Искусственные нейронные сети, предназначенные для имитации работы человеческого мозга, находятся на переднем крае развития ИИ несмотря на то, что упоминания об их приложениях можно найти даже в 1980-х гг. [4]. Благодаря быстрому развитию технологий *Big Data*, обеспечивающих улучшенные возможности хранения и сверхбыструю скорость обработки данных, новые системы ИИ повысили способность общества использовать данные для составления прогнозов и значительно снизили стоимость их составления. По мнению [5], возможность использовать ИИ для совершенствования процесса принятия решений, создания новых бизнес-моделей и экосистем, а также изменения эффективности взаимодействия с клиентами, может привести к окупаемости инвестиций в цифровые инициативы уже до 2025 г.

Экспертные системы для принятия бизнес-решений

Цель данного исследования – обозначить проблемы, связанные с использованием и влиянием нового поколения систем на основе ИИ для принятия решений, и определить возможности развития для исследователей информационных систем (ИС).

Использование ИИ для принятия решений было одним из наиболее важных приложений в богатой истории ИИ. В широком смысле системы ИИ могут использоваться либо для поддержки/помощи лицам, принимающим решения, либо для их замены.

Авторами [6] был проведен анализ экспертных систем для принятия бизнес-решений на различных уровнях и в различных ролях на основе экспериментов, состоявшихся два десятилетия назад. Роль ИИ (например, экспертных систем) рассматривается с использованием трех организационных уровней принятия решений, т. е. стратегических, тактических и оперативных решений. Их результаты показывают, что:

– экспертные системы, выполняющие роль замены, эффективны на оперативном и тактическом уровнях принятия решений, но имеют ограничения на стратегическом уровне;

– экспертные системы в роли поддержки могут помочь пользователям принимать более эффективные решения на всех трех уровнях принятия решений, но их эффективность может быть достигнута только через их пользователей;

– экспертная система, выполняющая роль поддержки, не обязательно экономит время пользователя, но экспертная система, выполняющая роль замены, повышает эффективность принятия решений;

– пользователи экспертных систем, выполняющие функции поддержки, не считали, что они извлекли уроки из использования системы.

В совместном исследовании с *Deloitte* компания *Davenport* [7] рассмотрела 152 проекта внедрения ИИ, в которых используются системы на основе ИИ для широкого спектра бизнес-функций и процессов. Основываясь на результатах опроса, *Davenport* распределяет системные приложения ИИ по трем категориям:

– когнитивная автоматизация процессов: автоматизация административной и финансовой деятельности бэк-офиса с использованием «роботизированной автоматизации процессов»;

– когнитивные знания: обнаружение закономерностей в данных и интерпретация их значения с помощью алгоритмов машинного обучения, основанных на статистике;

– когнитивная вовлеченность: привлечение сотрудников и/или клиентов с помощью чат-ботов обработки естественного языка, интеллектуальных агентов и машинного обучения.

Поскольку прогресс технологии ИИ позволяет исследователям создавать передовые машины, ИИ может также выполнять более сложные задачи, которые требуют когнитивных возможностей, таких как рассуждения, ощущение эмоций и процессы вождения, которые ранее казались невозможными. В результате все большее число рабочих операций автономно выполняется системами ИИ без человеческого контроля и надзора. Существует много публикаций о преимуществах ИИ для принятия решений, потому что считается, что ИИ способен помочь человеку в принятии лучших решений, повысить его аналитические и директивные способности, а также креативность [8]. Однако с развитием ИИ появляется симбиоз человек-машина, и возникает вопрос о том, как люди и новый искусственный интеллект могут дополнять друг друга для принятия прорывных решений.

Синергия систем искусственного интеллекта и человека

Мы рассмотрим проблемы и возможности исследований систем на основе ИИ для принятия решений в эпоху больших данных с точки зрения использования и взаимодействия. Поскольку разработка и применение ИИ охватывают широкий спектр областей, будущие направления исследований могут быть разнообразными. Чтобы помочь исследователям ИС в их стремлении расширить свои знания и понимание того, как максимально использовать преимущества систем ИИ нового поколения для принятия решений, предлагаются несколько направлений исследований, основанные на трех областях: концептуальная и теоретическая разработка, взаимодействие технологии ИИ с человеком и внедрение ИИ:

– так как ИИ применяется во многих областях и для описания систем на его основе для принятия решений используются различные термины, такие как: экспертные системы, системы на основе знаний, системы поддержки интеллектуальных решений, системы интеллектуальных программных агентов, интеллектуальные исполнительные системы и т. д., то необходимо и полезно пересмотреть концепцию ИИ и связанные с ней термины, чтобы отразить изменяющийся характер разработки и применения ИИ в эпоху больших данных;

– необходимо разработать и проверить теоретически обоснованные и практически осуществимые показатели воздействия ИИ для оценки его выгод в краткосрочной и долгосрочной перспективе с социальной, экономической и политической точек зрения;

– в области оценки степени взаимодействия технологии ИИ и человека с учетом того, что современные системы ИИ работают по принципу «черного ящика», не умея объяснить пользователю почему решения принимаются определенным образом, было бы разумно использовать ИИ в качестве инструмента поддержки/дополнения решений, а не в качестве автоматизации принятия решений вместо лиц, принимающих решения;

– на использование и успех ИИ значительно влияют личные черты пользователей ИИ, их знание и понимание технологий, поэтому актуально проводить регулярное ознакомление ЛПР с принципами работы новых систем;

– эргономичный дизайн систем ИИ важен для их успеха, но критерии их проектирования должны различаться между поддержкой, дополнением, заменой или автоматизацией систем с точки зрения взаимодействия технологии и ЛПР;

– производительность систем ИИ для принятия решений может быть улучшена путем их глубокого обучения с увеличением доступности больших данных с их объемом, разнообразием и скоростью. Поэтому необходимы дополнительные исследования для установления уникальных преимуществ, возникающих благодаря сочетанию этих технологий для полного понимания синергии ИИ и БД и ее последствий для использования ИИ;

– широкое использование ИИ для поддержки и автоматизации принятия решений человеком может привести к изменению культуры в обществе и в индивидуальном поведении, в то время как на развитие ИИ для принятия решений могут также оказывать влияние различные национальные особенности и личные ценности человека.

Заключение

Поскольку ИИ стал более популярным сегодня именно благодаря большим данным, усовершенствованным алгоритмам, улучшенным вычислительным мощностям и системам хранения данных, то системы ИИ становятся встроенным элементом цифровых систем и, в частности, оказывают глубокое влияние на принятие решений человеком. В результате возрастает спрос на исследователей информационных систем для изучения и понимания последствий этого влияния и содействия теоретическому прогрессу и практическому успеху приложений ИИ. Данная статья призвана удовлетворить эту потребность путем анализа и выделения важнейших проблем и возможностей для исследователей ИГ.

Библиографический список

1. Zakaria F. A Conversation with Ginny Rometti. URL: https://www.youtube.com/watch?v=mNEQsl1-iZs (дата обращения: 03.04.2022).

2. Cellan-Jones R. Stephen Hawking warns artificial intelligence could end mankind. URL: https://www.bbc.co.uk/news/technology-30290540 (дата обращения: 03.04.2022).

3. Rawlinson K. Microsoft's Bill Gates insists AI is a threat. URL: https://www.bbc.co.uk/news/31047780 (дата обращения: 03.04.2022).

4. Ford N. From Information-Management to Knowledge-Management – the Role of Rule Induction and Neural Net Machine Learning Techniques in Knowledge Generation // Journal of Information Science. 1989. № 15 (4–5), P. 299–304.

5. Panetta K. Gartner Top 10 Strategic Technology Trends for 2018/ URL: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/ (дата обращения: 03.04.2022).

6. Edwards J. S., Duan Y., Robins P. An analysis of expert systems for business decision making at different levels and in different roles // European Journal of Information Systems. 2000, № 9 (1), P. 36–46.

7. Davenport T. H., Ronanki R. Artificial Intelligence for the real world // Harvard Business Review. 2018. № 96 (1). P. 108–116.

8. Wilson J., Daugherty P. R. Humans and AI are joining forces // Harvard Business Review.2018. № 96 (4). P. 115–123.

УДК 004.67

И. Д. Попов*
ассистент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

О ПРИМЕНЕНИИ МЕТОДА НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ В MATLAB ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ НАБОРА ДАННЫХ KYOTO 2006

Рассмотрено использование FCM-метода для обнаружения вредоносного трафика. Рассмотрена нечеткая кластеризация данных готового набора *Kyoto* 2006. Приведена эффективность FCM-метода для этого набора данных.
Ключевые слова: система обнаружения сетевых атак, набор данных *Kyoto* 2006, метод нечеткой кластеризации, FCM, *Matlab*.

I. D. Popov*
Assistant
*St. Petersburg State University of Aerospace Instrumentation

ABOUT APPLYING THE FUZZY CLUSTERING METHOD IN MATLAB TO DETECT MALICIOUS TRAFFIC USING THE KYOTO 2006 DATASET

The use of the FCM method for detecting malicious traffic is considered. The fuzzy clustering of data from the ready-made Kyoto 2006 dataset is considered. The efficiency of the FCM method for this dataset is given.
Keywords: IDS, Kyoto 2006 dataset, fuzzy clustering, FCM, Matlab.

Введение

В области обнаружения сетевых атак одним из актуальных вопросов является классификация сетевого трафика. Одним из простых и популярных методов классификации является метод *k*-средних (kNN), который позволяет присвоить объекту один из классов на основе метрики (чаще используется евклидово расстояние). Данный метод не позволяет показать точность принадлежности объекта к тому или иному классу, но данную задачу может выполнить метод нечеткой кластеризации (FCM) [1].

В задачах классификации требуется большая выборка данных, примеры которых приведены в [2–3], и одна из них – *Kyoto* 2006 – использована в данной статье.

Подготовка данных Kyoto 2006 для обработки в Matlab

Исходный набор данных *Kyoto* 2006 содержит 24 признака для каждой записи. Их перечень и описание приведены в [4]. Из данных удалены: столбцы IPv6-адресов, так как авторами набора отмечено, что оригинальные адреса подменены; столбцы, которые отражают реакцию сторонних IDS на сетевой трафик, так как они не являются данными сетевого трафика.

Часть из оставшихся данных представлены не в числовом формате. В методах кластеризации могут использоваться вычисления расстояний, а символьные признаки не позволяют подставить значение в формулы FCM-метода [5]. Для того, чтобы записи данного набора можно было подать на вход существующего алгоритма, работающего с числами, написан скрипт на языке *python* [6], который преобразует все символьные признаки в числа.

Нечеткая кластеризация данных из набора Kyoto 2006

В рассматриваемом наборе данных *Kyoto* 2006 авторами выделено 3 возможные метки для записи: «была известная атака», «была неизвестная атака» и «атаки не было». Для удобства и простоты типы «была известная атака» и «была неизвестная атака» объединены в один тип – «атака была».

Имея 2 типа трафика, необходимо получить 2 кластера – области, в которых будут находится наиболее похожие объекты. В данном случае в одном кластере будут объекты, классифицированные как атака, а в другом – обычный трафик. Из-за того, что данные многомерны (18 признаков, следовательно, 18-мерное пространство; необходимо учесть, что часть признаков было удалено из набора данных), то визуализировать на одном графике не получится. Можно сделать попарные (каждый с каждым признаков) двумерные проекции.

На рис. 1 показан пример проекций по 6 признаку с каждым другим признаком. Красным цветом отмечен кластер – трафик с атакой, а синий – обычный трафик. Крестиками отмечены центры кластеров. По оси X отмечены нормализованные значения 6 признака, а по оси Y – нормализованные значения признака i (номер признака указан над каждым графиком).

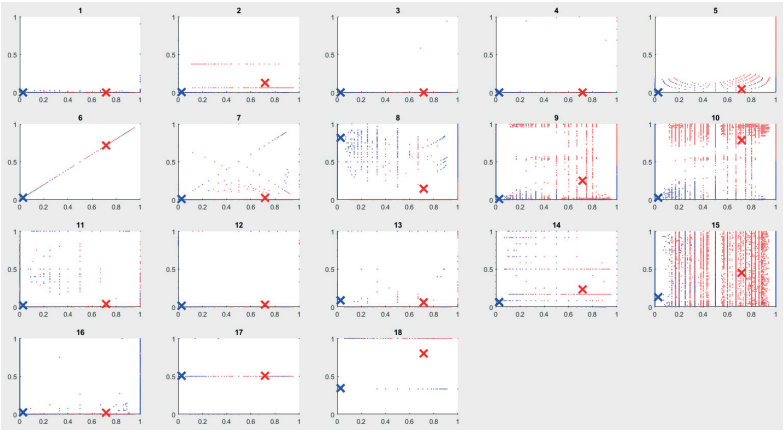


Рис. 1. Все проекции многомерной кластеризации по 6 признаку из набора

На некоторых проекциях отчетливо видно разделение на 2 кластера, но таких проекций немного. Далее приведены наиболее «удачные» разделения на кластеры для признака 8 (рис. 2).

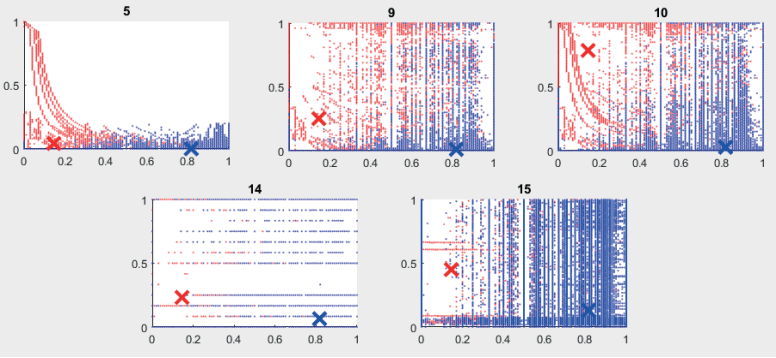


Рис. 2. Некоторые проекции по 8 признаку

Оценка точности нечеткой кластеризации данных из набора Kyoto 2006

Для эксперимента были выбраны все данные одного месяца каждого года, для которых имеются данные. Стоит отметить, что данные собраны по месяцам, так как объединить их в один файл проанализировать за одну итерацию не получается из-за большого объема данных и необходимости большого количества оперативной памяти. Так, для 4,5 Гб исходных данных (а именно столько занимают исходные данные суммарно за ноябрь всех годов), 16 Гб оперативной памяти – мало. Экспериментально было выявлено, что при 16 Гб оперативной памяти можно подать на вход файл размером 1,5–2 Гб.

Таблица 1

Результаты первого эксперимента

Характеристика	Год									
	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Количество записей в выборке, млн	2,66	2,7	2,43	6,79	12,3	7,3	4	10,3	11,1	9,6
Доля записей, помеченных авторами набора как атака, %	11,3	57,6	56,2	29	14,9	11,2	16,6	1,1	12,3	6,3
Accuracy, %	52	66,5	69	49	83,6	75,1	50	56,6	55,6	68,1
Precision, %	12,6	72,6	73,7	17,8	47,4	17,2	5,3	0,1	17,4	15,3
Recall, %	54,8	67,1	69,7	32,2	91,4	59,3	11,8	3,5	69,3	89,3
Средняя «уверенность» FCM-метода в атаке и ее отсутствии (верная и неверная классификация), %	68,9 73,4	79,6 68	78,7 68	74,6 82	73,2 85,8	78,8 89,3	89,1 73,6	73 70,1	81 74	69,4 77,9

FCM-метод – метод итеративный. По умолчанию *Matlab* ограничено количество итерации значением 100, но его можно изменить. Можно отметить, что в проведенных экспериментах этого количества итераций достаточно.

В табл. 1 представлены результаты нечеткой кластеризации записей за ноябрь каждого года (месяц ноябрь выбран случайным образом).

Из имеющихся в таблице характеристик стоит отметить среднюю уверенность в атаке и среднюю уверенность в отсутствии атаки. Данные характеристики показывают, насколько «уверен» алгоритм в том, как он классифицирует объект. Данная характеристика учитывает «уверенность» верных и неверных ответов.

Наилучшие показатели получились в результате анализа данных за 2010 год.

Во втором эксперименте были объединены файлы с данными за те годы, которые показали наилучшие результаты: 2007, 2008 и 2010. После чего был запущен тот же алгоритм и получены следующие результаты (табл. 2). В результате увеличения выборки наилучших результатов в предыдущем эксперименте получилось, что в основном показатели точности классификации остались примерно такими же, за исключением характеристики Precision, которая увеличилась примерно на 15%.

Третий эксперимент заключается в том, чтобы объединить данные из первого эксперимента за те годы, имеющие наилучшие и наихудшие показатели: 2010 и 2013 года, соответственно. Результаты анализа этих данных также приведены в табл. 2. Результаты не показывают повышения точности классификации.

Таблица 2

Результаты второго и третьего экспериментов

Характеристика	Значения второго эксперимента	Значения третьего эксперимента
Количество записей в выборке, млн	17,4	22,6
Доля записей, помеченных авторами набора как атака, %	27,3	8,6
Accuracy, %	83	59,4
Precision, %	63	12,7
Recall, %	91,3	64,6
Средняя уверенность в атаке (верная и неверная классификация), %	76,8	61,6
Средняя уверенность в отсутствии атаки, %	83,4	79

Заключение

Метод нечеткой кластеризации применим в задачах классификации сетевого трафика, но его эффективность зависит от выборки, о чем свидетельству-

ют проекции получившихся кластеров, где отчетливо видны границы кластеров.

Тестирование проводилось с использованием нескольких выборок, но только часть из них показали высокую точность классификации. Для повышения точности классификации необходимо либо расширить количество признаков, либо сократить (возможно, часть из низ являются избыточными). Повышение точности были получены при объединении тех выборок, которые по отдельности также показали точность выше среднего – более 60%.

К недостаткам можно отнести высокую степень ошибок второго рода.

Библиографический список

1. Браницкий А. А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А. А. Браницкий, И. В. Котенко // Информационно-управляющие системы. 2015. № 4. С. 69–77.

2. Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды ИСП РАН. Т. 33. Вып. 5. 2021. С. 83–104.

3. Датасеты по ИБ для машинного обучения. SecurityLab.ru. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/345789.php (дата обращения: 13.03.2022).

4. Description of Kyoto University Benchmark Data / Traffic Data from Kyoto University's Honeypots. URL: http://www.takakura.com/Kyoto_data/BenchmarkData-Description-New.pdf (дата обращения: 14.03.2022).

5. Fuzzy c-means clustering / MathWorks. URL: https://www.mathworks.com/help/fuzzy/fcm.html (дата обращения: 14.03.2022).

6. Kyoto FCM / Github/ URL: https://github.com/iIyaPopov/kyoto-fcm (дата обращения: 14.03.2022).

УДК 004.67

И. Д. Попов*
ассистент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

О РАЗМЕРНОСТИ ДАННЫХ KYOTO 2006 ПРИ ИСПОЛЬЗОВАНИИ МЕТОДА НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ

Рассмотрен вопрос сокращения размерности набора данных *Kyoto* 2006 при использовании метода нечеткой кластеризации. Приведена точность классификации данных при уменьшении их размерности.
***Ключевые слова*:** набор данных *Kyoto* 2006, метод нечеткой кластеризации, FCM, *Matlab*, оптимизация.

I. D. Popov*
Assistant
*St. Petersburg State University of Aerospace Instrumentation

ABOUT THE DIMENSION OF KYOTO 2006 DATASET WHEN USING THE FUZZY CLUSTERING METHOD

The issue of reducing the dimension of the Kyoto 2006 data set using the fuzzy clustering method is considered. The accuracy of data classification with decreasing their dimension is given.
Keywords: Kyoto 2006 dataset, fuzzy clustering, FCM, Matlab, optimization.

Введение

Метод нечеткой кластеризации (FCM) позволяет классифицировать объекты с некоторым значением вероятности (“уверенности”). В наборе данных *Kyoto* 2006 каждая запись характеризуется 24 признаками [1], что приводит к анализу данных из 24-мерного пространства. Уменьшение размерности пространства может снизить требуемые вычислительные ресурсы и получить точность классификации не ниже той, что получается при использовании полного набора признаков.

Классификация данных Kyoto 2006 при использовании всех признаков

Исходный набор данных *Kyoto* 2006 среди 24 признаков включает в себя поле с меткой о том, относится ли запись к классу вредоносного трафика, поэтому для тестирования данное поле не было использовано.

Для анализа в данной работе были использованы следующие признаки: все 14 основных признаков и 6, 8, 10 дополнительные признаки [1], т. е. всего 17.

Для вычислений использована функция FCM в *Matlab* [2], которая возвращает координаты центров кластеров (классы объектов) и вероятности отнесения объектов к каждому кластеру. Количество кластеров равно трем, так как с помощью поля с меткой класса трафика, авторами набора данных выделено

три типа: “была известная атака”, “была неизвестная атака”, “атаки не было”. Для упрощения типы “была известная атака” и “была неизвестная атака” объединены в один тип “была атака”. Таким образом, количество кластеров равно двум.

Пример проекций 17-мерного кластера приведен на рис. 1.

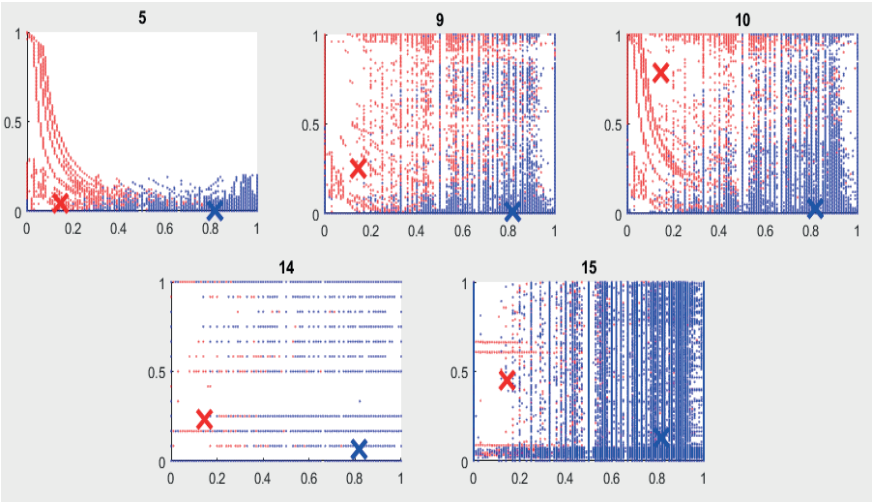


Рис. 1. Проекции 17-мерного кластера для признака 8

Точность классификации 17-мерных данных составляет *Accuracy* = 80,7%, *Recall* = 0,017%, что является совершенно низким показателем. Средняя “уверенность” FCM-метода при классификации составляет 95%.

Далее приведен анализ уменьшения размерности исходных 17-мерных данных.

Изменение размерности данных

Уменьшение размерности данных позволяет обрабатывать информацию быстрее, и также эта информация занимает меньше пространства в хранилище.

Если после уменьшения размерности данных точность классификации увеличится, это может значить, что в исходных данных были признаки, которые отрицательно влияют на итоговый результат. Если после уменьшения размерности данных точность классификации уменьшится, значит, исключенные признаки могут положительно влиять на результат, т. е. они важны. Наконец, если уменьшение размерности не привело к изменению точности, это может значить, что исключенные признаки были избыточны.

Может оказаться, что каждый признак отдельно вносит минимальный эффект в качество классификации данных, но в паре с другим признаком (или несколькими признаками) достигается максимальный результат.

В табл. 1 представлены некоторые результаты точности классификации при различных размерностях и наборах признаков (приведены наиболее эффективные варианты). Таблица со всеми полученными результатами представлена в [3].

Таблица 1

Точность классификации для малых размерностей данных

Размерность	Список признаков, на основе которых проведена классификация	*Recall*, %	*Precision*, %	FPR	Средняя «уверенность» FCM-метода в атаке и ее отсутствии, %
1	8 10	92,8 92,2	71 74,9	9 7,4	96,1 и 94,8 98 и 99
2	8, 13 9, 10 15, 16	92,8 92,3 55	70 73,3 43,6	9,5 8 17	94 и 89,9 86,8 и 99,3 90,6 и 97,2
3	8, 11, 13 7, 8, 13 9, 10, 11	92,8 92,8 92,8	69,7 69,9 73,3	9,7 9,6 8	93,5 и 87,9 94 и 88,4 86,8 и 99,3
4	2, 7, 10, 11 6, 7, 8, 10	92,2 92,2	74,9 74,9	7,4 7,4	97,9 и 99 97,9 и 99
5	1, 2, 6, 7, 10 1, 2, 8, 10, 14 1, 2, 8, 9, 10 1, 2, 5, 9, 10	92,2 92,2 92,3 92,3	74,9 74,8 73,3 73,3	7,4 7,4 8 8	97,2 и 98,8 97,1 и 98,7 86,2 и 99,1 85,4 и 99,1
6	1, 2, 6, 8, 9, 10 1, 2, 7, 8, 9, 10 1, 2, 8, 9, 10, 11 1, 2, 8, 9, 10, 12 1, 2, 8, 9, 10, 13 1, 2, 8, 9, 10, 17	92,3 92,3 92,3 92,3 92,3 92,3	73,3 73,3 73,3 73,3 73,3 73,3	8,1 8,1 8,1 8,1 8,1 8,1	86,2 и 99,1 86,2 и 99,1 86,2 и 99,1 86,2 и 99,1 86,2 и 99,1 86,2 и 99,1

Из результатов можно заметить, что наиболее часто встречаемым признаком является признак под номером 8 (*Srv_serror_rate*), и анализируя только его, можно с высокой “уверенностью” классифицировать записи из набора данных *Kyoto* 2006.

Стоит отметить, что результаты из табл. 1 (и те, что были ранее) приведены на основе анализа около 360 тысяч записей из всего набора.

Заключение

Исходный набор данных может содержать избыточные признаки, которые могут снижать эффективность классификации FCM-методом, из-за отсутствия какой-либо корреляции. Уменьшение размерности показало, что можно получить точность классификации не ниже той, что была бы получена при классификации исходных данных. В данной работе показаны результаты для размерностей 1–6. Большие размерности не анализировались из-за существенного увеличения времени анализа данных. Наиболее значимым признаком *Kyoto* 2006 оказался основной 8 признак (*Srv_serror_rate* – процент соединений с ошибкой за период), на основе которого (только одного его) можно с высокой вероятностью (более 90%) верно классифицировать объекты.

Библиографический список

1. Description of Kyoto University Benchmark Data // Traffic Data from Kyoto University's Honeypots. URL: http://www.takakura.com/Kyoto_data/BenchmarkData-Description-New.pdf (дата обращения: 14.03.2022).

2. Fuzzy c-means clustering / MathWorks/ URL: https://www.mathworks.com/help/fuzzy/fcm.html (дата обращения: 14.03.2022).

3. Kyoto-fcm / Github. URL: https://github.com/iIyaPopov/kyoto-fcm (дата обращения: 23.03.2022).

УДК 004.492.3

Д. Д. Савельева*
студент
Т. М. Татарникова*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

О СИСТЕМЕ КОНТРОЛЯ ЗА РАСХОДОМ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Рассмотрена система контроля за расходом трафика устройств интернета вещей для предотвращения угроз. Проблема рассмотрена в приложении к изучению дисциплины «Программно-защищенные инфокоммуникации» для бакалавров направления 11.03.02 «Инфокоммуникационные технологии и системы связи».
***Ключевые слова*:** системы контроля за расходом трафика, защищенные инфокоммуникации, функции защиты информации, интернет вещей.

D. D. Savelyeva*
Student
T. M. Tatarnikova*
PhD, Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

ABOUT THE SYSTEM FOR MONITORING THE TRAFFIC CONSUMPTION OF INTERNET OF THINGS DEVICES

The system of monitoring the traffic consumption of internet of things devices to prevent threats is considered. The problem is considered in the appendix to the study of the discipline "Software-protected infocommunications" for bachelors of the direction 11.03.02 "Infocommunication technologies and communication systems".
Keywords: traffic flow control systems, secure infocommunications, information security functions, internet of things.

Введение

Начиная с 21-го века, интернет вещей с каждым годом охватывает все новые области повседневной жизни человека и производства, оказывает существенное влияние на экономику. Сферы применения интернета вещей обширны и делятся на две группы: CIoT – *Consumer Internet of Things* и IIoT – *Industrial Internet of Things*.

Первая группа ориентирована на конечного пользователя и больше связана с умными бытовыми приборами и носимыми гаджетами. Вторая группа ориентирована на более крупные проекты для экономики, такие как умные города, электросети, автоматизация производства и многое другое [1 – 3].

Интернет угроз

Основная цель интернета вещей – это предоставление услуги без вмешательства человека. Однако, это же чревато появлением киберугроз, последствия от которых могут привести к разнообразным исходам – от потери работоспособности до перехвата управлением умными устройствами интернета вещей [4].

Самые популярные из киберугроз – это DDos-атаки и кража личных данных. В первом случае, атаки становятся возможными благодаря цепочке подключенных к интернету устройств и заражении каждого из них вредоносной программой, которая позволяет удерживать полный контроль над устройством без согласия владельца. Во втором случае, речь идет о данных, получаемых с различных датчиков и гаджетов пользователя, которые в случае кражи могут дать похитителю информацию личного характера. Например, датчик движения в доме может быть использован для получения информации о том, когда в доме есть активность, а когда дом пустует. Другими словами, во втором случае угроза состоит в потенциальной опасности попадания информации к злоумышленникам [5].

Большинство гаджетов не способны противостоять DDos-атакам и краже данных по ряду причин:

– Круглосуточная работа устройств позволяет даже в случаях частичного внешнего контроля обойти систему защиты.

– Полный контроль со стороны пользователя отсутствует.

– Сами владельцы редко замечают, что их устройства подвержены атаке или краже данных.

Таким образом, все причины связаны с тем, что внешний контроль пользователя отсутствует или очень слаб.

Система контроля за расходом трафика

Для усиления контроля за расходом трафика предлагается приложение, интегрированное в устройство интернета вещей. Приложение представляет собой информационную систему с функциями учета расхода трафика, контроля потребляемых ресурсов и прогнозирования объемов трафика и ресурсов, которая укажет пользователю на аномальные случаи. Таким образом, пользователь будет предупрежден о возможных атаках и краже.

Для улучшения результата работы система будет анализировать несколько характеристик трафика, полученного от устройства интернета вещей, такие как частота пакетов, передаваемых по определенному типу протокола, количество пакетов трафика за установленное время и т. д.

Процесс передачи трафика можно определить как нормальный или аномальный. Нормальным он будет считаться, если характеристики трафика проходят проверку по статистическим критериям.

Нормальное поведение устройства можно установить двумя способами: решение пользователя умного устройства и решение системы в период настройки параметров устройства. Любое поведение трафика отличное от заданного как нормальное будет считаться аномальным.

Для анализа и предсказания используется статическая проверка гипотезы о соответствии трафика нормальному поведению с помощью критерия согласия хи-квадрат χ^2. В модуле контроля информационной системы по ретроспективным данным фиксированных характеристик трафика выстраивается функция распределения характеристики. Выбор критерия χ^2 обусловлен несложными расчетами и самим назначением критерия для экспериментальных данных:

$$\chi^2 = \sum_n \frac{\left(f - \dot{f}\right)}{\dot{f}},$$

где f – наблюдаемая частота для каждой группы (интервала) функции распределения; $\dot{f}$ – ожидаемая (теоретическая) частота для каждой группы (интервала) функции распределения.

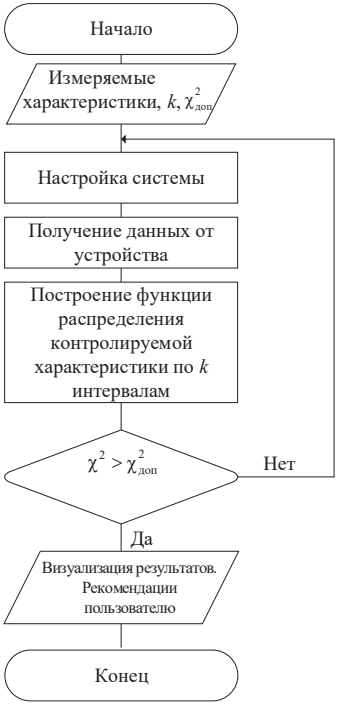


Рис. 1. Блок-схема работы системы за контролем трафика устройств интернета вещей

Интерпретация результатов:

– При $\chi^2 = 0$ – наблюдаемые и теоретически предсказанные значения частот точно совпадают, т. е. полученные данные попадают под определение нормального трафика.

– При $\chi^2 > 0$ – совпадений нет, чем больше значение χ^2, тем расхождения существеннее. Если $\chi^2 > \chi^2_{доп}$ гипотеза о нормальности трафика отвергается, $\chi^2_{доп}$ соответствует порогу, устанавливающего допустимое отклонение, ниже которого реальный трафик классифицируется как нормальный, иначе – как аномальный.

После анализа всех характеристик трафика по критерию χ^2 системой принимается решение о соответствии поведения умного устройства нормальному или аномальному поведению. В случае аномального поведения система сделает предположение о характере аномалии по соответствующей характеристике (характеристикам), которые не прошли проверку по критерию, и сообщит об этом пользователю. Планируется включить функцию отключения устройства дистанционно при обнаружении угрозы при разрешении пользователя и возможности гаджета при настройке.

Для улучшения взаимодействия с пользователем, система также будет выводить историю потребления трафика наглядно.

Библиографический список

1. Сахаров Д. В., Козлов Д. С. Обнаружение аномального поведения устройства IoT в сети на основе модели трафика. 2019. Т. 7. № 3. С. 50–55.

2. Ромасевич Е. П. Исследование агрегированного трафика беспроводных IoT устройств // Современные информационные технологии и ИТ-образование. 2017. Т. 3. № 3. С. 122–128.

3. Татарникова Т. М., Богданов П. Ю., Краева Е. В. Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 88–94.

4. Baddar S. A.-H., Merlo A., Mogliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Network, Ubiquitous Computing, and Dependable Applications. 2014. Vol. 5. No. 4. P. 29–64.

5. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36–41.

УДК 007.3

Е. В. Сайганова*
аспирант
*Государственный университет морского и речного флота имени адмирала С. О. Макарова

ЗАЩИТА ИНФОРМАЦИИ ОТНОСИТЕЛЬНО СОВРЕМЕННЫХ РЕАЛИЙ В ПРОЦЕССЕ СУДОРЕМОНТА

В статье рассмотрена проблема защиты информации при судоремонтных работах, которая недостаточно представлена и исследована Информация на судоремонтном предприятии должна быть представлена не только на бумажных носителях, но и на электронных, что позволит обеспечить дополнительную защиту информации от модификации, подлога или замены со стороны заинтересованных лиц, т. е. добиться состояния защищенности информации с точки зрения целостности.
***Ключевые слова*:** защита информации, съемные носители, судоремонтное предприятие, репутация предприятия.

E. V. Sayganova*
PhD Student
*Admiral Makarov State University of Maritime and Inland Shipping

PROTECTION OF INFORMATION ABOUT MODERN REALITIES IN THE PROCESS OF SHIP REPAIR

Protection of information about modern realities in the process of ship repair. It is narrated that information at a ship repair facility should be presented not only on paper, but also on electronic media, which will provide additional protection of information from modification, forgery or replacement by interested parties, so to achieve a state of information security from the point of view of integrity.
Keywords: information protection, removable media, ship repair company, reputation of the enterprise.

Рассмотрим проблему защиты информации при судоремонтных работах, если говорить о судоремонте как о производстве, то в данном контексте бумажные, электронные документы при работе дефектоскописта мало защищены от атак извне, в том числе ввиду отсутствия специализированной подсистемы защиты информации на устройствах и в программных продуктах, предназначенных для первичной и последующей обработки полученных сведений (результатов измерений), а также в следствие отсутствия готовых решений по организации защищенного канала передачи данных между устройством измерения и конечным банком данных для случаев электронного обмена информацией дефектоскопического характера. Чтобы предотвратить возможную утечку информации на любом производстве применяются специализированные защитные инструменты, включающие в себя как нормативно-правовое обеспечение (акты, инструкции, политика безопасности и разграничения доступа и т. д.), так и программно-аппаратные средства защиты.

Текущие мировые тенденции явно свидетельствуют о том, что информация в настоящее время остро нуждается в защите, в том числе и в части

применяемых съемных носителей информации, не утративших своей значимости во множестве отраслей несмотря на стремительную цифровизацию практически всех процедур по обработке, хранению, модификации (изменению), созданию и распространению информации в ходе происходящей в настоящий момент цифровой трансформации. Как правило, данные обстоятельство не остаются без внимания со стороны профильных учреждений, выступающих разработчики и дистрибьюторами тех или иных средств защиты. Так, например, комплексное решение по защите информации в учреждении от несанкционированного доступа (НСД) «*Dallas Lock*» в редакциях «*C*» и «*K*» позволяет при необходимости подключать дополнительный модуль, направленный на осуществление контролем за применением съемных машинных носителей информации.

Подробнее рассмотрим структуру судоремонтного предприятия. Основной структурной единицей предприятия является цех. В цехе происходит объединение однородных технологических процессов по изготовлению продукции (или части ее) или процессы по обслуживанию основного производства. В частности, нас интересует из множества цехов на производстве, таких как литейный, кузнечный, лесопильный, корпусно-сварочный цех и др. в особенности цех технической эксплуатации флота, что обусловлено необходимостью обработки данных и сведений, поступающих непосредственно от дефектоскописта, т. е. требующих, как и было обозначено ранее, проведения мероприятий и процедур, направленных на защиту таковых от посторонних вмешательств, а также от возможных искажений (в том числе вплоть до полного уничтожения) информации, связанных с физической составляющей процедуры снятия, обработки, хранения и передачи сведений такого характера. Отметим, что процедура дефектоскопического контроля может быть частично автоматизирована посредством применения методов и средств прогнозирования физического состояния металлического покрытия различных структурных элементов (оборудование, узлы, механизмы, силовые установки и т. д.) и корпуса судна в части деградации такового во времени, что также требует обеспечения защищенности сведений, хранящихся, обрабатываемых и вырабатываемых в предназначенном для выполнения данной процедуры устройстве. При этом, применение свойства мультизадачности современных электронно-вычислительных машин (ЭВМ) делает возможным применение одного выделенного автоматизированного рабочего места (АРМ) оператора, отвечающего за обработку результатов дефектоскопии, в качестве базовой структурной единицы, предназначенной также и для выполнения описанной процедуры прогнозирования деградации различных металлических покрытий на судне, что в свою очередь позволяет сформировать единое защищенное информационное пространство, защищенное посредством специализированных средств защиты от несанкционированного доступа (НСД), антивирусных и прочих выделенных ответственным за информационную безопасность данного предприятия угроз, а также сообщающееся с общей локально-вычислительной сетью (ЛВС) учреждения посредством шифрованного канала.

В случае с необходимостью формирования полномасштабной ЛВС учреждения, комплексная защита каждого АРМ может быть обеспечена посредством включения в систему обеспечения информационной безопасности средств, предназначенных для осуществления процедуры мониторинга и сканирования безопасности локальных сетей, таких как система контроля защищенности и соответствия стандартам *MaxPatrol* 8, сканер уязвимостей *XSpider* 7.8 и решения в составе защищенной *ViPNet*-криптосети (*ViPNet Policy Manager*, *ViPNet StateWatcher*, *ViPNet IDS NS* и т. д.).

Зададимся вопросом, зачем нам вообще защищать информацию на судне при ремонтных работах на предприятии. Так как предприятие выполняет многомерные с точки зрения формирования информационных потоков работы, в результате выполнения таковых вырабатывается ощутимое множество побочной информации, не касающейся данных работ напрямую, например, результаты переговоров между исполнителем и заказчиком, финансовые расчеты с контрагентами, деловая корреспонденция, отзывы в открытом сегменте сети Интернет и т. д. Исполнитель отвечает документами, подтвержденными Регистром Судоходства (далее – Регистр), что работы исполняются в полном объеме, но даже от Регистра можно умелыми дублерами листов скрыть коррозионные участки, которые не были заменены в процесс дефектоскопии. Если судно после ремонта выйдет из строя раньше положенного срока, ответственность за совершенные ошибки и недоработки понесет исполнитель.

Следовательно, для того, что чтобы предприятие функционировало долгое время и не терпело убытки, а также для предупреждения возможных чрезвычайных ситуаций и происшествий, вытекающих из всего вышесказанного, требуется обеспечить целостность полученной от дефектоскописта информации, т.е. невозможность внесения в таковую каких-либо правок под требования заказчика в целях достижения таковых краткосрочной экономической выгоды в силу отказа от проведения требуемых работ по физическому восстановлению судовых компонентов. Логично также предположить, ответственные работники производственного учреждения не будут жертвовать своей репутацией и репутацией своего предприятия, поддаваясь на уговоры недобросовестных заказчиков. Таким образом, данная задача целиком и полностью лежит в рамках процедуры обеспечения и поддержания информационной безопасности в учреждении, представленной следующими тремя составляющими: целостность, доступность и конфиденциальность.

Достижение требуемого уровня защищенности информации в данном случае подразумевает организацию системы обеспечения информационной безопасности на предприятии в соответствии со всеми критериями, представленными в основополагающих национальных стандартах по безопасности информации в автоматизированных и прочих системах.

Если рассматривать информацию как совокупность данных, то даже без проведения глубокого анализа защищенности информационных систем и потоков возможно заметить, что в судостроении и судоремонте присутствует огромный пласт данных, которые, как правило, ничем не защищены, но обладают при

этом значительной потенциальной ценностью для различного рода заинтересованных лиц: как для заказчика с исполнителем, так и для конкурентов и злоумышленников.

Как же защитить данные организации? Для этого в современном мире используются такие средства защиты информации, как применение съемных машинных носителей в совокупности со средствами их защиты. Основными съемными машинными носителями в настоящее время являются *flash*-накопители, CD/DVD/*Blu-Ray* диски и, возможно, дискеты для случаев, когда присутствует необходимость применения таковых, обусловленная особенностями функционирования сформированной в учреждении информационной системы.

Также допускается применение специальной парольной защиты съемных носителей, организуемой либо базовым набором инструментов на каждом таком носителей, либо посредством специальных сторонних программных продуктов. Непосредственно хранящиеся на таких носителях документы при этом могут быть дополнительно защищены посредством электронной цифровой подписи (ЭЦП), направленной на подтверждение подлинности юридически важной документации, а также не обеспечение невозможности отказа от авторства над таковой, что исключает подлог подобного рода документации при условии соблюдения требования по хранению и применению средств криптографической защиты информации (СКЗИ), предназначенных для корректного применения ЭЦП, таких как, например, мультиплатформенный криптопровайдер «КриптоПро CSP» версии 4.0 и 5.0.

Из всего вышесказанного следует однозначный вывод о том, что разработку и внедрение системы защиты информации внутри компании обязаны производить профессионалы, т. е. высококлассные специалиста необходимого профиля, не имеющие возможности извлечения собственной выгоды за счет нарушения какой-либо из составляющих информационной безопасности при обработке сведений, необходимых для осуществления основной деятельности учреждения.

Библиографический список

1. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. Москва: МИФИ, 1997. 537 с.

2. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении.

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определение.

4. Диева С. А. Организация и современные методы защиты информации / С. А. Диева, А. Г. Шаваева. М.: Концерн «Банковский деловой центр», 1998. 472 с.

5. Приказ ФСТЭК России от 18.02.2013 № 21. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6. Чекулаева Е. Н. Разработка системы противодействия угрозам информационной безопасности при идентификации съемных носителей в автоматизированной системе / Е. Н. Чекулаева, Е. В. Фомин // Международный научно-исследовательский журнал. 2020. № 5 (95). С. 87–93.

7. Чистов В. Б. Перспективы автоматизации процесса дефектации судов / В. Б. Чистов, А. Б. Гурьянова // Сб. науч. тр. СПГУВК. СПб.: СПГУВК. 1999.

УДК 004.492.3

А. В. Сверликов*
студент
Т. М. Татарникова*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МЕТОДИКА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ ПАТТЕРНОВ ПОВЕДЕНИЯ УМНЫХ УСТРОЙСТВ

Предлагается методика поиска аномального поведения устройств интернета вещей путем сравнения паттерна нормального поведения устройства, хранимого в базе эталонных данных, с паттерном текущего состояния.
***Ключевые слова*:** сетевой трафик, интернет вещей, паттерн поведения, аномальное поведение, система обнаружения вторжений.

A. V. Sverlikov*
Student
T. M. Tatarnikova*
Dr. Sc., Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

TECHNIQUE FOR DETECTING ANOMALOUS INTERNET OF THINGS TRAFFIC BASED ON BEHAVIOR PATTERNS OF SMART DEVICES

The method of searching for abnormal behavior of Internet of Things devices by comparing the pattern of normal behavior of the device stored in the reference database with the template of the current state is proposed.
Keywords: network traffic, internet of things, behavior pattern, anomalous behavior, intrusion detection system.

Введение

Система обнаружения вторжений IDS (*Intrusion Detection System*) является основным программным и(или) аппаратным решением по выявлению аномального сетевого трафика, несущего вредоносный код [1]. Методы, используемые в системах обнаружения вторжения, относятся к активным и реализуют поиск по сигнатуре или поиск по аномалии.

Поиск по сигнатуре позволяет обнаруживать только известные атаки, сигнатуры которых содержатся в базе данных IDS.

Для интернета вещей (IoT – *Internet of things*) рекомендуется поиск по аномалии, который подразумевает, во-первых, создание паттернов нормального поведения каждого из IoT-устройств и, во-вторых, выявление отклонения в ра-

боте IoT-устройства путем сравнения текущего поведения устройства с паттерном его нормального поведения [2].

В работе предлагается способ получения паттерна нормального поведения IoT-устройства и методика поиска по аномалии поведения.

Постановка задачи

Основой взаимодействия и подключения новых устройств интернета вещей является технология *Machine-to-Machine* (M2M) [3]. Организация M2M-взаимодействия основано на протоколе CoAP (*Constrained Application Protocol*). Этот протокол разработан специально для маломощных устройств, совместим с HTTP (*HyperText Transfer Protocol*) и реализует передачу данных такими, как они есть – без модификаций и инкапсулирования [4]. Протокол CoAP является бинарным и работает поверх UDP (*User Datagram Protocol* – протокол пользовательских датаграмм) [5]. В общем случае, взаимодействие клиента с умным устройством IoT выглядит, как на рис. 1, где подразумевается, что пакеты данных с IoT-устройства проходят через прокси-сервер, где инкапсулируются в HTTP-пакеты [6].

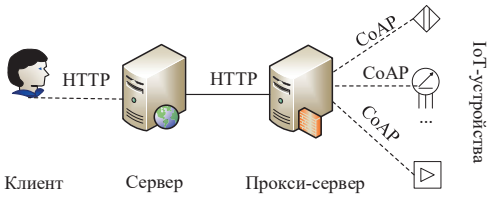


Рис. 1. Схема взаимодействия пользователя с IoT-устройством

Суть предлагаемого подхода заключается в следующем. В дискретные моменты времени регистрируются значения характеристик IoT-устройства, которые можно рассматривать как паттерн его поведения – случайную векторную функцию

$$X(t) = f(H(t), h(t)),\ t_0 \le t \le t_k, \qquad (1)$$

где $X(t)$ – наблюдаемая последовательность данных; $H(t)$ – характеристика передаваемого трафика; $h(t)$ – шумовая составляющая; t_0 и t_k – левая и правая граница соответственно интервала времени, в течение которого выполняется замер характеристик.

Определим множество состояний $S = \{s_0, s_1, \ldots, s_n\}$, в одном из которых в дискретный момент времени t_i может находится устройство. Характеристики фиксируются в дискретные моменты $t_i,\ i = \overline{0,k}$ временного ряда $x_i = X(t_i)$, так что $H_i = H(t_i)$.

Паттерны нормального поведения IoT-устройств определим как множество $P = \{p_0, p_1, \ldots, p_n\}$. Под паттерном нормального поведения будем понимать

набор характеристик в каждом из s_j, $j=\overline{0,n}$ состояний [7], хранимых в базе эталонных данных.

В качестве показателя, указывающего на аномальное поведение IoT-устройства, возьмем отклонение d между паттерном нормального поведения p и паттерном реального поведения p'. Таким образом для обнаружения аномального поведения IoT-устройства необходимо найти алгоритм A: $P \to S$, отражающий множество P во множество S. Разбивая множество S на два подмножества аномального $S1$ и нормального $S2$ состояний, решающее правило $\dot{R} \Leftrightarrow d$ алгоритма A ставит в соответствие наблюдению $X(t)$ одного из множеств: $S1$, при $d \geq_{доп}$ или $S2$, при $d < d_{доп}$, где $d_{доп}$ – пороговое значение. В качестве $\dot{R}$ предлагается проверка статистической гипотезы о функции распределения снимаемых характеристик, где значение $d_{доп}$ является статистическим критерием.

Построение паттерна поведения IoT-устойства

Для построения паттернов поведения нами будут использованы стендовые модели наподобие рис. 1. Аналоги IoT-устройств будут построены на платах ESP8266 с Wi-Fi модулем и платформах *DeviceHive* или *Blynk*, являющихся IoT-платформами с открытым исходным кодом.

Для построения паттерна, съем характеристик будет произведен в двух состояниях:

– отправки данных, при котором устройство передает данные, назовем это состояние s_1;

– получения команд, при котором устройство получает команды выполнения, назовем это состояние s_2.

На рис. 2 приведен пример графика передачи данных на платформе *DeviceHive*.

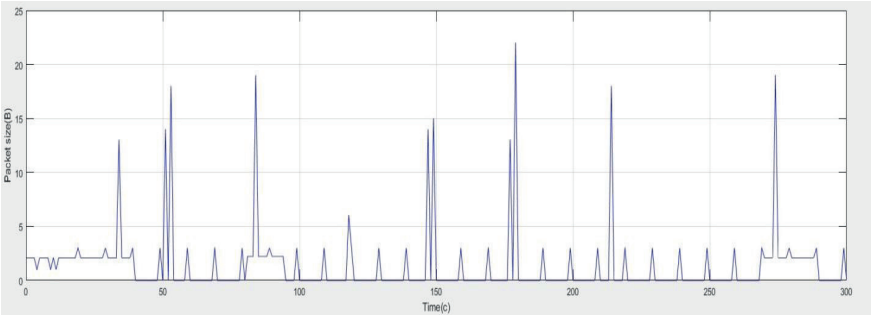


Рис. 2. Передача данных устройством (DeviceHive)

На основе зафиксированного временного ряда может быть построена плотность распределения снимаемой характеристики $F(X)$. Например, на рис. 3 приведена плотность распределения вероятностей временных задержек отправ-

ки пакетов розеткой *Xiaomi*.

Плотность распределения снимаемой характеристики аппроксимируется известной функций, которая ляжет в основу статистической проверки гипотез.

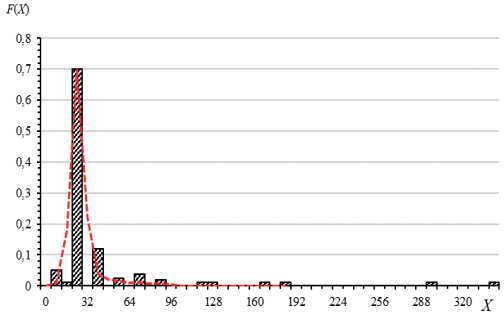


Рис. 3. Плотность распределения вероятностей временных задержек отправляемых пакетов данных от розетки

Методика обнаружения аномального поведения IoT-устройства

Предлагаемая методика включает следующие шаги:

1. Подготовка исходных данных:

1.1. Получение паттерна поведения умного устройства.

1.2. Запись паттерна поведения умного устройства в базу эталонных данных СОА.

1.3. Выбор порогового значение $d_{доп}$.

2. При передаче данных:

2.1. На сервере фиксируется временной ряд передаваемых пакетов данных в течении временного периода t_0 и t_k.

2.2. Подсчитать количество временных тактов n_i^1, $i=\overline{1,N}$ с измерением характеристики за период $[t_0, t_k]$, где N – количество временных тактов в периоде $[t_0, t_k]$. Подсчитывается количество состояний s_1.

2.3. Подсчитать относительные частоты временных тактов с соответствующими измерениями характеристики в периоде $[t_0, t_k]$: $\hat{p}_1=\frac{n_1^1}{N},...,\hat{p}_N=\frac{n_N^1}{N}$.

2.4. Построить p' – паттерн текущего поведения IoT-устройства, как плотность распределения частот $\hat{p}_1=\frac{n_1^1}{N},...,\hat{p}_N=\frac{n_N^1}{N}$ на периоде $[t_0, t_k]$.

2.5. Сервер обращается к базе эталонных данных и по ID устройства находит паттерн p его поведения.

2.6. Сервер выполняет потактовое сравнение p и p': $d=\sum_{j=1}^{N}\left(p_j-p'_j\right)^2$.

2.7. Сравнить d и $d_{доп}$. Если $d \geq d_{доп}$, то генерируется оповещение о состоянии $S1$. Если $d < d_{доп}$, то регистрируется, при необходимости, состояние $S2$.

3. При приеме данных от сервера на IoT-устройства действия аналогичны пп. 2.1–2.7, только анализируется трафик, принимаемый IoT-устройствами, и принимается решение о возможной компрометации сервера.

Заключение

Предложенная в статье методика анализа трафика с целью поиска аномалий, несущих атаку на устройства интернета вещей, является частью системы обнаружения вторжений и реализует свои функции на нижнем уровне архитектуры интернета вещей, т. е. на уровне IoT-устройств.

Библиографический список

1. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети. Сетевые аномалии. М.: Горячая линия. Телеком. 2013. 220 с.

2. Сахаров Д. В., Козлов Д. С. Обнаружение аномального поведения устройства IoT в сети на основе модели трафика. 2019. Т. 7. № 3. С. 50–55.

Bogatyrev V. A., Bogatyrev A. V., Bogatyrev S. V. Redundant Servicing of a Flow of Heterogeneous Requests Critical to the Total Waiting Time During the Multi-path Passage of a Sequence of Info-Communication Nodes // Lecture Notes in Computer Science. 2020. Vol. 12563. P. 100–112.

3. Татарникова Т. М., Богданов П. Ю., Краева Е. В. Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 88–94.

4. Lee Perry. Internet of Things Architects. Packt Publishing. 2018. 514 p.

5. Богатырев В. А., Богатырев А. В., Голубев И. Ю., Богатырев С. В. Оптимизация распределения запросов между кластерами отказоустойчивой вычислительной системы // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3 (85). С. 77–82.

6. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36–41.

УДК 621.391

А. Н. Трофимов*
кандидат технических наук, доцент
Ф. А. Таубин*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АНАЛИЗ КАСКАДНОГО КОДИРОВАНИЯ ДЛЯ МНОГОУРОВНЕВОЙ ФЛЭШ-ПАМЯТИ С ИСПОЛЬЗОВАНИЕМ СМЕШАННОЙ NORMAL-LAPLACE МОДЕЛИ

Проведен анализ помехоустойчивости кодовых конструкций для с многоуровневой флэш-памяти. В качестве внутреннего кода рассматриваются: а) конечные подмножества решеток Барнса – Уолла и б) двухуровневые конструкции. Внешним кодом служит расширенный код Рида – Соломона. Канал записи/считывания многоуровневой флэш-памяти аппроксимируется смешанной *Normal-Laplace* моделью. Показано, в частности, что рассмотренные конструкции позволяют обеспечить увеличение числа циклов перезаписи в 2–2,5 раза относительно номинального значения при сохранении требуемого значения вероятности ошибки на бит.
Ключевые слова: каскадное кодирование, многоуровневая флэш-память, смешанная *Normal-Laplace* модель, вероятность ошибки, аддитивная граница, число циклов перезаписи.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004 «Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств».

A. N. Trofimov*
PhD, Tech., Associate Professor
F. A. Taubin*
Dr. Sc., Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

ANALYSIS OF CONCATENATED CODING SCHEME FOR THE MULTILEVEL FLASH MEMORY USING NORMAL-LAPLACE MIXTURE

An analysis of the performance of concatenated coding scheme for multilevel flash memory has been carried out. As an inner code we consider a) finite subsets of Barnes-Wall lattices and b) two-level constructions; the outer code is the extended Reed-Solomon code. The write/read channel of a multilevel flash memory is approximated by a mixed Normal-Laplace model. It is shown, in particular, that the considered constructions make it possible to increase the number of P/E cycles by a factor of 2–2,5 with respect to the nominal value while maintaining the required value of the bit error probability.
Keywords: concatenated coding scheme, multilevel flash memory, mixture Normal-Laplace model, union bound, program/erase cycles.

Введение

Хорошо известно, что в результате повышения плотности записи, характеристики основных параметров многоуровневой NAND флэш-памяти: вероятность ошибки, выносливость и долговечность хранения, как правило, оказываются неприемлемыми (как по отдельности, так и в совокупности). Так, исходная вероятность ошибки в четырехуровневой флэш-памяти, даже при умеренных значениях числа циклов перезаписи и времени хранения, составляет порядка $10^{-4}...10^{-3}$ и более, тогда как требуемая вероятность ошибки лежит в диапазоне $10^{-12}...10^{-16}$. Стандартным решением, позволяющим улучшить характеристики многоуровневой флэш-памяти, является введение помехоустойчивого кодирования [1 – 4].

Одна из основных проблем, возникающих при реализации помехоустойчивого кодирования в NAND флэш-памяти связана с необходимостью учета наличия нескольких источников шума, характеристики которых изменяются при изменении как количества выполненных циклов программирования/стирания, так и времени хранения данных в памяти. Таким образом, эффективность введения помехоустойчивого кодирования в существенной степени определяется адекватностью модели, формализующей основные процессы, связанные с записью и чтением данных. В работах [3, 4] рассматривалась каскадная схема помехоустойчивого кодирования применительно к гауссовой модели шума с дисперсией, зависящей от уровня записи (*input-dependent additive Gaussian noise*, ID-AGN). В данной работе рассматривается более адекватная модель совокупности помех, определяющих случайные отклонения считываемых из ячейки сигналов от целевых уровней, а именно смешанная NL (*Normal-Laplace*) модель.

Смешанная NL модель искажений в многоуровневой NAND флэш-памяти

NL распределение представляет собой свертку гауссова распределения и распределения Лапласа. Общее выражение для плотности NL распределения имеет следующий вид. Пусть $\xi(m,\sigma)$ – гауссова случайная величина с плотностью распределения

$$f_g(\xi;m,\sigma)=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(\xi-m)^2}{2\sigma^2}\right),$$

где m – среднее значение, σ^2 – дисперсия. Пусть $\zeta(\lambda,\mu)$ – случайная величина с асимметричной плотностью распределения Лапласа

$$f_{sl}(\zeta;\lambda,\mu)=\begin{cases}\dfrac{\lambda\mu}{\lambda+\mu}\exp(-\lambda\zeta), & \zeta>0,\\ \dfrac{\lambda\mu}{\lambda+\mu}\exp(\mu\zeta), & \zeta\le 0,\end{cases}$$

где $\lambda > 0$, $\mu > 0$ – параметры перекошенного распределения Лапласа. Пусть $y = \xi(m,\sigma) + \zeta(\lambda,\mu)$; тогда случайная величина y имеет NL распределение с плотностью

$$f_{NL}(y;m,\sigma,\lambda,\mu) = \frac{1}{2}\frac{\lambda\mu}{\lambda+\mu}\times$$

$$\times\left(e^{\frac{\lambda(-2y+2m+\lambda\sigma^2)}{2}}\operatorname{erfc}\left(-\frac{y-m-\lambda\sigma^2}{\sqrt{2}\sigma}\right)+e^{\frac{\mu(2y-2m+\mu\sigma^2)}{2}}\operatorname{erfc}\left(\frac{y-m+\mu\sigma^2}{\sqrt{2}\sigma}\right)\right).$$

В работе [5] предложена два варианта модели четырехуровневой ячейки флэш-памяти, названные «идеальный» и «смешанный». Обозначим упорядоченную по возрастанию последовательность целевых уровней (состояний) напряжения в ячейке как x_0, x_1, x_2, x_3; наименьший по величине целевой уровень x_0 соответствует состоянию «стерто». В идеальном варианте условные функции плотности вероятности выходных значений заданы как:

$$\begin{aligned}
&p_{y|x_0}^{(ideal)}(y\,|\,x_0) = f_{sl}(y-x_0;\lambda_0,\infty),\\
&p_{y|x_1}^{(ideal)}(y\,|\,x_1) = f_{NL}(y;x_1,\sigma_1,\lambda_1,\mu),\\
&p_{y|x_2}^{(ideal)}(y\,|\,x_2) = f_{NL}(y;x_2,\sigma_2,\lambda_2,\mu),\\
&p_{y|x_3}^{(ideal)}(y\,|\,x_3) = f_{sl}(y-x_3;\infty,\mu).
\end{aligned} \tag{1}$$

Более точное соответствие с результатами экспериментальных измерений, достигается при использовании смеси распределений, задаваемых равенствами (1):

$$\begin{bmatrix} p_{y|x_0}(y\,|\,x_0)\\ p_{y|x_1}(y\,|\,x_0)\\ p_{y|x_2}(y\,|\,x_0)\\ p_{y|x_3}(y\,|\,x_0)\end{bmatrix} = \begin{bmatrix} k_{00} & 0 & k_{02} & k_{03}\\ 0 & k_{11} & k_{12} & k_{13}\\ 0 & 0 & k_{22} & k_{23}\\ 0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix} p_{y|x_0}^{(ideal)}(y\,|\,x_0)\\ p_{y|x_1}^{(ideal)}(y\,|\,x_1)\\ p_{y|x_2}^{(ideal)}(y\,|\,x_2)\\ p_{y|x_3}^{(ideal)}(y\,|\,x_3)\end{bmatrix}, \tag{2}$$

где все величины $k_{00}, k_{01}, ..., k_{33}$ положительны, и кроме того $k_{00}+k_{02}+k_{03}=1$, $k_{11}+k_{12}+k_{13}=1$, $k_{22}+k_{23}=1$ и $k_{33}=1$. Такое описание канала называется смешанной NL (*mixed Normal-Laplace*) моделью. Конкретный вид функций плотности вероятности вида (2) определяется значениями пятнадцати параметров: четырех значений уровней $x_0, ... x_3$, шести значений параметров плотностей в (1) $\lambda_0, \sigma_1, \lambda_1, \mu, \sigma_2, \lambda_2$ и пяти весовых коэффициентов $k_{02}, k_{03}, k_{12}, k_{13}, k_{23}$ в правой части равенства (2). В работе [5] указаны значения этих параметров в зависимо-

сти от отношения N / N_{nom}, где N – число циклов перезаписи, N_{nom} – число циклов перезаписи, гарантируемое производителем устройства памяти, или номинальное число циклов перезаписи.

Численные результаты и выводы

В работах [3, 4] были предложены и исследованы несколько вариантов каскадной схемы помехоустойчивого кодирования применительно к ID-AGN модели искажений в многоуровневой NAND флэш-памяти. В этой схеме внутренний код построен либо основе решеток Барнса – Уолла, либо на основе циклически усеченного сверточного кода и кода с проверкой на четность, и декодируется по максимуму правдоподобия (МП). В качестве внешнего кода выбран расширенный (удлиненный на один символ) код Рида – Соломона. В рамках данной работы ряд вариантов каскадной схемы кодирования был проанализирован применительно к изложенной выше смешанной NL модели искажений. Основная проблема при анализе помехоустойчивости указанной каскадной схемы кодирования связана с вычислением аддитивной оценки вероятности ошибки декодирования внутреннего кода. Она решается с помощью расширения на смешанную NL модель искажений ранее разработанного подхода [3, 4, 6], базирующегося на использовании характеристических функций. В качестве примера, иллюстрирующего применение этой техники оценки помехоустойчивости каскадного кодирования для канала, заданного смешанной NL моделью, на рис. 1 представлены результаты вычисления верхней границы вероятности ошибки декодирования P_b в зависимости от значений нормированного числа циклов перезаписи N / N_{nom} для каскадной схемы с внутренним кодом на основе решетки Λ_{16} (имеющим минимальное расстояние $\sqrt{8}$) и внешним кодом Рида – Соломона с длиной 1024. В целом, проведенный анализ рассмотренных каскадных кодовых конструкций позволяет сделать следующие выводы.

1. Для каждой из рассмотренных конструкций при числе циклов перезаписи N в диапазоне от $0{,}1N_{\text{nom}}$ до N_{nom} незначительное увеличение плотности записи (это увеличение может быть даже несколько тысячных) сопровождается существенным ростом вероятности ошибки (на порядок и более).

2. Номинальное число циклов перезаписи N_{nom} в смешанной NL модели может рассматриваться, как своего рода граничное значение. Так, увеличение числа циклов перезаписи N на порядок – от $0{,}1N_{\text{nom}}$ до $1{,}0N_{\text{nom}}$, приводит к росту вероятности ошибки на 1,5…2 порядка, тогда как дальнейшее увеличение числа циклов перезаписи N на порядок – до $10N_{\text{nom}}$, приводит к неприемлемым значениям вероятности ошибки.

3. За счет очень незначительного снижения плотности записи можно обеспечить увеличение числа циклов перезаписи в 2–2,5раза относительно номинального значения N_{nom} при сохранении требуемого значения вероятности ошибки на бит. Как видно на рис. 1, при снижении плотности записи с 1,2231 до 1,2158 бит/ячейка вероятность ошибки на бит остается в пределах $\approx 2\ 10^{-15}$ при значении $N/N_{\text{nom}} = 2$.

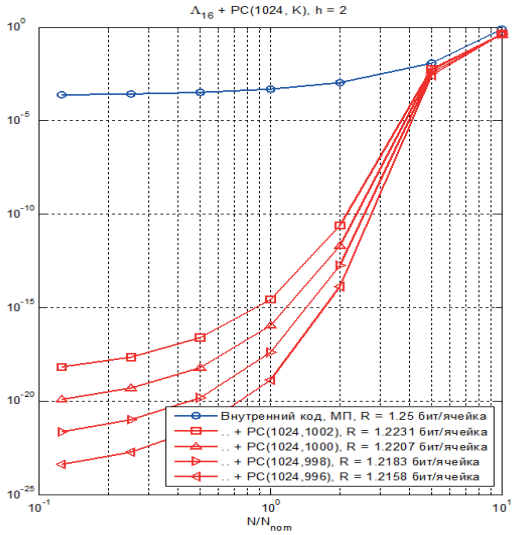


Рис. 1. Зависимость границы вероятности ошибки P_b от нормированного числа циклов перезаписи N/N_{nom}

Библиографический список

1. Micheloni R. Error Correction Codes for Non-Volatile Memories / R. Micheloni, A. Marelli, R. Ravasio. Springer Science & Business Media, 2008. 338 p.

2. Dolecek L. Channel coding for nonvolatile memory technologies: Theoretical advances and practical considerations / L. Dolecek, Y. Cassuto // Proc. of the IEEE. 2017. № 9. P. 1705–1724.

3. Таубин Ф. А. Каскадное кодирование на основе многомерных решеток и кодов Рида – Соломона для многоуровневой флэш-памяти / Ф. А. Таубин, А. Н. Трофимов // Труды СПИИРАН. 2018. Вып. 2 (57). С. 75–103.

4. Таубин Ф. А. Каскадное кодирование для многоуровневой флэш-памяти с исправлением ошибок малой кратности во внешней ступени / Ф. А. Таубин, А. Н. Трофимов // Труды СПИИРАН. 2019. Вып. 1 8(5). С. 1149–1181.

5. Parnell T. Modelling of the Threshold Voltage Distributions of Sub-20nm NAND Flash Memory / T. Parnell, N. Papandreou, T. Mittelholzer, H. Pozidis // IEEE Global Communications Conference. 2014. P. 2351–2356.

6. Трофимов А. Н. Вычисление аддитивной границы вероятности ошибки декодирования с использованием характеристических функций / А. Н. Трофимов, Ф. А. Таубин // Информационно-управляющие системы. 2021. № 4. С. 71–85.

УДК 621.391

А. Н. Трофимов*
кандидат технических наук, доцент
Ф. А. Таубин*
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ВЫЧИСЛЕНИЕ АДДИТИВНОЙ ГРАНИЦЫ ВЕРОЯТНОСТИ ОШИБКИ ДЕКОДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ ДЛЯ КАНАЛОВ С ПАМЯТЬЮ

Представлен подход к вычислению границы вероятности ошибки декодирования для каналов с памятью. Он состоит в численном интегрировании выражения, построенного с использованием решетки кода и решетки канала, и включающего характеристические функции для логарифмов отношения правдоподобия.
***Ключевые слова*:** каналы с памятью, модель с конечным числом состояний, модель с детерминированными переходами, декодирование по максимуму правдоподобия (МП), аддитивная граница вероятности ошибки, характеристическая функция.

A. N. Trofimov*
PhD, Tech., Associate Professor
F. A. Taubin*
Dr. Sc., Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

EVALUATION OF THE UNION BOUND FOR THE DECODING ERROR PROBABILITY USING CHARACTERISTIC FUNCTIONS FOR CHANNELS WITH MEMORY

We present an approach for evaluation of the union bound on decoding error probability for channels with memory. It consists in numerical integration of an expression contained characteristic functions of the log likelihood ratio. This expression is obtained using a combination of the code trellis and the channel trellis.
Keywords: channels with memory, finite state model, model with deterministic transitions, maximum likelihood decoding, union bound, characteristic function.

Введение

Для произвольных кодов и каналов вычисление аддитивной границы оказывается весьма сложным, поэтому обычно используются получаемые в замкнутой форме те или иные аппроксимации аддитивной границы. В работе [1] предоставлен метод точного вычисления аддитивной границы вероятности ошибочного декодирования для широкого класса кодов и моделей каналов без памяти. Предложенный метод включает получение точного выражения для попарной вероятности ошибки за счет использования характеристических функций логарифма отношения правдоподобия для произвольной пары кодовых слов. Полученное интегральное выражение для аддитивной границы оказывает-

ся удобным для расчетов с использованием процедуры численного интегрирования. В настоящей работе представлено распространение этого подхода на некоторые модели каналов с памятью.

Модель канала

Пусть переходные вероятности для канала с дискретным выходом или функции плотности вероятности (ф.п.в.) для канала с непрерывным выходом, определяющие канал, заданы как

$$p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) = \sum\nolimits_{\mathbf{s}} p_{\mathbf{yxs}}(\mathbf{y},\mathbf{x},\mathbf{s}) \,/\, p_{\mathbf{x}}(\mathbf{x}),$$

где $\mathbf{s} = (s^{(0)}, s^{(1)}, ..., s^{(n)}, ...)$ последовательность состояний канала, $s^{(n)} \in S$, S – множество состояний канала, $|S| < \infty$; $p_{\mathbf{yxs}}(\mathbf{y},\mathbf{x},\mathbf{s})$ – совместная вероятность (ф.п.в) векторов $\mathbf{y}$, $\mathbf{x}$ и $\mathbf{s}$.

Можно показать, что

$$p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) = \sum\nolimits_{\mathbf{s}} p_{\mathbf{y}|\mathbf{xs}}(\mathbf{y}\,|\,\mathbf{x},\mathbf{s})\, p_{\mathbf{s}|\mathbf{x}}(\mathbf{s}\,|\,\mathbf{x}),$$

где $p_{\mathbf{y}|\mathbf{sx}}(\mathbf{y}\,|\,\mathbf{s},\mathbf{x})$ – условная вероятность (условная ф.п.в.) выхода канала при фиксированных векторах $\mathbf{x}$ и $\mathbf{s}$, и $p_{\mathbf{s}|\mathbf{x}}(\mathbf{s}\,|\,\mathbf{x})$ – условная вероятность состояний канала при фиксированном входном векторе $\mathbf{x}$. Предположим, что канал задан как вероятностный конечный автомат, т. е.:

$$p_{\mathbf{y}|\mathbf{xs}}(\mathbf{y}\,|\,\mathbf{x},\mathbf{s}) = \prod\nolimits_{n=1}^{N} p_{y|xs}(y^{(n)}\,|\,x^{(n)}, s^{(n-1)}),$$

$$p_{\mathbf{s}|\mathbf{x}}(\mathbf{s}\,|\,\mathbf{x}) = p_s(s^{(0)}) \prod\nolimits_{n=1}^{N} p_{s|xs}(s^{(n)}\,|\,x^{(n)}, s^{(n-1)}),$$

где $p_s(s^{(0)})$ – безусловное распределение на множестве S, $p_{s|xs}(s^{(n)}\,|\,x^{(n)}, s^{(n-1)})$ – условная вероятность перехода канала из состояния в состояние, и $\Pr[x^{(n)} = x, s^{(n-1)} = s] = p_x(x)\, p_s(s)$, т. е. вход канала $x^{(n)}$ и текущее состояние канала $s^{(n-1)}$ независимы. Такая модель представляется достаточно общей, и она широко используется в исследованиях (см., например, [2] и приведенные там ссылки). Укажем некоторые частные случаи этой модели: 1) каналы, у которых переходы из состояния в состояние не зависят от входного символа (*channel with freely evolving states*) [2], т. е. $p_{s|xs}(s^{(n)}\,|\,x^{(n)}, s^{(n-1)}) = p_{s|s}(s^{(n)}\,|\,s^{(n-1)})$; канал Гилберта – Эллиотта представляет собой пример такой модели; 2) каналы с детерминированными переходами, в этом случае

$$p_{s|xs}(s^{(n)}\,|\,x^{(n)}, s^{(n-1)}) = \begin{cases} 1, & \text{если } s^{(n-1)} \xrightarrow{x^{(n)}} s^{(n)} \\ 0, & \text{в противном случае} \end{cases}. \qquad (1)$$

Примером такой модели может служить канал с межсимвольной интерференцией. Условные вероятности (условные ф.п.в) $p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x})$ можно представить как

$$p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) =$$

$$= \sum_{s^{(0)}} \cdots \sum_{s^{(N-1)}} \sum_{s^{(N)}} p_s(s^{(0)}) \left(\prod_{n=1}^{N} p_{y|xs}(y^{(n)}\,|\,x^{(n)}, s^{(n-1)}) p_{s|xs}(s^{(n)}\,|\,x^{(n)}, s^{(n-1)}) \right). \quad (2)$$

Аддитивная граница для каналов с памятью

Решающее правило декодировании по максимуму правдоподобия (МП) имеет вид $\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x})$, где $p(\mathbf{y}\,|\,\mathbf{x})$ – условная вероятность (для канала с дискретным выходом) или N-мерная условная ф.п.в., задающая распределение выходных значений $\mathbf{y} = (y^{(1)}, ..., y^{(N)})$ канала с непрерывным выходом, где $\mathbf{x}$ – переданное кодовое слово длиной N. В работах [1, 3] было показано, что аддитивная граница вероятности ошибки декодирования по МП может быть ограничена сверху в виде:

$$p_e < \frac{1}{\pi M} \int_0^{\infty} \mathrm{Re} \frac{D(\alpha - j\beta) - M}{\beta + j\alpha} d\alpha, \quad (3)$$

где

$$D(\omega) = \sum\nolimits_{\mathbf{x}} \sum\nolimits_{\mathbf{x}'} C_Z(\omega; \mathbf{x}, \mathbf{x}'),$$

$$C_Z(\omega; \mathbf{x}, \mathbf{x}') = \overline{\exp(j\omega Z(\mathbf{y}\,|\,\mathbf{x}, \mathbf{x}'))} = \overline{\left(p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}') / p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) \right)^{j\omega}} \; -$$

характеристическая функция (х. ф.) случайной величины $Z(\mathbf{y}\,|\,\mathbf{x}, \mathbf{x}')$, $Z(\mathbf{y}\,|\,\mathbf{x}, \mathbf{x}') = \ln\left(p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}') / p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) \right)$, черта сверху означает усреднение по распределению (ф.п.в) $p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x})$. Вычисление правой части выражения (3) выполняется с использованием методов численного интегрирования; при этом главная задача состоит в вычислении значений функции $D(\omega)$. Для каналов без памяти эта задача решена [1, 3]; в настоящей работе приводится описание подхода к ее решению для канала с памятью, задаваемого моделью с детерминированными переходами (1). Для модели с детерминированными переходами (1) каждая сумма по $s^{(0)}$, $s^{(1)}, \ldots,$ $s^{(N)}$ в (2) содержит только одно слагаемое. Следовательно, $p_{\mathbf{y}|\mathbf{x}}(\mathbf{y}\,|\,\mathbf{x}) = \prod_{n=1}^{N} p_{y|xs}(y^{(n)}\,|\,x^{(n)}, s^{(n-1)})$ при этом последовательность переходов в множестве состояний $s^{(0)} \to s^{(1)} \to \ldots \to s^{(N)}$ однозначно определяется кодовым словом $\mathbf{x} = (x^{(1)}, x^{(2)}, ..., x^{(N)})$. Отсюда следует, что

$$C_Z(\omega; \mathbf{x}, \mathbf{x}') = \prod_{n=1}^{N} c_z(\omega; x^{(n)}, s^{(n-1)}, x'^{(n)}, s'^{(n-1)}),$$

где $c_z(\omega, x, s, x', s') = \overline{\left(p_{y|xs}(y \mid x', s') / p_{y|xs}(y \mid x, s)\right)^{j\omega}}$, и черта сверху означает усреднение по условной вероятности (ф.п.в.) $p_{y|xs}(y \mid x, s)$. Поэтому для функции $D(\omega)$ можно записать, что

$$D(\omega) = \sum_{\mathbf{x}} \sum_{\mathbf{x}'} \prod_{n=1}^{N} c_z(\omega; x^{(n)}, s^{(n-1)}, x'^{(n)}, s'^{(n-1)}). \qquad (4)$$

В дальнейшем рассмотрении мы используем понятия решетчатой диаграммы [4] для описания кода и канала. Пусть $\Omega_c = \{V_c, E_c, X\}$ – решетка, задающая блоковый код, где V_c, E_c, X – множество вершин, множество ребер и множество меток ребер (алфавит кода) соответственно. Множество ребер E состоит из троек $e = (v, v', x)$, $v, v' \in V_c$, $x \in X$. Множество вершин V_c кодовой решетки разделяется на непересекающиеся подмножества как

$$V_c = V_c^{(0)} \cup V_c^{(1)} \cup \ldots \cup V_c^{(N-1)} \cup V_c^{(N)},$$

где каждое множество $V_c^{(n)}$ образует вершины n-го уровня диаграммы, $n = 0, 1, 2, \ldots, N$. При этом каждое ребро $e \in E_c$ начинается в вершине из $V_c^{(n))}$ и заканчивается в вершине из $V_c^{(n+1)}$, и каждая вершина $v \in V_c$ лежит хотя бы на одном из путей от вершины из множества $V_c^{(0)}$ до вершины из множества $V_c^{(N)}$. Обозначим $\Sigma_c^{(n)} = \{0, 1, \ldots, \left|V_c^{(n)}\right| - 1\}$. Будем считать, что зафиксировано взаимнооднозначное соответствие $V_c^{(n)} \leftrightarrow \Sigma_c^{(n)}$, обозначаемое как $\Sigma_c(v) = k$, $v \in V^{(n)}$, $0 \le k \le |V_c^{(n)}| - 1$. Тогда элементы множества $\Sigma_c^{(n)}$ представляют собой индексы вершин n-го уровня. Аналогичным образом может быть определена решетка $\Omega_{ch} = \{V_{ch}, E_{ch}, X\}$, описывающая канал, множества $\Sigma_{ch}^{(n)}$ и отображения $\Sigma_{ch}(v)$. Заметим, что в решетке Ω_{ch} из каждого узла выходит $|X|$ ребер, отмеченных различными символами кодового алфавита X. Абстрактные иллюстративные примеры решетчатых диаграмм Ω_c и Ω_{ch} приведены на рис. 1.

Введем композицию решеток Ω_c и Ω_{ch}, обозначаемую как $\Omega = \Omega_c \circ \Omega_{ch}$. Эта композиция представляет собой решетку, в которой вершины задаются парами (v_c, v_{ch}), $v_c \in V_c$, $v_{ch} \in V_{ch}$, а ребра имеют вид $((v_c, v_{ch}), (v_c', v_{ch}'), x)$, если:

1) $v_c \in V_c^{(n-1)}$, $v_c' \in V_c^{(n)}$, $v_{ch} \in V_{ch}^{(n-1)}$, $v_{ch}' \in V_{ch}^{(n)}$, и

2) $(v_c, v_c', x) \in E_c^{(n)}$, $(v_{ch}, v_{ch}', x) \in E_{ch}^{(n)}$.

Очевидно, что $\Omega \subseteq \Omega_c \times \Omega_{ch}$. Пример решетки $\Omega = \Omega_c \circ \Omega_{ch}$ также показан на рис. 1. Для получения выражения для функции $D(\omega)$, заданной равенством (4), используется подход, ранее использовавшийся в [3 – 5].

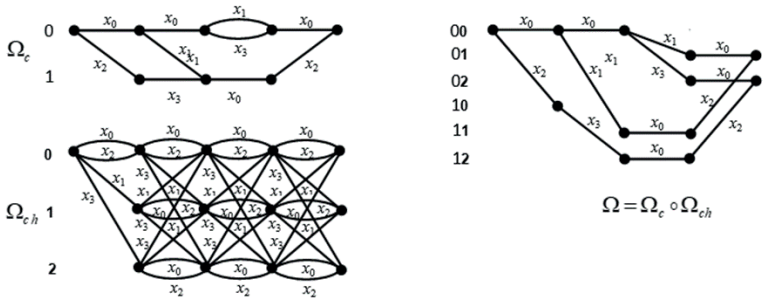


Рис. 1. Примеры решеток Ω_c *и* Ω_{ch} *(слева) и композиции* $\Omega = \Omega_c \circ \Omega_{ch}$ *(справа)*

Чтобы построить функцию $D(\omega)$ надо рассмотреть все пары кодовых слов **x**, **x**′, или все возможные пары путей в решетчатой диаграмме $\Omega = \Omega_c \circ \Omega_{ch} = (V, E, X)$. Суммирование по **x** и **x'** в выражении (4) соответствует суммированию по всем путям в решетке $\Omega^2 = \Omega \times \Omega = (V \times V, E_2, \{c_z(\omega, x, s, x', s')\})$, в которой любое ребро задано как $((v_1, v_2), (v_1', v_2'), c_z(\omega, x, s, x', s'))$, если в решетке Ω соответствующие ребра на одном уровне решетки имеют вид $(v_1, v_2, x) \in E^{(n)}$ и $(v_1', v_2', x') \in E^{(n)}$, $x, x' \in X$ при этом величины s и s' в выражении для метки ребра $c_z(\omega, x, s, x', s')$ определяются как $s = \Sigma_{ch}(v_2)$, $s' = \Sigma_{ch}(v_2')$.

Заключительные замечания

В предложенном подходе к вычислению границы вероятности ошибки *точно* вычисляется значение каждого слагаемого в аддитивной границе. Поэтому его применение дает существенное улучшение границы вероятности ошибки для конкретных кодов по сравнению с обычной аддитивной границей в комбинации с границей Чернова. Предложенный подход может быть применен и к известным моделям каналов с памятью с детерминированными переходами в множестве состояний. Характерным примером таких каналов может служить модель с линейной и нелинейной интерференцией. Заметим, что важнейшая положительная черта предложенного подхода состоит в его универсальности, что позволяет применить его к любому каналу, заданному указанной моделью, и обеспечить при этом высокую точность оценивания при малых вычислительных затратах.

Библиографический список

1. Trofimov A. N., Taubin F. A. Evaluation of the Union Bound Using Characteristic Functions for Coded Transmission over Memoryless Channels // 2021

Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2021. P. 1–6. DOI: 10.1109/WECONF51603.2021.9470730.

2. Arnold D. M., Loeliger H.-A., Vontobel P. O., Kavcic A., Wei Zeng. Simulation-Based Computation of Information Rates for Channels with Memory // IEEE Trans. Inf. Theory. Aug, 2006. Vol. 52, No 8. Pp. 3498–3508.

3. Трофимов А. Н., Таубин Ф. А. Вычисление аддитивной границы вероятности ошибки декодирования с использованием характеристических функций // Информационно-управляющие системы. 2021. № 4. С. 71–85. DOI:10.31799/1684-8853-2021-4-71-85.

4. Vardy A. Trellis Structures of Codes // Handbook of Coding Theory. Ed. V. S. Pless and W. C. Huffman. Elsevier, Amsterdam. 1998. Vol. 2. 1106 p. Ch. 24.

УДК 629.735.33

С. Г. Фомичева*
кандидат технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОПЕРАТОРЫ ТОФФОЛИ В АРИФМЕТИЧЕСКИХ ОПЕРАЦИЯХ С МНОГОРАЗРЯДНЫМИ КВАНТОВЫМИ РЕГИСТРАМИ

В статье рассмотрены особенности выполнения арифметических операций в квантовых системах. Предложена схема построения *k*-управляющих гейтов при использовании стандартного универсального базиса квантовых вычислений: оператор Тоффоли и оператор Адамара.
***Ключевые слова*:** квантовый регистр, оператор Тоффоли, оператор Адамара, модификатор управления.

S. G. Fomicheva*
PhD, Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

THE TOFFOLI OPERATORS IN ARITHMETIC OPERATIONS WITH MULTI-QUBIT QUANTUM REGISTERS

The article discusses the features of performing arithmetic operations in quantum systems. Methods for constructing k-control gates using the standard universal basis of quantum computing are proposed: the Toffoli operator and the Hadamard operator.
Keywords: quantum register, Toffoli operator, Hadamard operator, control modifier.

Введение

Для реализации квантовых вычислений используются унитарные операторы (*gates*), изменяющие в процессе их использования состояния квантовых объектов (кубитов, кутритов). Управление вычислениями при этом выполняется операторами, имеющими два или более входов, среди которых часть входов являются управляющими, а оставшаяся часть – управляемыми входами. Для этого в большинстве квантовых схем используется модификатор управления [1], который позволяет некоторому квантовому оператору срабатывать в зависимости от состояния кубита управления. Когда управляющий кубит находится в состоянии $|1\rangle$, целевой кубит(ы) претерпевает требуемое унитарное преобразование. Напротив, никакие операции не выполняются, если кубит управления находится в базовом состоянии $|0\rangle$. Если управляющий кубит находится в состоянии суперпозиции, то результирующая операция следует из линейности унитарного преобразования. С помощью модификатора управления можно реализовать любой унитарный оператор. При этом они обозначаются с приставкой «*C*», например. *CZ, CY, CCNOT*. В частности, модификатор управления превращает гейт *CNOT* в гейт Тоффоли (*Toffoli gate*), также известный как вентиль с двойным управляемым *NOT* (*CCX* или *CCNOT*). В результате гейт Тоффоли имеет два управляющих кубита и один управляемый кубит (цель). Он применя-

ет *NOT* к цели только тогда, когда оба элемента управления находятся в состоянии $|1\rangle$. Следует отметить, что гейт Тоффоли с вентилем Адамара (*H*) – это универсальный набор операторов (базис) для квантовых вычислений [1], т. е. с их помощью может быть реализована любая квантовая схема.

Не все квантовые симуляторы в наборе свих инструментов содержат возможность создавать *k*-управляющие гейты, например, популярный ресурс IBM *Compositor* [2] позволяет из *X*-гейта создать только гейт Тоффоли. Это затрудняет формирование квантовых схем с длинными квантовыми регистрами, в которых *k*-управляющие гейты используются повсеместно [4–5]. В данной статье предложена схема построения *k*-управляющих гейтов при использовании стандартного универсального базиса квантовых вычислений: оператор Тоффоли (*CCNOT*) + оператор Адамара (*H*).

Особенности арифметических операций в квантовых системах

При реализации квантовых алгоритмов повсеместно возникает потребность применять арифметические операции к регистрам кубитов, находящихся как в базовых состояниях, так и в суперпозиции. В квантовых приложениях входные регистры часто находятся в суперпозиции, и квантовые арифметические операции должны воздействовать на все значения в суперпозиции (квантовый параллелизм). Поэтому при построении различных квантовых схем, использующих арифметические и логические операции, требуется учитывать следующее:

1. Особенности перемещений и невозможность копирования кубитов. Квантовая вычислительная система может перемещать кубиты с использованием команд, меняющих их местами с другими кубитами (например, используя гейт SWAP), при этом копирование (клонирование) принципиально невозможно. В результате оператор присваивания, не может использоваться для присваивания одного состояния кубита другому.

2. Требование обязательной обратимости квантовый операций и очистки данных. В отличие от многих традиционных логических операций, основные квантовые операции (кроме инициализации и измерения) обратимы в силу законов квантовой механики. Поэтому квантовые гейты являются унитарными операторами. Простейший способ реализации любой традиционной схемы в квантовой системе заключается в замене ее эквивалентной традиционной схемой, использующей **только обратимые операции**.

Рис. 1. Квантовая схема реализации операций инкремента и декремента

Рассмотрим две простейшие целочисленные арифметические операции, которые предназначены для увеличения на 1 (инкремент) и уменьшения на 1 (декремент) числа. Соответствующая квантовая схема для регистра из трех кубитов представлена на рис. 1.

Шаг 1. Инициализация регистра кубитов и подготовка входных данных

В квантовых системах инициализация необходима вследствие как вероятностного характера самих квантовых вычислений, так и из-за влияния шумов и эффектов декогеренции. Поэтому, не являясь частью операции инкремента (декремента), процесс инициализации кубита в базовом состоянии перед началом вычислений обязателен. На рис. 1 инкрементируемым числом является 1, которая получена инвертированием кубита q_0. После инициализации и подготовки начального значения квантовый регистр хранит значение 1 (младшим на квантовой схеме является верхний кубит).

Шаг 2. Реализация инкремента числа. Как видно из рис. 1. операция инкремента реализована тремя гейтами (Тоффоли*, CNOT и X).* В результате выполнения шага 2 квантовый регистр хранит значение 2=1+1. По сути, выполняя операцию инкремента, реализуется «сложение столбиком» двоичных чисел с переносом разрядной единицы. Так гейт Тоффоли проверяет: если кубит q_0 находится в состоянии $|1\rangle$ и кубит q_1 находится в состоянии $|1\rangle$, то разрядная единица была бы «перенесена» в кубит q_2. Далее гейт *CNOT* проверяет выход гейта Тоффоли и также, если кубит q_0 находится в состоянии $|1\rangle$, то инвертирует состояние кубита q_1. На заключительном шаге инвертируется состояние самого младшего кубита.

Шаг 3. Чтобы выполнить операцию декремента, зеркально отражаем схему инкремента. Схема рис. 1 удовлетворяют всем требованиям, предъявляемым к квантовыми алгоритмам, в частности:

- **Обратимость.** Операция декремента представляет собой операцию инкремента, выполненную в обратном порядке составляющих операций.
- **Операция с суперпозицией**. Реализация инкремента корректно работает со входными данными в суперпозиции. Установив в состояние суперпозиции кубит q_1, результаты вычислений подтверждают корректность выполняемых операций.

Гейты Тоффоли в арифметических операциях на длинных квантовых регистрах

Операция инкремента может быть реализована и для более «длинных» квантовых регистров. Поэтому предлагается эквивалентная схема (рис. 2), позволяющая на базе операторов Тоффоли реализовать унитарный оператор *CCCNOT*.

Чтобы реализовать эквивалентную схему для *CCCNOT* требуется обязательный вспомогательный кубит, который необходимо инициализировать в базовое состояние $|0\rangle$. Используя эквивалентную схему для гейта *CCCNOT* становится возможной реализация более сложных квантовых схем в IBM *Quantum Composer*.

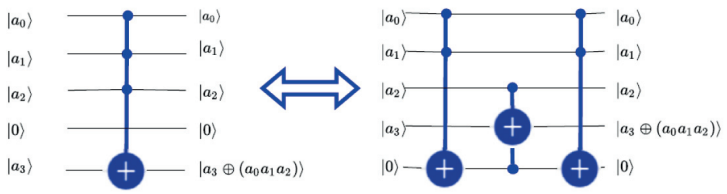


Рис. 2. Эквивалентные схемы для CCCNOT-гейта

Например, приведем реализацию операции вычитания 2-квантовых 3-разрядных чисел. Вычитание реализуется, как сложение двух слагаемых, одно из которых отрицательное. Чтобы получить из положительного числа отрицательное, его нужно инвертировать, получив дополнительный код. и прибавить единицу к младшему разряду (рис. 3). Как показано на рис. 3, имеются два регистра *A* и *B* (в каждом из них теоретически может храниться суперпозиция целых значений), и необходимо выполнить операцию арифметического сложения. При выполнении арифметического слежения (вычитания) на традиционных компьютерах данная операция *(C=A+B)* необратима, т. е. имея на выходе алгоритма сумму, нельзя однозначно сказать, чему были равны слагаемые (таких вариантов может быть много!). Чтобы обойти это ограничение, реализован оператор инкремента на заданное значение *A+=B*. Получив в регистре *A* результат сложения и не меняя состояния регистра *B*, получаем обратимую операцию.

Хотя служебные кубиты часто необходимы, как в нашем случае (вспомогательный) кубит на схеме рис. 3, они обычно входят в состояние квантовой запутанности. При этом возникают две проблемы: служебные кубиты редко оказываются в чисто нулевом состоянии.

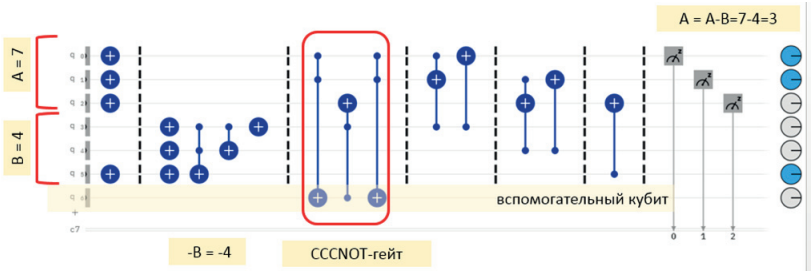


Рис. 3. Квантовая схема вычитания двух 3-кубитных чисел

И это является недостатком, так как служебные кубиты приходится сбрасывать, чтобы они могли снова использоваться в дальнейшей работе. Во-вторых, поскольку использование служебных кубитов почти всегда приводит к их запутанности с кубитами выходного регистра, выполнение операции измерения с ними может иметь катастрофические последствия для выходного со-

стояния всей квантовой системы. Однако, существует прием, решающий эту проблему: он называется *отменой вычислений (uncomputing).* Концепция отмены вычислений заключается в обращении операций, приведших к запутанности служебного кубита, и возврате его в исходное незапутанное состояние $|0\rangle$.

Заключение

В статье рассмотрены особенности выполнения арифметических операций в квантовых системах. Базируясь на требованиях, предъявляемых к квантовым системам, предложены методы построения *k*-управляющих гейтов при использовании стандартного универсального базиса квантовых вычислений: оператор Тоффоли (*CCNOT*) + оператор Адамара (*H*). Приведены примеры использования разработанных эквивалентных квантовых схем при выполнении арифметических операций в квантовых системах.

Библиографический список

1. Холево А. С. Квантовые системы, каналы, информация. М.: МЦНМО, 2014. 327 с.

2. Симуляторы IBM Quantum. IBM Quantum simulators. URL: https://quantum-computing.ibm.com/lab/docs/iql/manage/simulator/ (дата обращения: 24.02.2022).

3. Фомичева С. Г. Теоретические аспекты квантования баз знаний в мультиагентных системах // Информационно-управляющие системы. 2017. № 3(88). С. 2–10.

4. Fomicheva S. Soft quantization of the production’s knowledgebases for multi-agent systems. В сборнике: Conference of Open Innovation Association, FRUCT. Proceedings of the 20th Conference of Open Innovations Association, FRUCT 2017. С. 69–76. DOI: 10.23919/FRUCT.2017.8071294.

УДК 629.735.33

С. Г. Фомичева*
кандидат технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

СИМУЛЯЦИЯ СОСТОЯНИЙ ЗАПУТАННОСТИ В КВАНТОВЫХ РЕГИСТРАХ

В статье приведены результаты проведенной автором серии экспериментов в IBM *Quantum* с целью исследовать состояния запутанности кубитов. Продемонстрировано, что для корректного извлечения информации о кубитах, находящихся в состоянии запутанности требуются механизмы синхронизации измерений на передающей и принимающей стороне.
***Ключевые слова*:** квантовый регистр, квантовая запутанность, состояния Белла, состояние суперпозиции.

S. G. Fomicheva*
PhD, Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation

SIMULATION OF ENTANGLEMENT STATES IN QUANTUM REGISTERS

The paper presents the results of the author experimental series in IBM Quantum in order to investigate the states of qubit's entanglement. It is demonstrated that mechanisms for synchronizing measurements on the transmitting and receiving sides are required for the correct extraction of information about qubits in the entanglement state.
Keywords: quantum register, quantum entanglement, Bell's states, superposition state.

Введение

Экспоненциальный рост объемов, обрабатываемых информационными системами, данных и невозможность за адекватное время реализовать многие поисковые и вычислительные алгоритмы привели к стремительному развитию квантовых вычислительных систем. Логические квантовые схемы реализуются квантовыми вентилями (гейтами), каждый из которых является унитарным оператором над гильбертовым пространством [1]. Квантовые схемы из двух или более кубитов принято называть квантовыми регистрами. Каждый кубит квантового регистра меняет свое состояние в ходе квантовых вычислений. Следует особо отметить, что квантовое состояние кубита может изменяться во времени двумя принципиально различными путями: применением унитарного квантового оператора и измерением (наблюдением за состоянием кубита).

Принципиальная разница от традиционных вычислительных процессов заключается в том: что унитарная операция, по определению, является обратимой, а измерение, является необратимой операцией. При измерении происходит, так называемый, коллапс волновой функции

$$|\varphi\rangle = \sum_{j=0}^{N-1} \lambda_j |j\rangle$$

где $|\varphi\rangle$ – текущее состояние квантового объекта (кубита), λ_j –комплексное число, обозначающее амплитуду вероятности того, что в результате измерения квантовый объект будет находиться в базовом состоянии $|j\rangle$, а N – количество базовых состояний квантового объекта) в следствии шумов и эффекта декогеренции квантовый объект «схлопывается» до одного их своих граничных состояний.

Именно данный коллапс приводит к невозможности выполнять промежуточные измерения в ходе квантовых вычислений, а в классическом компьютере промежуточные измерения являются обычным делом, не нарушающим вычислительного процесса. Запутанное состояние двух кубитов может быть достигнуто с помощью использования гейта Адамара *(H*) на управлявшем кубите, за которым следует гейт *CNOT*. В результате генерируется особое состояние максимально запутанных двух кубитов, известное как *состояние Белла*, названное в честь Джона Стюарта Белла [1–3].

Состояние запутанности является основополагающим явлением всех квантовых систем. Эффекты запутанности лежат в основе принципов передачи информации в квантовых системах, а также используются как сохраняемый ресурс, расходуемый в отложенном временном промежутке для телепортации кубитов и реализации сверхплотного кодирования информации [4], а также в алгоритмах квантования знаний [3]. Поэтому важно понимать, как меняются состояния кубитах при создании запутанных пар и групп кубитов большего их количества.

В данной статье приведены результаты проведенных автором исследований состояний кубитов на квантовой системе IBMQ_*manila* [2], в которой применяется физический тип кубита, называемый сверхпроводящим трансмон-кубитом *(superconducting transmon qubit*). Данные физические реализации кубитов сделаны из сверхпроводящих материалов, таких как ниобий и алюминий, нанесенных на кремниевую подложку.

Исследование состояний Белла при измерении отдельных кубитов

Всего существует четыре состояний Белла (или ЭПР состояний, названных также в честь Эйнштейна, Подольского и Розена, которые первыми указали на необычные свойства этих состояний) [1]. С целью исследовать, как проявляется квантовая запутанность, была проведена серия экспериментов. В регистре $|mn\rangle=|q_0q_1\rangle$ кубит *n* будем считать, что он имеет нулевой номер, а кубит *m* – первый номер (рис. 1). Схема на рис.1, *а* состоит из U_{CNOT} – квантового гейта *CNOT*, на управляющий вход которого помещен гейт Адамара (*H*).

Оператор *L*, описывающий эту квантовую схему (*I* – единичная матрица), имеет вид:

$$L = (I \otimes H) \cdot U_{CNOT} \cdot$$

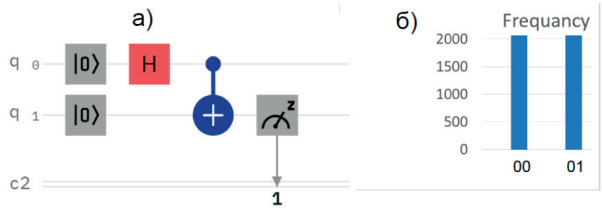


Рис. 1. Состояние Белла (а) и частоты состояний (б) при z-измерении на кубите 0

Чтобы исследовать состояния Белла для отдельных кубитов регистра $|mn\rangle=|q_0q_1\rangle$, сформулирован ряд вопросов, на которые экспериментально получены ответы:

1) Каково состояние нулевого и первого кубита в стандартном базисе?
2) Каково состояние нулевого и первого кубита в базисе суперпозиции?

Для ответа на первый вопрос, реализована на квантовом процессоре *Falcon r*5.11 схема, отображенная на рис. 1, *а*. Выполнив 4096 запусков схемы на квантовой системе *ibmq_manila*, использующей квантовый процессор *Falcon r*5.11/*Version*: 1.0.20, получены результаты реализации данной квантовой схемы, отображенные на рис. 1, *б*. Как видно из рис.1, *б*, результат случайный: в половине случаев нулевой кубит (он находится справа и соответствует младшему кубиту в регистре) находится в $|0\rangle$, а в другой половине зафиксировано базовое состояние $|1\rangle$.

Рис. 2. Состояние Белла + X – измерение на кубите 0

Отвечая на второй вопрос, измерен нулевой кубит в другом базисе (рис. 2), чтобы отличать состояние суперпозиции от состояния запутанности, и получены результаты выполнения (рис. 3).

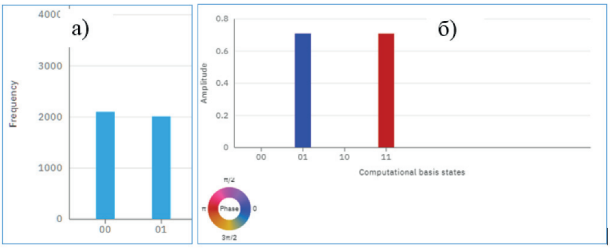


Рис. 3. Частоты (а) и вектор состояния (б) Белла + X-измерения на кубите 0

В этом случае результат также остается случайным. Это говорит о том, что на самом деле при измерении состояния одного из кубитов квантового регистра нам ничего не известно о состоянии нулевого кубита. Аналогичные результаты получены при проверке первого кубита.

По результатам данных экспериментов может быть сделан промежуточный вывод – изолированное измерение одного из кубитов запутанной пары не позволяет отличить состояние запутанности пары кубитов от состояния суперпозиции отдельных кубитов квантового регистра.

Исследование состояний Белла квантового регистра при синхронных измерениях

Теперь одновременно измерим оба кубита регистра $|mn\rangle=|q_0q_1\rangle$ в общем вычислительном (ZZ) базисе и XX-базисе, отвечая на следующие вопросы (рис. 4):

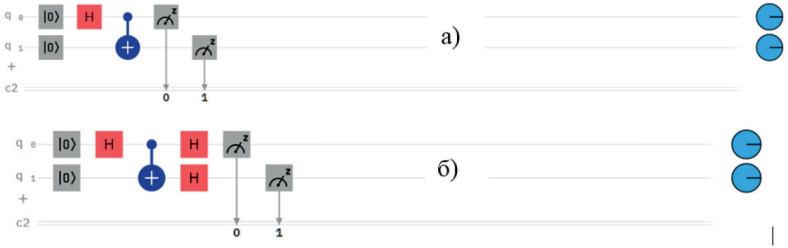


Рис. 4. Состояние Белла + ZZ-измерение (а) и XX – измерение(б) на двух кубитах

1) Каково состояние обоих кубитов в стандартном базисе?
2) Каково состояние обоих кубитов в базисе суперпозиции?

На рис. 5 видно, что независимо от базиса измерения, с большой вероятностью, если кубит q_0 находится в состоянии 0, то кубит q_1 также будет находится в 0, то же самое, если кубит q_0 находится в состоянии 1, то кубит q_1 также будет находится в 1. Они идеально коррелированы! Измерения в базисе XX также подтверждают их «сильную корреляцию».

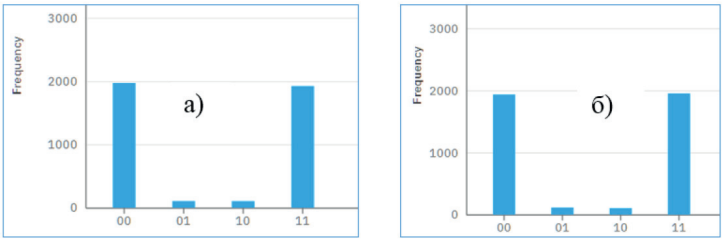


Рис. 5. Вектор состояния Белла + ZZ-измерение (а) и XX-измерение(а) на двух кубитах

Следовательно, если измеряется q_0 в состоянии $|0\rangle$, то q_1 тоже находится в этом состоянии $|0\rangle$, аналогично, если q_0 измеряется в состоянии $|1\rangle$, q_1 также находится в этом состоянии $|1\rangle$, (в любом базисе измерения).

Следует отметить, что возможно трехкубитное обобщение состояний Белла, называемое GHZ-состоянием. Их формальное представление задается выражением $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$. Существуют и другие схемы запутывания трех и более кубитов. В частности, в Китае успешно запутаны 18 кубитов, а также австрийские и китайские ученые смогли запутать кутриты (квантовые объекты с тремя граничными состояниями) и передать с помощью них информацию на расстояние 1200 километров [4].

Заключение

В статье приведены результаты проведенных автором серии экспериментов с целью исследовать состояния запутанности кубитов. Результаты проведенных экспериментом показали, что *изолированное* измерение одного из кубитов запутанной пары не позволяет отличить состояние запутанности пары кубитов от состояния суперпозиции отдельных кубитов квантового регистра. Также для корректного извлечения информации о кубитах, находящихся в состоянии запутанности требуются механизмы синхронизации измерений на передающей и принимающей стороне. Как правило, на сегодняшний день такие механизмы реализуются с помощью классических (не квантовых) каналов связи.

Библиографический список

1. Холево А. С. Квантовые системы, каналы, информация. М.: МЦНМО, 2014. 327 с.

2. Симуляторы IBM Quantum. IBM Quantum simulators. URL: https://quantum-computing.ibm.com/lab/docs/iql/manage/simulator/ (дата обращения: 24.02.2022).

3. Фомичева С. Г. Теоретические аспекты квантования баз знаний в мультиагентных системах // Информационно-управляющие системы. 2017. № 3 (88). С. 2–10.

4. Yi-Han Luo, Han-Sen Zhong, Manuel Erhard, Xi-Lin Wang, Li-Chao Peng, Mario Krenn, Xiao Jiang, Li Li, Nai-Le Liu, Chao-Yang Lu, Anton Zeilinger, and Jian-Wei Pan, Quantum Teleportation in High Dimensions. Phys. Rev. Lett. 123, 070505. Published 15 August 2019 URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.123.070505 (дата обращения: 14.03.2022).

УДК 621.396.96

Д. А. Шепета*
кандидат технических наук, доцент
В. В. Боженко*
ассистент
Е. Н. Долгов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АЛГОРИТМ МОДЕЛИРОВАНИЯ КОРРЕЛИРОВАННЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, РАСПРЕДЕЛЕННЫХ ПО ЗАКОНУ ВЕЙБУЛЛА

Синтезированы алгоритмы моделирования коррелированных числовых последовательностей, распределенных по закону Вейбулла. Приведены аналитические выражения, связывающие статистические характеристики моделируемых последовательностей со статистическими характеристиками «порождающих» нормальных последовательностей.
Ключевые слова: математическое моделирование, распределение Вейбулла, статистические характеристики, корреляция, двумерный закон распределения.

D. A. Shepeta*
PhD, Tech., Associate Professor
V. V. Bozhenko*
Assistant
E. N. Dolgov*
Student
*St. Petersburg State University of Aerospace Instrumentation

ALGORITHM FOR MODELING CORRELATED NUMERICAL SEQUENCES WITH WEIBULL DISTRIBUTION

Algorithms for modeling Weibull distributed correlated numerical sequences are described. Analytical expressions that connect the statistical characteristics of the simulated sequences with the statistical characteristics of the "generating" normal sequences are given.
Keywords: mathematical modeling, Weibull distribution, statistical characteristics, correlation, two-dimensional distribution law.

Введение

Распределение Вейбулла широко используется в научных исследованиях, связанных с изучением экстремальных значений, для описания флюктуаций локационных сигналов, отраженных от подстилающей земной поверхности и т. д. [1, 2]. В настоящее время это распределение широко используется при имитационном моделировании, связанном с изучением отражений локационных сигналов от разных видов земной поверхности [3, 4].

Моделирование последовательностей независимых случайных величин, распределенных по закону Вейбулла, не представляет никаких сложностей, поскольку функции генерации этого распределения входят во все математические пакеты. Однако, когда необходимо моделировать последовательности коррелированных случайных величин, распределенных по закону Вейбулла, то синтез такого алгоритма, уже не столь прост [5].

Ввиду многообразия земных поверхностей и, следовательно, многообразия корреляционных зависимостей, обобщенная модель отражений, учитывающая корреляцию отраженных локационных сигналов, с целью универсальности, загрубляется [6]. Модель учитывает лишь ширину энергетического спектра отраженных сигналов, которая является одним из наиболее информативных параметров при классификации земных поверхностей.

При моделировании корреляционных зависимостей это эквивалентно учету ширины нормированной корреляционной функции флюктуаций на некотором уровне. Подобное загрубление математической модели отражений позволяет для синтеза алгоритмов моделирования использовать лишь двумерную плотность распределения Вейбулла.

Семейство распределений Вейбулла

Распределение Вейбулла в общем виде можно записать как [4]

$$f_W(x) = \alpha_W \lambda_W x^{\alpha_W - 1} \exp\left(-\lambda_W x^{\alpha_W}\right), x > 0, \tag{1}$$

где α_W – параметр формы, а λ_W – параметр масштаба распределения.

Математическое ожидание и дисперсия выражаются как:

$$\begin{cases} m_W = M(x) = \dfrac{\lambda_W^{-\frac{1}{\alpha_W}}}{\alpha_W} \cdot \Gamma\left(\dfrac{1}{\alpha_W}\right), \\ D_W = D(x) = \lambda_W^{-\frac{2}{\alpha_W}} \cdot \left[\dfrac{2}{\alpha_W}\Gamma\left(\dfrac{2}{\alpha_W}\right) - \dfrac{1}{\alpha_W^2}\Gamma^2\left(\dfrac{1}{\alpha_W}\right)\right], \end{cases} \tag{2}$$

где $\Gamma(\cdot)$ – гамма функция.

Частными случаями распределения Вейбулла являются экспоненциальное распределение и распределение Рэлея, которые следуют из выражения (1) при параметрах формы α_W равных $\alpha_W = 1$ и $\alpha_W = 2$, соответственно.

Распределение Рэлея и экспоненциальное распределение широко используются в теоретических исследованиях, поскольку они представляют плотности распределения вероятностей огибающей $A(t)$ и квадрата огибающей $P(t)$ узкополосного стационарного нормального случайного процесса $\xi(t)$ [7].

$$\xi(t) = U(t)\cos\omega_0 t + V(t)\sin\omega_0 t, \tag{3}$$

$$\begin{cases} A(t) = \sqrt{U^2(t) + V^2(t)}, \\ P(t) = A^2(t) = U^2(t) + V^2(t), \end{cases} \tag{4}$$

где $U(t)$ и $V(t)$ – синусная и косинусная квадратуры процесса $\xi(t)$, соответственно, а ω_0 – центральная частота его энергетического спектра.

Квадратуры $U(t)$ и $V(t)$ распределены нормально с нулевыми средними значениями $m_U = m_V = 0$ и равными дисперсиями $\sigma_U^2 = \sigma_V^2 = \sigma^2$.

Квадрат огибающей $P(t)$ случайного процесса $\xi(t)$, пропорциональный мощности процесса, имеет экспоненциальное распределение [5]:

$$f_P(x) = f_W(x) = \lambda_W \exp(-\lambda_W x) = \frac{1}{\sigma^2}\exp\left(-\frac{x}{\sigma^2}\right), x > 0, \tag{5}$$

$$\begin{cases} m_P = m_W = M(x) = \dfrac{1}{\lambda_W} = \sigma^2, \\ D_P = D_W = D(x) = \dfrac{1}{\lambda_W^2} = \sigma^4. \end{cases} \tag{6}$$

В выражениях (5) и (6) приняты обозначения параметров закона Вейбулла традиционно используемые при описании экспоненциального распределения.

Для распределений $A(t)$ и $P(t)$ в литературе приведены двумерные плотности распределения, учитывающие корреляционные характеристики этих процессов. Наиболее простые выражения получаются при использовании двумерного экспоненциального закона, который является частным случаем распределения Вейбулла с параметром формы $\alpha_W = 1$.

Двумерное экспоненциальное распределение записывается в виде [7]:

$$f_W(x_1, x_2) = f_P(x_1, x_2) =$$
$$= \frac{1}{4\sigma^4(1-R^2)}\exp\left\{\frac{x_1 + x_2}{2\sigma^2(1-R^2)}\right\} \times I_0\left[\frac{R\sqrt{x_1 x_2}}{\sigma^2(1-R^2)}\right], \quad x_1 > 0, \quad x_2 > 0, \tag{7}$$

где R – коэффициент корреляции случайных величин x_1 и x_2. В работе [7] показано, что двумерная плотность распределения вероятностей $f_W(x_1, x_2) = f_P(x_1, x_2)$ квадрата огибающей случайного процесса $\xi(t)$ связана с нормированной корреляционной функцией $r(\tau)$ квадратур $U(t)$ и $V(t)$ функциональной зависимостью $R(\tau) = r^2(\tau)$.

Выражения, приведенные выше, позволяют записать алгоритм моделирования отсчетов процесса $P(t)$, связанных корреляционной зависимостью $R(\tau)$, при использовании отсчетов двух независимых нормальных процессов $U(t)$ и $V(t)$.

Алгоритм моделирования последовательности коррелированных случайных величин, распределенных по экспоненциальному закону

Рассмотрим отсчеты двух независимых стационарных процессов $U(t)$ и $V(t)$:

$$\begin{cases} \mathbf{U}(t) = \left(U(t_1), U(t_2), \ldots U(t_k), \ldots\right) = (U_1, U_2, \ldots U_k, \ldots), \\ \mathbf{V}(t) = \left(V(t_1), V(t_2), \ldots V(t_k), \ldots\right) = (V_1, V_2, \ldots V_k, \ldots). \end{cases} \quad (8)$$

Эти отсчеты, при каждом фиксированном моменте времени t, распределены нормально.

Пусть нормированная корреляционная функция $r(\tau)$ процессов $U(t)$ и $V(t)$ определяется выражением

$$r(\tau) = r(\tau = \Delta_\tau |i-j|) = r_{|i-j|} = \exp\left(-\alpha^* \cdot \Delta_\tau |i-j|\right) = \exp\left(-\alpha |i-j|\right) = r_{|i-j|}. \quad (9)$$

где $r = r_1$ – коэффициент корреляции между двумя соседними отсчетами последовательностей $\mathbf{U}_k = (U_1, U_2, \ldots, U_k)$ и $\mathbf{V}_k = (V_1, V_2, \ldots, V_k)$. Тогда плотность распределения вероятностей нормальных векторов $\mathbf{U}_k$ и $\mathbf{V}_k$ может быть представлена в виде [8]:

$$\begin{cases} f(\mathbf{U}_k) = f(U_1) \cdot \prod_{l=2}^{k} f(U_l / \mathbf{U}_{l-1}) = f(U_1) \cdot \prod_{l=2}^{k} f(U_l / U_{l-1}), \\ f(\mathbf{V}_k) = f(V_1) \cdot \prod_{l=2}^{k} f(V_l / \mathbf{V}_{l-1}) = f(V_1) \cdot \prod_{l=2}^{k} f(V_l / V_{l-1}). \end{cases} \quad (10)$$

Из последнего следует, что последовательности $\mathbf{U}_k$ и $\mathbf{V}_k$ – марковские.

Моделирование отсчетов $\mathbf{U}_k$ и $\mathbf{V}_k$ хорошо известно [8]. Алгоритм моделирования последовательности $\mathbf{P}_k = (P_1, P_2, \ldots, P_k)$ можно записать в следующем виде:

$$\begin{cases} U_i = r \cdot U_{i-1} + \sqrt{1-r^2} \cdot \eta_i, \\ V_i = r \cdot V_{i-1} + \sqrt{1-r^2} \cdot \eta_i^*, \\ P_i = U_i^2 + V_i^2, i = 1, 2, \ldots. \end{cases} \quad (11)$$

где η_i и η_i^* – последовательности независимых в совокупности нормальных случайных величин с нулевыми математическими ожиданиями и дисперсиями σ^2, $U_0 = \eta_0$, $V_0 = \eta_0^*$.

Последовательность отсчетов $\mathbf{P}_k$ – числовая последовательность коррелированных экспоненциально распределенных случайных со средними значениями и дисперсиями, определенными выражением (2) и коэффициентами корреляции равными

$$R_{|i-j|} = r^{2|i-j|}.$$

Следует отметить, что подобная корреляционная зависимость позволяет учесть только ширину спектра флюктуаций. Учитывая сказанное выше о необходимости «загрубления» данных о корреляционных зависимостях, подобный подход к учету корреляции отсчетов наблюдаемых процессов с практической точки зрения вполне достаточен.

Библиографический список

1. Irvine M. L. Monitoring Coastal Change in Newfoundland and Labrador: 2014 UPDATE // Current Research. 2015. P. 263–276.

2. Исаков В. И. Моделирование локационных сигналов, отраженных от кромки земля-море / В. И. Исаков, Д. А. Шепета // Информационно-управляющие системы. 2017. № 5 (90). С. 89–94.

3. Isakov V. I. Simulation of location signals when determining a coastal edge / V. I. Isakov, D. A. Shepeta // 2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2021.

4. Wattimena G. M. Determination of the coastal edge using on-board radar / G. M. Wattimena, D. A. Shepeta, V. I. Isakov // SPIE FutureSensing Technologies. 2021.

5. Исаков В. И. Плотность распределения мощности огибающей локационных сигналов, отраженных от кромки земля-море / В. И. Исаков, Д. А. Шепета // Обработка, передача и защита информации в компьютерных системах: 21 Международ. науч. конф. (СПб., 14–22 апреля 2021 г.): сб. докл. 2021. С. 25–28.

6. Блаунштейн Н. Ш. Прикладные аспекты электродинамики / Н. Ш. Блаунштейн, М. Б. Сергеев, А. П. Шепета. СПб.: Аграф+, 2016. 272 с.

7. Левин Б. Р. Теоретические основы статистической радиотехники / Б. Р. Левин. М.: Радио и связь, 1989. 656 с.

8. Шепета А. П. Синтез нелинейных формирующих фильтров для моделирования входных сигналов локационных систем // Современная радиолокация. 1994. С. 81–85.

УДК 621.396.96

Д. А. Шепета*
кандидат технических наук, доцент
В. И. Исаков*
кандидат технических наук, доцент
В. А. Тюринова*
магистрант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПРЯМОЙ МЕТОД МОДЕЛИРОВАНИЯ ЛОГАРИФМИЧЕСКИ-НОРМАЛЬНОГО РАСПРЕДЕЛЕНИЯ

Синтезированы алгоритмы моделирования логарифмически-нормальных процессов с заданными корреляционно-спектральными характеристиками на основе прямого вычисления условных плотностей распределения, что позволяет непосредственно использовать встроенные в математические пакеты процедуры и функции генерации последовательностей логарифмически-нормальных случайных величин.
Ключевые слова: моделирование логарифмически-нормальных процессов, заданные корреляционно-спектральные характеристики.

D. A. Shepeta*
PhD, Tech., Associate Professor
V. I. Isakov*
PhD, Tech., Associate Professor
V. A. Tyurinova*
Postgraduate Student
*St. Petersburg State University of Aerospace Instrumentation, SUAI

A DIRECT METHOD FOR MODELING A LOGARITHMIC-NORMAL DISTRIBUTION

Algorithms for modeling logarithmically normal processes with specified correlation and spectral characteristics are synthesized based on direct calculation of conditional distribution densities, which allows direct use of procedures and functions for generating sequences of logarithmically normal random variables built into mathematical packages.
Keywords: modeling of logarithmically normal processes, given correlation and spectral characteristics.

Введение

Логарифмически-нормальное распределение широко используется в научных исследованиях, связанных с изучением экономических зависимостей, для описания флюктуаций эхо-сигналов при локации физических объектов [1, 2], для обработки экспериментальных данных [3, 4] и т. д. Наиболее часто это распределение используется при имитационном моделировании исследуемых систем.

В том, случае, когда необходимо учесть корреляционные зависимости логарифмически-нормальных последовательностей традиционно используют

стандартное нормальное распределение и экспоненциальное функциональное преобразование коррелированных нормальных величин. При таких преобразованиях меняются все статистические характеристики моделируемой «нормальной» последовательности, что не очень удобно при имитационном моделировании. В работе синтезируются алгоритмы моделирования логарифмически-нормальных процессов с заданными корреляционными свойствами прямыми методами вычисления условных плотностей распределения.

Многомерное логарифмически-нормальное распределение

Многомерную логарифмически-нормальную плотность распределение запишем в виде

$$w(\mathbf{X}_M) = \frac{1}{\sqrt{(2\pi)^M D_M \prod_{p=1}^{M} \sigma_p X_p}} \exp\left\{ -\frac{1}{2D_M} \sum_{p=1}^{M} \sum_{q=1}^{M} \frac{D_{pq}}{\sigma_p \sigma_q} \ln \frac{X_p}{\bar{X}_p} \ln \frac{X_q}{\bar{X}_q} \right\}, \quad (1)$$

где $\bar{X}_p$ и σ_p – параметры распределения, связанные с математическими ожиданиями $m_p = M(X_p)$, дисперсиями $\sigma_p^2 = D(X_p)$ и коэффициентами вариации K_p, $p = 1, 2, ..., M$, соотношениями, приведенными в [5]:

$$\begin{cases} M(X_p) = m_p = \bar{X}_p \cdot \exp\left(\dfrac{\sigma_p^2}{2}\right), \\ D(X_p) = \sigma_p^2 = \bar{X}_p^2 \cdot \exp(\sigma_p^2) \cdot \left(\exp(\sigma_p^2) - 1\right), \\ K_p = \sqrt{\exp(\sigma_p^2) - 1}, p - 1, 2, \ldots M, \end{cases} \quad (2)$$

D_M – определитель матрицы $\mathbf{D}_M$, элементами r_{pq} которой являются коэффициенты корреляции логарифмов случайных величин X_p и X_q, $p, q = 1, 2, \ldots, M$, т. е.

$$r_{pq} = \frac{1}{\sigma_p \sigma_q} M\left(\left(\ln X_p - \ln \bar{X}_p\right)\left(\ln X_q - \ln \bar{X}_q\right)\right), \quad (3)$$

D_{pq} – алгебраические дополнения элементов r_{pq} матрицы $\mathbf{D}_M$. Коэффициенты корреляции R_{pq} случайных величин X_p и X_q выражаются через коэффициенты корреляции логарифмов случайных величин r_{pq} по формулам [5, 6]

$$R_{pq} = \frac{1}{K_p K_q}\left[\left(1 + K_p K_q\right)^{r_{pq}} - 1\right], \; p, q = 1, 2, \ldots M. \quad (4)$$

Коэффициенты корреляции r_{pq} и R_{pq} удовлетворяют равенствам $r_{pq} = r_{qp}, R_{pq} = R_{qp}, r_{pp} = R_{pp} = 1, p,q = 1,2,\ldots M$, а матрица $\mathbf{D}_M$ – положительно определенная т. е. $D_M = \det \mathbf{D}_M > 0$.

Моделирование последовательности логарифмически-нормальных случайных величин

Алгоритм моделирования случайных последовательностей, распределенных по логарифмически-нормальному закону, получим прямым вычислением условных плотностей распределения. Прямой метод вычисления состоит в следующем.

Пусть вектор $\mathbf{X}_M = (X_1, X_2, \ldots X_M)$ при произвольном M имеет плотность распределения вероятностей $f(\mathbf{X}_M)$, тогда, полагая, что элементы вектора вычисляются последовательно во времени, можно сразу записать $f(\mathbf{X}_M)$ в виде

$$f(\mathbf{X}_M) = f(X_1) \cdot f(X_2 / X_1) \cdot \ldots \cdot f(X_M / X_{M-1}, X_{M-2}, \ldots X_2, X_1) = \\ = f(X_1) \cdot \prod_{l=2}^{M} f(X_l / \mathbf{X}_{l-1}), \tag{5}$$

где $f(X_l / \mathbf{X}_{l-1}) = f(X_l / X_{l-1}, X_{M-2}, \ldots X_2, X_1)$, т. е. $\mathbf{X}_l = (X_{l-1}, X_{l-2}, \ldots X_1)$, $l = 2, 3, \ldots, M$.

Прямой метод и состоит в моделировании последовательности условно независимых случайных величин $(X_l / \mathbf{X}_{l-1})$, l = 2, 3, …, M, при l = 1 $(X_l / \mathbf{X}_{l-1}) = X_1$.

На практике наиболее часто известен не сам функциональный вид корреляционной функции, а лишь ее длительность τ_δ на некотором уровне δ. В качестве уровня δ чаще всего используется уровень 0,5, поскольку ширина энергетического спектра $\Delta f_{\delta=0.5}$ генерируемой последовательности на уровне δ = 0,5 от максимума приближенно обратно пропорциональна длительности нормированной корреляционной функции на уровне 0,5, т. е. $\Delta f_{0.5} \approx 1 / \tau_{0.5}$.

Кроме того, ограничимся рассмотрением случая равенства коэффициентов вариации, т. е. будем считать, что $K = K_p = K_q$, поскольку при этом ограничении последовательность логарифмически-нормальных случайных величин при неограниченном увеличении M будет представлять собой дискретный марковский случайный процесс. Ограничение $K = K_p = K_q$ не накладывает каких-либо ограничений на изменение средних значений и дисперсий, важно лишь, чтобы отношение среднеквадратического отклонения к математическому ожиданию оставалось постоянным.

При этих ограничениях выражение (5) переписывается в виде

$$f(\mathbf{X}_M) = f(X_1) \cdot f(X_2 / X_1) \cdot f(X_3 / X_2) \cdot \ldots \cdot f(X_M / X_{M-1}) = \\ = f(X_1) \cdot \prod_{l=2}^{M} f(X_l / X_{l-1}), \tag{6}$$

поэтому для синтеза алгоритма моделирования достаточно найти переходную вероятность, определяемую условной плотностью распределения вероятностей, для вычисления которой достаточно знать лишь двумерный закон распределения.

Из выражения (1) получаем двумерную плотность распределения вероятностей

$$f(X_p, X_q) = \frac{1}{2\pi\sigma_p\sigma_q X_p X_q\sqrt{1-r_{pq}^2}}\exp\left\{-\frac{1}{2(1-r_{pq}^2)}\times\right.$$
$$\left.\times\left[\left(\frac{\ln X_p - \ln\overline{X_p}}{\sigma_p}\right)^2 - \left(\frac{\ln X_q - \ln\overline{X_q}}{\sigma_q}\right)^2 - \right.\right.$$
$$\left.\left.-2r_{pq}\left(\frac{\ln X_p - \ln\overline{X_p}}{\sigma_p}\right)\left(\frac{\ln X_q - \ln\overline{X_q}}{\sigma_q}\right)\right]\right\}, \quad (7)$$

из которого следует условная плотность распределения вероятностей

$$f\left(X_p / X_q\right) = \frac{f\left(X_p, X_q\right)}{\int\limits_0^{+\infty} f\left(X_p, X_q\right)dX_p} = \frac{1}{\sqrt{2\pi}\sigma_p^*}\exp\left\{-\frac{\left[\ln X_p - \ln\overline{X_p^*}\right]^2}{2\sigma_p^{*2}}\right\}, \quad (8)$$

$$\begin{cases}\sigma_p^* = \sigma_p\sqrt{1-r_{pq}^2}, \\ \ln\overline{X}_p^* = \ln\overline{X_p} - r_{pq}\dfrac{\sigma_p}{\sigma_q}\left(\ln X_q - \ln\overline{X}_q\right),\end{cases} \quad (9)$$

параметры условных плотностей распределения.

Полагая $q = p - 1$, из выражений (8) и (9) получаем алгоритм моделирования последовательности логарифмически-нормальных случайных величин $\varepsilon_1, \varepsilon_2, \varepsilon_3 \ldots \varepsilon_k, \ldots$ Запишем алгоритм моделирования при использовании стандартной процедуры или функций математического пакета, которые возвращают логарифмически-нормальные случайные величины с заданными параметрами распределения. Если для эффективности (в смысле быстродействия) ограничиться стационарными в широком смысле марковскими процессами, то необходимо принять ограничения, изложенные выше, а именно

$$\ln\overline{X}_p = \ln\overline{X}_q = \ln\overline{X}\ ,\ \sigma_p = \sigma_q = \sigma\ ,\ R_{pq} = R_{|p-q|} = R,\ p,q = 1,2,\ldots,$$

при этом будут выполнены равенства

$$K_p = K_q = K,\ r_{pq} = r_{|p-q|},\ p,q = 1,2,\ldots.$$

Пусть функция, возвращающая логарифмически-нормальную случайную величину ε, записывается в виде $\varepsilon = rlnorm\left(\ln \bar{X}_0, \sigma_0\right)$. Тогда, последовательность случайных величин $\varepsilon_1, \varepsilon_2, \varepsilon_3 \ldots \varepsilon_k, \ldots$ представляет собой последовательность независимых в совокупности случайных величин распределенных по логарифмически-нормальному закону с параметрами $\left(\ln \bar{X}_0, \sigma_0\right)$, а последовательность $\eta_1, \eta_2, \eta_3 \ldots \eta_k, \ldots$, где

$$\begin{cases} \eta_1 = \varepsilon_1 = rlnorm\left(\ln \bar{X}_0, \sigma_0\right), \\ \eta_p = rlnorm\left(\ln \bar{X}_p^*, \sigma_p^*\right) = rlnorm\left(\ln \overline{X_0} - r\ \left(\ln X_{p-1} - \ln \bar{X}_0\right), \sigma_0 \sqrt{1 - r^2}\right), \end{cases} \quad (10)$$

для p = 2, 3, …, k, … является последовательностью логарифмически-нормальных случайных величин, каждая из которых имеет среднее значение m, дисперсию σ^2 и коэффициент вариации K. Выражение (10) и определяет искомый алгоритм моделирования.

В работе приведен машиноориентированный алгоритм моделирования коррелированных логарифмически-нормальных случайных величин, основанный на прямом вычислении условной плотности распределения.

Библиографический список

1. Isakov V. I., Shepeta D. A. Simulation of location signals when determining a coastal edge // 2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2021. Pp. 1–5, (June 2021).

2. Исаков В. И., Шепета Д. А. Моделирование локационных сигналов, отраженных от кромки земля-море // Информационно-управляющие системы. 2017. № 5 (90). С. 89–94.

3. Шепета А. П., Подоплекин Ю. Ф. Корреляционные функции эхосигналов кораблей при перестройке несущей частоты бортовой РЛС // Морская радиоэлектроника. 2021. № 1 (75). С. 50–53.

4. Wattimena G. M., Shepeta D. A., Isakov V. I. Determination of the coastal edge using on-board radar // Proc. SPIE 11914, SPIE FutureSensing Technologies 2021, 119140D (14 November 2021).

5. Исаков В. И., Шепета Д. А. Плотность распределения мощности огибающей локационных сигналов, отраженных от кромки земля-море // Обработка, передача и защита информации в компьютерных системах: 21 Междунар. науч. конф. СПб.: ГУАП, 2021. С. 25–28.

6. Блаунштейн Н. Ш. Прикладные аспекты электродинамики / Н. Ш. Блаунштейн, М. Б. Сергеев, А. П. Шепета. СПб.: Аграф+, 2016. 272 с.

УДК 517; 517.9

А. А. Щеголева*
студент
М. Д. Поляк*
старший преподаватель
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ДИНАМИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ЛОТКИ-ВОЛЬТЕРРЫ С ВНУТРЕННЕЙ КОНКУРЕНЦИЕЙ

В работе рассматривается задача разработки математической модели для системы поддержки принятия решений (СППР) управления водными объектами, основанной на системе типа «хищник-жертва» для двух популяций. Применение техники аналитического конструирования агрегированных регуляторов (АКАР) синергетической теории управления и компьютерного моделирования позволяют получить модель для решения практических задач в сфере биомониторинга. Предложена управляемая модель сосуществования двух биологических видов, определены допустимые диапазоны значений ее параметров, при которых могут сосуществовать оба вида.
***Ключевые слова*:** теория синергетического управления, метод АКАР, хищник-жертва, математическое моделирование.

A. A. Shchegoleva*
Student
M. D. Polyak*
Senior lecturer
*St. Petersburg State University of Aerospace Instrumentation

MATHEMATICAL MODELING OF DYNAMICAL SYSTEMS BASED ON LOTKA-VOLTERRA MODEL WITH INTRASPECIFIC COMPETITION

The paper considers the problem of developing a mathematical model for a decision support system (DSS) in water bodies. The model is a system of differential equations describing predator-prey relationships for two populations. The application of the technique of analytical design of aggregated regulators (ADAR) and the theory of synergetic control will provide a model for solving new practical problems in the field of environmental monitoring, assessment of various bio- and ecosystems. The purpose of introducing control is to create a controllable model with a given maximum capacity of the medium and a proportional ratio. The developed mathematical model will become the main part of DSS for determining the ranges of values of the system parameters under which both species can coexist.
Keywords: synergetic control theory, ADAR method, predator-prey, mathematical modeling of water bodies.

Введение

Вольтерра в своей работе [1] предложил общую модель в виде системы уравнений «хищник-жертва» для описания взаимодействий между несколькими биологическими видами:

$$\frac{dx_i}{dt} = \left(\alpha_i - \sum_{s=1}^{n} \beta_{is} x_s \right) x_i, \qquad (1)$$

где x_i – размер популяции i-го вида, n – количество видов, α_i, β_{is} – коэффициенты рождаемости и смертности.

Внутривидовая конкуренция является наиболее общим и важным типом взаимодействия в водных объектах [2, 3], а модель (1) расширяет классическую модель Лотки-Вольтерры. Численное решение модели Лотки – Вольтерры без внутривидовой конкуренции представляет собой незатухающие периодические колебания, отражающие сезонность, где при отсутствии хищников происходит экспоненциальный рост жертв. Введение внутривидовой конкуренции приводит к затухающим колебаниям, а система приходит к точке равновесия. Конкретизируем рассматриваемую модель на основе (1):

$$\begin{cases} \dfrac{dx_1}{dt} = f_1 = \alpha_1 x_1 - \beta_1 x_1 x_2 - \gamma_1 x_1^2 \\ \dfrac{dx_2}{dt} = f_2 = -\alpha_2 x_2 + \beta_2 x_1 x_2 - \gamma_2 x_2^2 \end{cases}, \qquad (2)$$

где α_1, β_2 – коэффициенты рождаемости, α_2, β_1 – коэффициенты смертности, γ_1, γ_2 – коэффициенты смертности в результате внутривидовой конкуренции.

В качестве хищников и жертв в рамках рассматриваемой предметной области могут выступать, например, зоопланктон и фитопланктон, либо иные биологические виды. Подробный анализ динамической системы для выявления точек равновесия и возможных режимов работы системы (2) применительно к водным объектам выполнен в работе [4].

Введем общие предположения для системы (2):

1. В произвольный момент времени численность всех популяций неотрицательна $x_i(t) \geq 0, i = 1, 2, t \in [0; T]$.

2. Все параметры системы положительны $\alpha_i, \beta_i, \gamma_i > 0, i = 1, 2$.

3. Коэффициенты рождаемости больше коэффициентов вымирания $\alpha_1 > \beta_1, \alpha_1 > \gamma_1, \beta_2 > \alpha_2, \beta_2 > \gamma_2$.

Система с управлением

Для возможности достижения новых устойчивых стационарных состояний в модель (2) вводится аддитивное управление. Управляющее воздействие интерпретируется как внешнее воздействие среды. Например, это может быть перераспределение особей в водоеме благодаря наличию течений, ветрового волнения и иных процессов водопереноса, естественная и искусственная миграция и др. Для синтеза управления применяется метод АКАР [5 – 7]. Под действием управления изображающая точка фазового пространства переводит систему из заданного начального состояния в целевое состояние, задающееся макропеременной $\psi(t) \to 0$.

Цель управления представим как $\psi(t) = x_1 - \rho x_2 + d$, где параметр d интерпретируется как максимальная емкость среды, при которой в соотношении ρ могут сосуществовать два вида. Макропеременная должна доставлять глобальный минимум функционалу качества $\Phi = \int_0^\infty \left(\psi^2(t) + T^2\dot{\psi}^2(t)\right)dt \to \min$, для этого она должна быть решением уравнения Эйлера – Лагранжа $T\frac{d\psi(t)}{dt} + \psi(t) = 0$. Здесь коэффициент T определяется как параметр, влияющий на время переходного процесса в системе.

Применяя метод АКАР по аналогии с работами [8, 9] получим аналог системы (2) с управлением:

$$\begin{cases} \frac{dx_1}{dt} = f_1 = \alpha_1 x_1 - \beta_1 x_1 x_2 - \gamma_1 x_1^2 + u \\ \frac{dx_2}{dt} = f_2 = -\alpha_2 x_2 + \beta_2 x_1 x_2 - \gamma_2 x_2^2 \\ \psi = x_1 - \rho x_2 + d \\ u = \beta_1 x_1 x_2 - \alpha_1 x_1 + \gamma_1 x_1^2 + \rho f_2 - \frac{\psi}{T} \end{cases}, \tag{3}$$

где u – функция управления.

Для системы (3) при достижении макропеременной целевого значения $\psi(t) = 0, t \to \infty$ выведем точки равновесия для дальнейшего анализа динамических режимов системы. Общие предположения касательно системы (3) аналогичны системе (2) с добавлением ограничений на параметры $\rho, d, T : \rho > 0, d > 0, T > 0$.

Можно выделить две точки равновесия:

1. $E_0(-d, 0)$ – точка не удовлетворяет требованию не отрицательности численности популяции.

2. $E_1\left(x_{1s}^*, x_{2s}^*\right)$, где $x_{1s}^* = \frac{d\gamma_2 + \alpha_2\rho}{\beta_2\rho - \gamma_2}, x_{2s}^* = \frac{\alpha_2 + \beta_2 d}{\beta_2\rho - \gamma_2}$.

Рассмотрим подробнее условия перехода системы в точку равновесия E_1. Получим аналитическое решение системы (3) при условии достижения цели:

$$x_1(t) = \frac{-\alpha_2\rho + de^{(\alpha_2+\beta_2 d)(\rho C_1 + t)}(\gamma_2 - \beta_2\rho) - d\gamma_2}{(\beta_2\rho - \gamma_2)\left(e^{(\alpha_2+\beta_2 d)(\rho C_1 + t)} - 1\right)};$$
$$x_2(t) = \frac{\alpha_2 + \beta_2 d}{(\gamma_2 - \beta_2\rho)\left(e^{(\alpha_2+\beta_2 d)(C_1 + t)} - 1\right)}. \tag{4}$$

Анализируя выражения (4) можно выделить несколько дополнительных условий для существования точки равновесия, удовлетворяющей ограничениям на систему:

$$\gamma_2 < \rho\beta_2; \gamma_2 > \frac{\rho\left(\alpha_2 + \beta_2 d e^{\left((\alpha_2+\beta_2 d)(t+C_1\rho)\right)}\right)}{d\left(e^{\left((\alpha_2+\beta_2 d)(t+C_1\rho)\right)} - 1\right)}; \gamma_2 > \rho\beta_2.$$

Очевидно, что условия $\gamma_2 < \rho\beta_2$ и $\gamma_2 > \rho\beta_2$ не могут выполняться одновременно, что говорит о невозможности перевода системы в равновесную точку E_1. Единственной возможной точкой равновесия является точка E_0, однако она не удовлетворяет ограничениям, наложенным на систему. Такой вид макропеременной $\psi(t) = x_1 - \rho x_2 + d$ делает невозможным применение системы (3) для моделирования экологических систем водных объектов. Для решения возникшей проблемы предлагается другой вид макропеременной: $\psi(t) = x_1 + \rho x_2 - d$. Новый синтез закона управления:

$$\begin{cases} \dfrac{dx_1}{dt} = f_1 = \alpha_1 x_1 - \beta_1 x_1 x_2 - \gamma_1 x_1^2 + u \\ \dfrac{dx_2}{dt} = f_2 = -\alpha_2 x_2 + \beta_2 x_1 x_2 - \gamma_2 x_2^2 \\ \psi = x_1 + \rho x_2 - d \\ u = \beta_1 x_1 x_2 - \alpha_1 x_1 + \gamma_1 x_1^2 - \rho f_2 - \dfrac{\psi}{T} \end{cases}. \qquad (5)$$

Система (5) также имеет две равновесные точки:

1. $E_0(d,0)$ – популяция хищников вымирает, все пространство заполняют жертвы.

2. $E_1\left(x_{1s}^*, x_{2s}^*\right)$, где $x_{1s}^* = \dfrac{d\gamma_2 + \alpha_2\rho}{\gamma_2 + \beta_2\rho}, x_{2s}^* = \dfrac{\beta_2 d - \alpha_2}{\gamma_2 + \beta_2\rho}$.

Для существования точки E_1 необходимо выполнение условия $d > \dfrac{\alpha_2}{\beta_2}$. Для поиска дополнительных условий существования решим дифференциальные уравнения при условии достижения цели:

$$x_1(t) = \frac{e^{C_1\alpha_2\rho+\beta_2 dt}\left(\alpha_2\rho + d\gamma_2\right) - d e^{C_1\beta_2 d\rho+\alpha_2 t}\left(\beta_2\rho + \gamma_2\right)}{\left(\beta_2\rho + \gamma_2\right)\left(e^{C_1\alpha_2\rho+\beta_2 dt} - e^{C_1\beta_2 d\rho+\alpha_2 t}\right)};$$

$$x_2(t) = \frac{\left(-\alpha_2 + \beta_2 d\right)e^{C_1\alpha_2+\beta_2 dt}}{\left(\beta_2\rho + \gamma_2\right)\left(e^{C_1\alpha_2+\beta_2 dt} - e^{C_1\beta_2 d+\alpha_2 t}\right)}.$$

Относительно выражений можно ввести дополнительное ограничение для перехода в равновесную точку E_1: для $x_1(t)$ должно выполняться условие

$$\gamma_2 > \frac{\rho\left(\alpha_2 e^{C_1\alpha_2\rho+\beta_2 dt} - \beta_2 d e^{\alpha_2 t + C_1\beta_2 d\rho}\right)}{d\left(e^{\alpha_2 t + C_1\beta_2 d\rho} - e^{C_1\alpha_2\rho+\beta_2 dt}\right)}.$$

В данной системе нет условий, противоречащих друг другу, при выполнении двух условий система переходит в равновесную точку E_1.

Численное моделирование (рис. 1) подтвердило, что система переходит в стационарное состояние при выполнении заданных условий и установившиеся значения соответствуют равновесной точки E_1. Ограничение на d задает минимально возможную емкость системы, при которой могут сосуществовать оба вида. Параметры управления: $\rho = 2, d = 50, T = 5$. Коэффициенты рождаемости, смертности и внутренней конкуренции:

$$\alpha_1 = 0{,}0625, \alpha_2 = 0{,}1223, \beta_1 = 0{,}1046, \beta_2 = 0{,}0065, \gamma_1 = 0{,}001, \gamma_2 = 0{,}001.$$

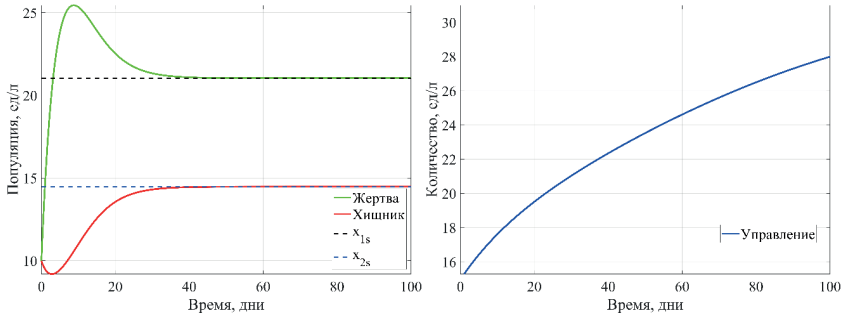


Рис. 1. Численное решение системы (5), установившиеся значения x_{1s} и x_{2s} рассчитываются по формулам для равновесной точки E_1

Заключение

В работе исследованы две системы хищник-жертва с управлением и внутривидовой конкуренцией. Для обеих систем найдены стационарные точки и получены аналитические решения для дифференциальных уравнений. Проведен анализ динамических систем для выявления возможных режимов работы системы и условий перехода в них. Доказано, что для макропеременной $\psi(t) = x_1 - \rho x_2 + d$ управляемая система может находиться только в одной равновесной точке, в которой один из видов вымирает, другой принимает отрицательные значения. Для второй макропеременной $\psi(t) = x_1 + \rho x_2 - d$ выделены диапазоны параметров среды и внутривидовой конкуренции, в которых оба вида могут сосуществовать. Проведенная работа доказывает возможность исполь-

зования математических моделей с АКАР-управлением в качестве основы для СППР биологических систем водных объектов.

Библиографический список

1. Volterra V. Variations and Fluctuations of the Number of Individuals in Animal Species living together // ICES Journal of Marine Science. 1928. № 3. Pp. 3–51.

2. Intraspecific Competition URL: https://www.sciencedirect.com/topics/agricultural-and-biological-sciences/intraspecific-competition (дата обращения: 24.02.2022).

3. Базыкин А. Д. Биофизика взаимодействующих популяций. М.: Наука, 1985.

4. Щеголева А. А. Модель «хищник-жертва с внутривидовой конкуренцией» / А. А. Щеголева, М. Д. Поляк // Обработка, передача и защита информации в компьютерных системах '22: Вторая международная научная конференция: сб. докладов. Санкт-Петербург, 11–15 апреля 2022 года. СПб.: ГУАП, 2022. С. 120–126.

5. Колесников А. А. Синергетика и проблемы теории управления. М.: ФИЗМАТЛИТ, 2004. 504 с.

6. Колесников А. А. Методы АКАР и АКОР в задачах синтеза нелинейных систем управления / А. А. Колесников, Ал. А. Колесников, А. А. Кузьменко // Мехатроника, автоматизация, управление. 2016. № 10. С. 657–669.

7. Колесникова С. И. Синтез управления нелинейным объектом второго порядка с неполным описанием // Автоматика и телемеханика. 2018 № 9. С. 18–30.

8. Polyak M., Kolesnikova S. (2020). Novel approach to Design and Analysis of Water Resources Development Model in Terms of Phytoplankton Population Dynamics. IOP Conference Series: Earth and Environmental Science. 459. 032072. 10.1088/1755-1315/459/3/032072.

9. Щеголева А. А. Модель «хищник-жертва с питанием» / А. А. Щеголева, М. Д. Поляк // Обработка, передача и защита информации в компьютерных системах '21. Международная научная конференция: сб. докладов, Санкт-Петербург, 14–22 апреля 2021 года. СПб.: ГУАП, 2021. С. 86–91.

УДК 004.56

Е. С. Юмашева*
аспирант
*Государственный университет морского и речного флота им. адмирала С. О. Макарова

АРХИТЕКТУРА АГЕНТОВ, КАК СПОСОБ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

В работе поднят исследовательский вопрос, о способах автоматизации тестирования на проникновение, а также проведен краткий обзор одной из передовых, на данный момент, разработок в данной области – архитектуры агентов.
Ключевые слова: тестирование на проникновение, информационная безопасность.

E. S. Yumasheva*
PhD Student
*Admiral Makarov State University of Maritime and Inland Shipping

AGENT ARCHITECTURE AS A WAY TO AUTOMATE PENETRATION TESTING

The article raises a research question about ways to automate penetration testing, and also provides a brief overview of one of the most advanced developments in this field at the moment – agent architecture.
Keywords: penetration testing, information security.

В последние годы вредоносные сетевые атаки становятся все более серьезной угрозой как для обычных людей, организаций, так и для национальной информационной безопасности. Тестирование на проникновение – это хорошо зарекомендовавший себя упреждающий подход к оценке безопасности цифровых активов путем активного выявления и использования существующих уязвимостей. Этот процесс имитирует реальные атаки, осуществимые хакерам, не влияя при этом на доступность системы, что дает администраторам целевой системы интуитивное представление о текущих проблемах безопасности системы. С одной стороны, тестирование на проникновение может проверить, эффективно ли работают меры безопасности системы или нет с точки зрения злоумышленника. С другой стороны, потенциальные риски безопасности могут быть выявлены в реальных событиях, что повышает уровень осведомленности соответствующего персонала по вопросам безопасности. В настоящее время это достаточно широко используемый подход к повышению уровня информационной защищенности целевой системы.

По оценке *Accenture* рост расходов в сфере кибербезопасности будет расти на 13% в год и к 2025 году достигнет $94 млрд [1]. Однако уже в 2021 году индустрия ИБ столкнулась с нехваткой рабочей силы в 3,5 млн человек [2]. Тестирование на проникновение (*penetration testing* – далее PT) – это довольно сложная, дорогостоящая и трудоемкая задача. Более того, результаты тестиро-

вания в значительной степени зависят от навыков и опыта тестировщика или команды. Автоматизация в этой сфере может значительно сократить время, затраты и человеческий труд, необходимые на этапе сбора, анализа и использования информации. Что касается защиты конфиденциальной информации, то автоматизированный пентест может предотвратить утечку конфиденциальной информации тестировщиками-людьми.

Существует 4 различных уровня описания степени автоматизации РТ [4]:

- Полностью автономный (уровень 4): система полностью автономна при выполнении всех задач РТ.
- Частично автономный (уровень 3): система полуавтономна при выполнении задач РТ. В этом случае система находится под постоянным наблюдением специалистов.
- Режим содействия принятию решений (уровень 2): система действует вместе с экспертом-человеком и помогает ему в принятии решений.
- Режим обучения (уровень 1): система работает в фоновом режиме, чтобы извлекать уроки из решений, принимаемых экспертами-людьми, во время его работы.

На сегодняшний день в области автоматизированного тестирования на проникновение было проведено довольно мало исследований, и эта область информационной безопасности все еще находится на начальной стадии развития. Многие исследования и реализации автоматизации просто сопоставляют результаты сканирования уязвимостей с соответствующими инструментами эксплуатации. Из-за преимущественно неинтерактивной обработки такие решения могут работать только с детерминированными целями. Однако целевая среда РТ обычно динамична, неопределенна и сложна. Тестировщик должен взаимодействовать со средой или целями и выбирать наилучшие действия для компрометации целевой системы на основе собранной информации. Для решения этих проблем предлагается архитектура на основе агентов для автоматизации РТ.

Интеллектуальный агент – это программа, которая может принимать решения или выполнять услугу на основе своей среды, пользовательского ввода и опыта. Эти программы могут использоваться для автономного сбора информации по регулярному, запрограммированному расписанию или по запросу пользователя в режиме реального времени. Агент (бот) может взаимодействовать с окружающей средой посредством восприятия, принятия решений и действий.

Более того, поведение агента может быть гибким и обычно характеризуется как автономное, инициативное и социальное. В настоящее время агентные технологии считаются перспективными для применения в различных областях. Модель *Belief-Desire-Intention* (BDI) относится к числу классических и наиболее репрезентативных моделей когнитивной архитектуры. Это позволяет агентам обладать когнитивными способностями справляться с динамичными, неопределенными и сложными условиями, используя психологические состояния и характеристики, установки, такие как убеждения, желания и намерения.

Архитектура агента является одним из кандидатов для моделирования и решения проблем взаимодействия РТ. Боты могут воспринимать окружающую среду с помощью датчиков и выполнять различные действия по ее изменению с помощью механизмов исполнения. Самый важный вопрос для агента заключается в том, как решить, что делать в соответствии с информацией, полученной в результате его восприятия. Функция бота сопоставляет любые последовательности восприятия с действием, как показано ниже:

$$f : P^* \to A. \tag{1}$$

Среда агента может быть как физической, так и программной. Агент обладает определенными отличительными характеристиками, такими как:

- Автономность: способность автоматически корректировать свое поведение в соответствии с изменениями во внешней среде.
- Социальность: способность взаимодействовать с другими людьми и агентами.
- Реактивность: способность воспринимать изменения окружающей среды и реагировать на них.
- Проактивность: способность демонстрировать целенаправленное поведение.

Архитектура агента является важной частью агента. Он определяет, как представлены знания или информация и какие действия должен предпринять агент, основываясь на механизме рассуждения. Были предложены три типа архитектуры агентов: классическая, когнитивная и семантическая.

Классическая архитектура включает архитектуру, основанную на логике, реактивную архитектуру, архитектуру BDI и гибридную архитектуру. Архитектура, основанная на логике, основана на традиционном подходе к искусственному символическому моделированию среды и действий агентов. Логический подход – это процесс вывода, основанный на наборе правил вывода. Основная проблема архитектуры, основанной на логике, заключается в том, что трудно перевести восприятие или информацию об окружающей среде в символическое представление для рассуждений. Архитектура реактивного агента основана на сопоставлении ситуации с действием без способности рассуждать. В этой архитектуре агент выполняет действие в соответствии с изменением среды, и каждая ситуация отображается в действие. Преимущество реактивной архитектуры заключается в том, что ее легко спроектировать и внедрить. Однако эта архитектура обладает меньшей способностью к долгосрочному планированию. Поэтому нелегко создавать агенты, управляемые задачами, и решать сложные задачи. Гибридная архитектура допускает как реактивное, так и преднамеренное поведение агента, состоящее из двух типов взаимодействия, которые протекают между горизонтальным и вертикальным уровнями.

Когнитивная архитектура основана на когнитивных науках, которые фокусируются на человеческом познании и психологии, в то время как семантическая архитектура используется в семантической технологии.

Архитектура BDI основана на практических рассуждениях, предложенных Братманом. Практическое рассуждение – это рассуждение о действиях, процесс определения того, что делать, в то время как процесс теоретического рассуждения направлен на получение выводов с использованием знаний. Человеческое практическое мышление состоит из двух видов деятельности, а именно обдумывания и рассуждения о средствах достижения цели.

Рассуждение о средствах достижения цели более известно в области искусственного интеллекта как планирование, которое определяет план действий для достижения конкретной цели. Основные проблемы этого подхода заключаются в том, что он требует больших вычислительных затрат и не позволяет планировать и действовать в режиме реального времени. Агентная технология – это естественный подход для решения сложных задач в динамичной среде. В архитектуре BDI агенты состоят из трех логических компонентов, представляющих ментальные состояния, а именно:

• Убеждения: информация, которой располагает агент об окружающей среде.

• Желания: мотивация агента или возможные варианты, которые агент может захотеть выполнить.

• Намерения: положение дел, которое агент решил выполнить.

Намерения являются ключевыми компонентами практических рассуждений и имеют решающее значение для успеха агента. BDI является наиболее известной архитектурой [3], а система процедурных рассуждений является одной из ее наиболее известных реализаций. Первоначально (*procedural reasoning system*) PRS был разработан в Стэнфордском исследовательском институте Майклом Джорджеффом и Эми Лански [5]. На сегодняшний день это оказался один из самых надежных подходов к разработке агентов. Чтобы создать систему рассуждений в реальном времени, PRS может решать сложные задачи в динамичных средах. Архитектура PRS состоит из четырех ключевых элементов: убеждений, желаний, намерений и планов, а также интерпретатора.

В системе PRS планы указывают курс действий агента для достижения своих намерений. Планы создаются вручную и предварительно определяются с помощью библиотеки программистом агента. Планы в PRS включают следующие компоненты:

• контекст: предварительное условие плана.

• тело: порядок действий, которые необходимо выполнить.

• цель: постусловие плана.

Интерпретатор агента используется для обновления убеждений на основе наблюдений за окружающей средой, генерирования новых желаний на основе убеждений и выбора желаний в качестве намерений. Наконец, интерпретатор выбирает действие для выполнения текущих намерений агента.

В данной статье мы кратко рассмотрели исследовательский вопрос в области тестирования на проникновения, а также рассмотрели базовую структуру агатных архитектур, в частности BDI. Модель обеспечивает обоснование от результатов действий до реагирования на окружающую среду.

Библиографический список

1. Информационная безопасность (мировой рынок) // Tadviser Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_%28мировой_рынок%29 (дата обращения: 01.03.2022).

2. Steve Morgan. Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021. Cybercrime Magazine, 2019.

3. Ровбо М. А., Овсянникова Е. Е. Методы локального планирования поведения агентов с BID-архитектурой // Искуственный интеллект принятие решений. URL: http://www.isa.ru/aidt/images/documents/2019-01/74-86.pdf (дата обращения: 05.03.2022).

4. Три уровня автоматизации тестирования // ПроТестинг.ru URL: http://www.protesting.ru/automation/functional/autolevel.html (дата обращения: 05.03.2022).

5. Система процедурного обоснования // ru.knowledgr. URL: https://ru.knowledgr.com/03403824/ПроцедурнаяСистемаРассуждения (дата обращения: 04.03.2002).

УДК 004.627; 519.21

М. Ю. Ястребов[*]
кандидат экономических наук, профессор
А. Д. Ястребова[**]
исследователь-программист
[*]Санкт-Петербургский государственный университет морского и речного флота имени адмирала С. О. Макарова
[**]Санкт-Петербургский государственный архитектурно-строительный университет

ОЦЕНКА ИРРЕГУЛЯРНОСТИ ХЕШ-КОДОВ

Предложен показатель виртуальной рандомизации эвристических процедур хеширования.
Ключевые слова: анализ алгоритмов; хеширование; оценка качества; инверсии перестановки.

M. YU. Yastrebov[*]
PhD, Economic, Professor
A. D. Yastrebova[**]
Researcher programmer
[*]Admiral Makarov State University of Maritime and Inland Shipping
[**]Saint Petersburg State University of Architecture and Civil Engineering

TESTIMATION OF IRREGULARITY OF HESH-CODES

The indicators of virtual randomization of heuristic hashing procedures are formulated.
Keywords: analysis of algorithms; hashing; measures of efficiency; inversion of permutation.

В публикациях [1, 3] намечен подход к дефиниции степени иррегулярности хеш-кодов, вырабатываемых различными алгоритмами хеширования. Здесь мы формализуем показатель иррегулярности и приводим данные машинных экспериментов по его оценке для некоторых эвристических алгоритмов.

При хешировании (см. [2]), потенциально большой, но разреженный динамический массив K сжимается тем или иным образом в массив H длины $|\mathrm{H}|$. Оценка качества сжатия описана в [2] (см. также [5]).

Хеширование, как сжатие с перемешиванием, имеет и криптографическую мотивацию. Поэтому целесообразно наряду со статистическими критериями случайности последовательности хеш-кодов, которые при заданном пороговом значении дают дискретный ответ «да/нет», использовать количественные показатели. Мы отталкиваемся от классического алгоритма хеширования методом деления заданному модулю в качестве эталонного. Ему следует приписать минимальную (нулевую) степень иррегулярности, так как на диапазоне номеров $1 - m$ число инверсий перестановки $(1,2,...,m-1,m)$ равно нулю. Максимум инверсий $(m-1)m/2$ в зеркальной перестановке $m,m-1,...,2,1)$ также свидетельствует о полной регулярности.

При формировании показателя I иррегулярности мы исходим из статистически оцениваемой средней удаленности числа инверсий n перестановки хеш-адресов, полученной на случайно формируемой входной последовательности адресов из K варьируемой длины $l\,|\mathrm{H}|$, от среднего числа инверсий

$$\overline{I} = (l-1)l/4:\ I = \left|n - \overline{I}\right| / l\,.$$

Чем большее значение имеет показатель I, тем менее иррегулярна перестановка, доставляемая хеш-алгоритмом. По этой причине, а также в целях нормировки показателя иррегулярности на промежуток от нуля до единицы (что повышает наглядность), мы вводим нормированный показатель иррегулярности $I_{norm} = 1 - I/\overline{I}$. Теперь большее значение I_{norm} означает более высокую степень иррегулярности

Опорные значения для l: $|\mathrm{H}|/4,\ |\mathrm{H}|/2,\ 3|\mathrm{H}|/4,\ |\mathrm{H}|$. Возникающие коллизии (когда $(h(k') = h(k''), k' \neq hk'')$ мы здесь не рассматриваем, так как их анализ их частоты, как одного из критериев качества хеш-алгоритма, описан в [3]; таким образом на случайную последовательность входных номеров хешируемого массива накладывается требование отсутствия совпадений ее элементов.

1. Метод умножения

Хеширование задается параметризованной формулой $h(K) = [|\mathrm{H}|\{Ka\}]$. Значения приведены в табл. 1.

Таблица 1

l	0,25	0,5	0,75	1
I	0,000418	0,00004	0,000052	0,000011

2. Биллиардный метод

При биллиардном хешировании [3] единичная окружность с центром в точке $(0,0)$ (или другая гладкая замкнутая линия) разбивается против часовой стрелки на $p = |\mathrm{H}|$ равных дуг (P_{i-1}, P_i), $i = 1,...,p$, длины β. Далее, для адреса (натурального числа) K выбирается начальный угол $\alpha_1 = \alpha_1(K) \in (0,\pi)$ и количество $n(K)$ последовательных отражений от окружности луча, исходящего в начале из точки $O(1,0)$ под углом $\pi - \alpha_1$ к оси Ox. Хеш-адрес $h(K)$ определяется как номер m дуги (P_{m-1}, P_m), в которую луч попадает в результате последнего отражения. При этом угол α_i каждого следующего упругого отражения подвергается случайной деформации. Результаты приведены в табл. 2.

Таблица 2

l	0,25	0,5	0,75	1
I	0,002056	0,000141	0,000086	0,000025

3. Хеширование Фибоначчи

Хеширование на основе поиска Фибоначчи подробно изложено в [4]. Оно осуществляет сжатие массива размера $3^s - 1$ в массив размера $F_{s+3} - 1$, где F_s – s -е число Фибоначчи. Результаты приведены в табл. 3.

Таблица 3

l	0,25	0,5	0,75	1
I	0,008214	0,001663	0,0009	0,000521

Рассматриваемые совместно показатели качества сжатия [3] и параметр I_{norm} дают всестороннюю характеристику эвристических алгоритмов хеширования, которые всегда, тем не менее, зависят от способа задания параметров. Исследование подобной зависимости для каждого отдельно взятого хеш-алгоритма может являться самостоятельным предметом исследования.

Библиографический список

1. Ястребов М. Ю. К оценке иррегулярности хеш-кодов // Материалы V межрегиональной научно-практической конференции ПНРОИТ. (Севастополь 24–28 сентября 2019 года). С. 401–402.

2. Кнут В. Искусство программирования. Т. 3. Сортировка и поиск. 2-е изд. М.: Издательский дом “Вильямс”, 2003. 820 с.

3. Ястребов М. Ю. [и др.] Показатели качества и анализ некоторых эвристических хеш-алгоритмов и др. // Системы компьютерной математики и их приложения: материалы XX Международной научной конференции. Вып. 21. Смоленск: Изд-во СмолГУ, 2019. С. 54–56.

4. Ястребов М. Ю. Поиск Фибоначчи – обоснование, система счисления и хеширование // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2013. № 3 (174). С. 53–58.

5. Communications of the Association for Computing Machinery, 1971. Vol. 14. P. 228–239.

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

УДК 629.7.06

Г. Ю. Анисимов*
студент
К. А. Семенюк*
студент
П. А. Назаренко*
ассистент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АЛГОРИТМЫ ДЕТЕКТИРОВАНИЯ ОСОБЫХ ТОЧЕК ИЗОБРАЖЕНИЯ ORB, BRISK, AKAZE В РАБОТЕ ТЕХНИЧЕСКОГО ЗРЕНИЯ БАС

В данной статье рассмотрены такие алгоритмы детектирования особых точек, а также их дескрипторы. Предложены сферы применения алгоритмов для беспилотных авиационных систем (БАС) и проблемы, которые можно минимизировать при использовании того или иного алгоритма детектирования особых точек. В эксперименте предполагается работа алгоритмов с «эталонным» изображением, т. е. с уже готовым, качественным изображением местности (возможно спутниковый снимок).
Ключевые слова: ORB, AKAZE, BRISK, FAST, BRIEF, дескриптор, особая точка, яркость точек, БАС, навигация, тушение пожаров, поиск людей.

G. U. Anisimov*
Student
K. A. Semenuk*
Student
P. A. Nazarenko*
Assistant
*St. Petersburg State University of Aerospace Instrumentation

ALGORITHMS FOR DETECTING SINGULAR IMAGE POINTS ORB, BRISK, AKAZE IN THE WORK OF UAS TECHNICAL VISION

This article discusses such algorithms for detecting singular points, as well as their descriptors. The fields of application of algorithms for UAS and problems that can be minimized when using a particular algorithm for detecting singular points are proposed. In the experiment, algorithms are supposed to work with a "reference" image, that is, with a ready-made, high-quality image of the terrain (possibly a satellite image).
Keywords: ORB, AKAZE, BRISK, FAST, BRIEF, descriptor, special point, brightness of points, UAS, navigation, fire extinguishing, search for people.

Введение

Беспилотные авиационные системы в нынешних реалиях выполняют большое количество операций, помогая как в поиске людей, так и в локализации пожаров. Не редко в таких случаях используется видеосъемка или так называемое «техническое зрение». Также компьютерное зрение применяется и в навигации БАС. Неточное определение очагов возгорания или ложное обна-

ружение человека ведет к потере времени, необходимого для локализации пожара или спасения жизни человека. В навигации, неточное определение посадочной зоны, влечет за собой финансовые расходы по ремонту, а что еще хуже к покупке нового аппарата. Оборудование, устанавливаемое на БАС, предполагает работу с алгоритмами детектирования особых точек получаемого (эталонного) изображения. В статье пойдет речь о таких алгоритмах, как ORB (*Oriented FAST and Rotated BRIEF*), AKAZE (*Accelerated-KAZE*) и BRISK (*Binary Robust Invariant Scalable Keypoints*).

Алгоритм ORB

ORB представляет собой слияние детектора ключевых точек FAST (FAST *Keypoint Orientation*) и бинарного дескриптора BRIEF с модификациями для повышения производительности. Сначала применяется детектор FAST, который создает в окрестности каждой точки изображения окружность равную 16 пикселям для обнаружения угловых точек. Затем оценивается яркость точек на окружности по сравнению с яркостью ее центра. В случае, когда таких точек найдется больше 3/4, то центр окружности можно считать особой точкой. Затем применяется мера угла Харриса [1], чтобы среди всех найденных особых точек оставить только наиболее подходящие.

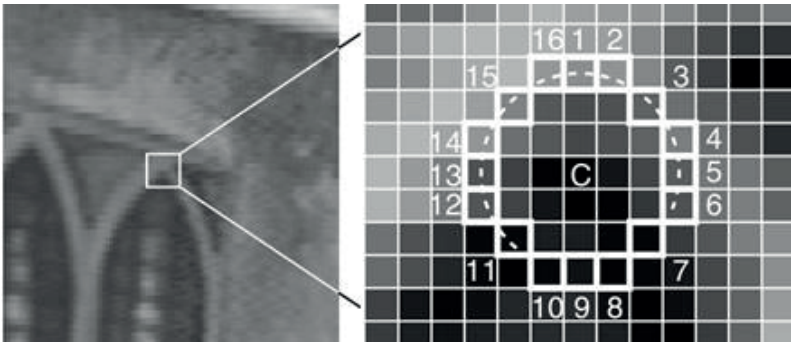


Рис. 1. Радиус точки FAST детектора

После детектора ключевых точек FAST в работу вступает дескриптор BRIEF, задача которого заключается в детектировании объекта при его вращении. Дескриптор имеет вид вектора длиной 256, который представляет из себя результаты бинарных тестов в радиусе особой точки. Сравниваются значения яркости в окрестности, но с большим радиусом. Вся битовая характеристика BRIEF обладает значительной дисперсией, которая достигает значения 0,5. Особенность заключается в том, что как только вектор совпадает с направлением ключевой точки, то его дисперсия становится более рассредоточенной. Большое значение дисперсии делает функцию более понятной, потому что ее реакция на входные значения будет более существенной

Алгоритм AKAZE

AKAZE основан на нелинейной диффузионной фильтрации, подобной KAZE, но его нелинейные масштабные пространства построены с использованием вычислительной структуры *Fast Explicit Diffusion* (FED), которая отвечает за поиск ключевых точек изображения. Алгоритм строит пирамиду изображений (пирамидальная структура) для увеличения скорости нелинейных пространственных вычислений в масштабе.

Детектирование особых точек происходит с помощью построения функциональной детерминанты для каждого компонента нелинейных масштабных преставлений L_i исходного изображениям, а затем вычисления определителя [2]:

$$L_H^i = \sigma_{i,norm}^2 (L_{xx}^i L_{yy}^i - L_{xy}^{i\ 2})\ L_H^i = \sigma_{i,norm}^2 (L_{xx}^i L_{yy}^i - L_{xy}^{i\ 2}), \qquad (1)$$

где $L_{xx}^i, L_{yy}^i, L_{xy}^i$ – производные *i*-го изображения второго порядка, $\sigma_{i,norm}$ – коэффициент, определяемый масштабом изображений, на котором вычисляется значение функции.

Дескриптор AKAZE основан на модифицированном двоичном алгоритме локальной разности (*Modified-Local Difference Binary*, M-LDB). Работает он следующим образом: для особой точки, найденной в ограниченном масштабе (σ_i), применяются первые производные L_x и L_y, затем, основываясь на полученных данных, все рассматриваемые области ориентируются в направлении заданным детектором.

Алгоритм BRISK

BRISK в качестве детектора особых точек изображения использует FAST, а роль дескриптора выполняет BRIEF. Как только особые точки были обнаружены строится пирамида, которая состоит из 4 внешних октав c_i и 4 внутренних октав d_i, $i = 0\ldots3$ [3]. Это делается для того, чтобы алгоритм «узнавал» фотографию с разных ракурсов. Формирование октав происходит путем уменьшения исходного изображения (c_0) в 2^i раза. А внутренние октавы уменьшаются в $\frac{2}{3}2^i$ раза от c_0 и располагаются между c_i и c_{i+1}.

Дескриптор BRIEF, учитывая набор ключевых точек (с уточнением до субпикселей и соответствующих значений масштаба с плавающей запятой), составляется в виде двоичной строки путем объединения результатов сравнения яркости. Сравнение яркости происходит с помощью разбиения области вокруг особо точки на 60 участков. Чтобы достичь инвариантности вращения (узнаваемости участка с любого ракурса) дескриптором определяется характерное направление каждой ключевой точки.

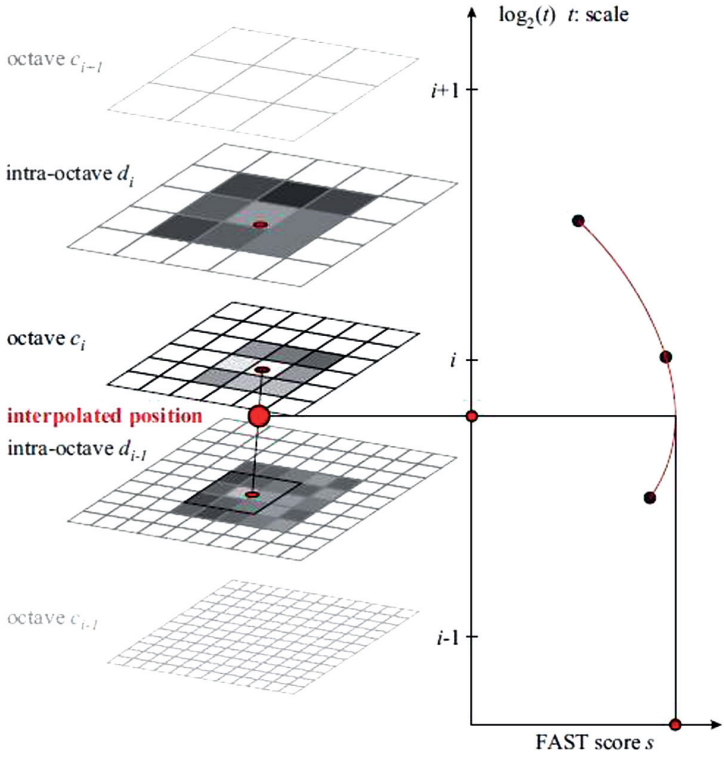


Рис. 2. Поиск особой точки с максимальным значением S [4]

Сравнение и результаты

Проводим сравнение рассматриваемых в работе алгоритмов ORB, AKAZE, BRISK основываясь на результатах, полученных в ходе экспериментов. Входные данные по таблицам: 100 фотографий с ярко выраженными деталями. Обращаю внимание, что сравнение фотографий происходит с разных ракурсов, т. е. ракурс «эталонной» фотографии отличается, от ракурса фотографии, для которой совершается поиск.

Работа выполнена в разработанной Патиным Михаилом Владиславовичем приложении для ОС *Android*.

Пояснения к таблицам:

- «$v_{\max}$» – максимальная скорость выполнения операции. Параметр $v_{\max}$ ={0.7, 0.75, 0.8, 0.85, 0.9}.
- «Сжатие» – количество пикселей.
- «Время» – время, затраченное на выполнение операции. Единица измерения – секунды.

• «Групп» – количество определенных групп.

• «Ложных групп» – группы, в которых все сопоставления ложные.

• «Ошибки в группах» – если есть как минимум две схожих фотографии в группе, то каждая не схожая с этими двумя считается ошибкой.

• «Фотографии без группы» – фотографии, которые не были определены в какую-либо группу.

• «Кол-во связей» – число связей, по которым были определены группы, связи фотографий без групп не учитываются.

Таблица 1

Лучшие результаты работы программы. Фотографии высокого качества

Метод	v_{max}	Сжатие	Время сек.	Групп	Ложных групп	Ошибок в группах	Фотографий без группы	Кол-во связей
ORB	0,8	300	35	39	3	1	12	4002
ORB	0,75	600	35	38	1	0	15	4024
BRISK	0,8	300	115	42	0	0	2	6695
BRISK	0,75	600	550	43	0	0	0	13862
AKAZE	0,8	300	26	38	0	1	14	3315
AKAZE	0,9	600	262	41	0	0	5	14631

При работе программы наилучшие результаты показал алгоритм BRISK. Алгоритм выбран лучшим по сравнению с AKAZE из-за наименьших показателей параметров «ошибок в группах» и «фотографий без группы».

Таблица 2

Лучшие результаты работы программы. Фотографии с шумом

Метод	v_{max}	Сжатие	Время сек.	Групп	Ложных групп	Ошибок в группах	Фотографий без группы	Кол-во связей
ORB	0.8	300	34	35	2	2	19	2073
ORB	0.9	600	176	38	0	3	12	4655
BRISK	0.85	300	430	41	0	1	6	4250
BRISK	0.8	600	3264	42	0	1	2	6044
AKAZE	0.8	300	23	34	3	6	20	1996
AKAZE	0,85	600	219	40	0	1	5	6165

В случае, когда на фотографии добавлен шум, лучшие результаты показал алгоритм AKAZE. Данный алгоритм выбран лучшим из-за наименьшего количества ошибочных, ложных групп и фотографий без группы.

Таблица 3

Лучшие результаты работы программы. Размытые фотографии

Метод	v_{max}	Сжатие	Время сек.	Групп	Ложных групп	Ошибок в группах	Фотографий без группы	Кол-во связей
ORB	0,75	300	21	34	0	0	26	2246
ORB	0,85	600	32	32	4	4	23	2736
BRISK	0,75	300	6	22	1	0	51	994
BRISK	0,8	600	6	30	4	1	34	1272
AKAZE	0,85	300	17	33	4	6	21	1922
AKAZE	0,8	600	21	38	0	0	14	2936

Первенство забирает алгоритм AKAZE. Дескриптор наилучшим образом справился при размере изображения 600 пикселей, показав 0 ложных групп и 0 ошибок в группах, хотя ORB при размере изображения 300 пикселей не уступает в вышеперечисленных параметрах, но имеет большее количество фотографий без групп.

Заключение

В двух из трех проведенных экспериментов лучшим себя показал алгоритм AKAZE. Для работы БАС при тушении пожаров и поиска людей с имеющимися спутниковыми снимками алгоритм AKAZE обеспечит высокие параметры точности обнаружения человека или очага возгорания.

Точность обнаружения человека позволит поисково-спасательной группе самым быстрым образом найти и помочь потерявшемуся.

Точная локализация пожара позволит БАС быстро приступить к ликвидации очага пожара или препятствию его распространения, в том числе своевременно среагировать службам спасения.

Если рассматривать техническое зрение, как помощник в навигации БАС (посадке), то алгоритм AKAZE позволит свести обнаружение ложных мест посадки к минимуму, что в свою очередь уменьшает затраты на ремонт и время на поиски потерявшихся БАС.

Библиографический список

1. Краснобаев Е. А. Сравнение бинарных дескрипторов особых точек изображений в условиях искажений / Е. А. Краснобаев, Д. В. Чистобаев, А. Л. Малышев // Компьютерная оптика. 2019. Т. 43. № 3. С. 434–445.

2. Патин М. В. Сравнительный анализ дескрипторов особых точек изображений с внедрением алгоритмов под операционной системой «Android». URL: https://dspace.spbu.ru/bitstream/11701/3991/1/st010290.pdf (дата обращения: 13.03.2022).

3. Karami E. Image Matching Using SIFT, SURF, BRIEF and ORB: Performance Comparison for Distorted Images / E. Karami, S. Prasad, M. Shehata. URL:

https://arxiv.org/ftp/arxiv/papers/1710/1710.02726.pdf (дата обращения: 13.03.2022).

4. Антипова Е. А. Разработка приложения для поиска ресурса по характерному изображению на примере сайта библиотеки комиксов. URL: AntipovaEA_2019.pdf (utmn.rhttps://elib.utmn.ru/jspui/bitstream/rutsu/4455/1/AntipovaEA_2019.pdfu) (дата обращения: 13.03.2022).

5. Чеканов М. О. Исследование влияния природы рентгеновских изображений на качество детекции и дескрипции особых точек / М. О. Чеканов, О. С. Шипитько // Сенсорные системы. 2020. Т. 34. № 2. С. 156–171.

6. Shaharyar Ahmed Khan Tareen. A Comparative Analysis of SIFT, SURF, KAZE, AKAZE, ORB, and BRISK / Shaharyar Ahmed Khan Taleem, Zahra Saleem // International Conference on Computing, Mathematics and Engineering Technologies. 2018.

УДК 65.012.1, 656.072

А. А. Добровольская*
ассистент
Н. Н. Майоров*
доктор технических наук, профессор
М. Р. Язвенко*
лаборант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИССЛЕДОВАНИЕ ВАРИАНТОВ МОДЕРНИЗАЦИИ ИНФРАСТРУКТУРЫ ТРАНСПОРТНОГО ТЕРМИНАЛА НА ОСНОВЕ ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ

Сегодня морские пассажирские порты и терминалы (крупные транспортные терминалы) требуют разработки новых моделей и методов для эффективного планирования работы и точного прогнозирования развития портовой инфраструктуры с учетом влияния внешней среды. Такие ключевые элементы как развитие морских пассажирских портов, их модернизация, изменения в маршрутных круизных и паромных сетях, особенно актуальны в условиях восстановления пассажиропотока после постепенного снятия ограничений Covid-19. Стремясь достичь докризисного уровня интенсивности круизных судов и пассажиропотока, необходимо включать вероятностные процессы в модели управления портом. Необходимо производить оценку не только на основе имеющегося расписания судозаходов, но и оценивать различные варианты на основе моделирования с учетов вероятностных процессов. Ввиду увеличения размеров круизных и паромных судов перед многими портами стоит задача модернизации системы причалов. В качестве объекта исследования был выбран регион Балтийского моря. Объектом исследования был выбран поток круизных и паромных судов морского пассажирского порта Санкт-Петербурга "Морской фасад". В результате исследования представлена новая стохастическая модель и проведено сравнение результатов с известными законами распределения. На основе полученных данных определена надежная область принятия решений по интенсивности круизных линий и необходимости модернизации инфраструктуры. Предлагаемая модель формируется на оценке динамики нестационарной интенсивности движения с последующим применением корреляционно-регрессионного анализа и последующим исследованием характеристик случайной функции, описывающей интервалы между отдельными прибытиями круизных судов. Далее полученные данные используются для оптимизационных экспериментов в программной среде *AnyLogic* для моделирования годовой ситуации с целью комплексной оценки работы морского порта и принятия решения по модернизации причалов.
***Ключевые слова*:** транспортные процессы, математическое моделирование, паромная сеть, стохастическая модель, модернизация инфраструктуры, морской пассажирский порт, принятие решений

A. A. Dobrovolskaia*
Assistant
N. N. Maiorov*
PhD. Sc., Tech., Professor
M. R. Yazvenko*
Laboratory Assistant
*St. Petersburg State University of Aerospace Instrumentation

RESEARCH OF VARIANTS OF MODERNIZATION OF TRANSPORT TERMINAL INFRASTRUCTURE BASED ON STOCHASTIC MODELS

Modern passenger ports and terminals (main transport hubs) require the development of new models and methods for effective work planning and accurate forecasting of infrastructure development today. Such key transport infrastructure point as development of sea passenger ports, their modernization, and changes in route cruise and ferry networks are especially relevant in conditions of passenger traffic recovery after gradual lifting of Covid-19 restrictions. In an effort to achieve pre-crisis levels of cruise ship and passenger traffic, it is necessary to incorporate stochastic processes into port management models. It is necessary to make an assessment not only based on the existing schedule of ship arrivals, but also to evaluate various options based on modeling with regard to probabilistic processes. In view of increase in size of cruise and ferry vessels, many ports face the task of modernization of berths. The Baltic Sea region was chosen as an object of research. The flow of cruise and ferry vessels of the sea passenger port "Passenger port St. Petersburg "Sea Facade" was chosen as an object of research. As a result of the research a new stochastic model was presented and the results were compared with known distribution laws. Based on the obtained data a reliable decision-making area on cruise lines intensity and the necessity of infrastructure modernization is defined. The proposed model is formed on the estimation of the dynamics of non-stationary intensity of traffic with subsequent application of correlation-regression analysis and subsequent investigation of the characteristics of the random function describing the intervals between individual arrivals of cruise ships. Then the obtained data are used for optimization experiments in the software environment AnyLogic for modeling the annual situation for the purpose of complex assessment of the seaport operation and making decisions on modernization of berths.
***Keywords**:* transport processes, mathematical modeling, ferry network, stochastic model, infrastructure modernization, sea passenger port, decision making

Введение

Актуальность проблемы исследования обусловлена постоянно возрастающей ролью морских пассажирских портов в мировых транспортно-экономических системах. Кризисные явления и усиление конкуренции между морскими портами во всех звеньях логистических сетей создают растущее экономическое давление на операционную деятельность каждого из них, что требует увеличения портовых мощностей. Текущая ситуация имеет очень сложный характер, связанный с внешней средой, оказывающей существенное влияние на морскую паромную и круизную индустрию. Переход от известных детерминированных моделей в сфере исследования пассажирских морских перевозок к разработке вероятностных моделей, сегодня находится в центре внимания. Необходимо отметить, что данная проблема особенно актуальна при строительстве нового морского пассажирского терминала или модернизации нескольких причалов, при ситуации, когда один причал может использоваться как для паромного судна, так и для грузового. Руководителям пассажирских морских терминалов необходимо решать проблему стратегического развития для максимизации пассажиропотока и увеличения интенсивности круизных и паромных судов, изменения положения порта в регионе моря и на рынке пассажирских перевозок. В статье [1] предлагается модель и метод на основе диаграмм *Circos* для определения положения порта по отношению к другим.

Известно, что реализация долгосрочных целей устойчивого развития морских пассажирских перевозок, достижение желаемых результатов, преодо-

ление негативного воздействия факторов нестабильной внешней среды определяется выбранным курсом, заложенным в основу стратегического управления. В связи с пандемией COVID-19 глобальная круизная мобильность приостановилась, чего нельзя сказать о локальной мобильности. Именно локальная мобильность сегодня дает возможность возобновить регулярное движение как можно быстрее. К таким регионам, следует отнести регион Балтийского моря.

Морские пассажирские порты и терминалы требуют разработки новых моделей и методов на основе имитационного моделирования для оценки путей модернизации инфраструктуры, оценки эффективности портовых операций для эффективного планирования работы и точного прогнозирования развития морского пассажирского порта. Также следует отметить, что актуальными являются вопросы модернизации портовой инфраструктуры и околотерминального городского транспортного пространства и исследование моделей взаимодействия систем "круизная компания – морской пассажирский порт – город". Эти вопросы актуальны для портов, которые активно модернизируют инфраструктуру, внедряют новые логистические услуги и, как следствие, меняют как свое положение в регионе и на рынке, так и повышают привлекательность города и страны.

Имитационное моделирование необходимо использовать при принятии решения о модернизации морских пассажирских портов ввиду возможности оценки различных сценариев. Несмотря на известный график прибытия судов в порт в начале навигации, для модернизации инфраструктуры необходимо моделировать различные варианты загруженности причалов. В данной работе предлагается использовать стохастическое моделирование как один из вариантов учета различных сценариев для определения различных вариантов загрузки причалов. При этом проверка предлагаемого математического аппарата производится на основе известных данных расписаний судозаходов. На основе выполненного исследования, как приведено в работах [2, 3], предлагаемый вариант значительно повышает точность принятия решения по модернизации инфраструктуры морского пассажирского порта.

Анализ загруженности причалов морского пассажирского порта

Основными исходными параметрами для исследования инфраструктуры морского порта являются входящий поток круизных и паромных судов, размеры круизных и паромных судов, их пассажировместимость, время швартовки и обработки, маршрутные паромные сети. При начальном строительстве каждого морского порта широко используются аналитические модели [1, 2]. Они соответствуют нормативному количеству причалов и интенсивности прибытия судов. Как правило, через определенный промежуток времени возникает необходимость изменить инфраструктуру порта, увеличить причалы для возможности швартовки более крупных круизных судов. В статье авторов [3] на основе детального анализа таких моделей как *Anyport*, *Workport*, *Three generations* [3, 4, 5] представлены различные модели развития морских пассажирских портов, характеризующиеся различными уровнями развития маршрутных транспорт-

ных сетей. На основе анализа этих моделей определена необходимость исследования интенсивностей входного потока круизных и паромных судов и определения зависимости от портовой инфраструктуры. К примеру, с точки зрения привлечения новых круизных маршрутов руководителям портов необходимо точное понимание возможностей портовой инфраструктуры. Эта проблема должна решаться только путем моделирования и разработки новых цифровых транспортных моделей, которые позволят решить задачу прогнозирования развития морского порта с учетом факторов внешней среды и возможных стохастических процессов.

Ключевую роль в таких исследованиях должны играть стохастические модели, которые учитывают фактор неопределенности и характеризуют его влияние на деятельность порта. Использование этих моделей позволяет повысить надежность работы портовой системы. Несмотря на существование графиков прибытия судов, развитую координацию расписаний и планов, при решении проблемы прогнозирования развития необходимо переходить к моделированию различных сценариев, которые базируются на цифровых транспортных моделях. Транспортный поток оказывает прямое влияние на процессы работы порта. Прежде всего, необходимо оценить имеющуюся интенсивность судозаходов круизных и паромных судов. На рис. 1 приведена статистика прибытий судов в пассажирский порт Санкт-Петербург "Морской фасад", когда проводилась навигация с 2015–2019 годов (по имеющимся данным расписания [7]).

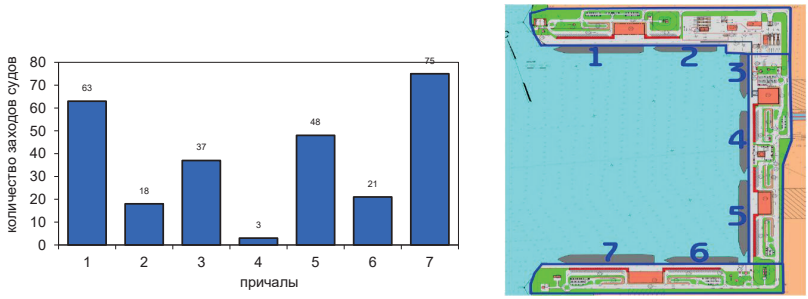


Рис. 1. Распределение прибытий круизных и паромных судов в "Пассажирский порт Санкт-Петербург "Морской фасад", схема причалов морского порта (1–7 причалы)

На основе известного графика судов был выполнен анализ размеров круизных и паромных судов и их распределение по причалам. Результат выполненного анализа представлен на рис. 2.

На основе анализа размеров и тоннажа круизных судов было установлено, что большинство круизных судов имеют длину более 218 м, почти половина из них – более 288 м. Следовательно, нагрузка на причалы № 1 и № 7 в морском порту должна быть повышенной для крупных судов. Кроме того, эти причалы находятся ближе всего к морю, что упрощает маневрирование судов. Это

подтверждает диаграмма распределения судов по причалам, представленная на рис. 1.

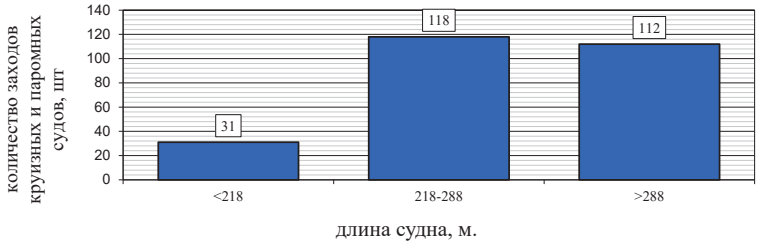


Рис.2. Анализ длины круизных и паромных судов для пассажирского порта Санкт-Петербурга "Морской Фасад"

На основе анализа погрузочных причалов было установлено, что крупные суда длиной от 218 до 288 м швартуются у причалов № 3 и 5. Такая конфигурация может принять наибольшее количество крупных лайнеров в порту. Причал № 4 очень редко принимает суда, только 3 в течение 2019 года.

Стохастическая модель прибытия круизных судов в морской пассажирский терминал

Моделирование различных вариантов заходов круизных и паромных судов необходимо выполнять для прогнозирования и обоснования будущих изменений инфраструктуры порта [2, 3, 8]. Классическая модель оценки интенсивности движения основана на пуассоновском законе распределения [9, 10] (или к примеру, на основе моделей систем массового обслуживания), следовательно, интервал между прибытиями судов подчиняется экспоненциальному распределению с плотностью:

$$f_k(t) = \lambda e^{-\lambda t}, \tag{1}$$

Известно, что пуассоновский поток является стационарным, ординарным и не имеет последействия. Если круизные суда работают на линии, то время прибытия (захода) в порт известно с определенной точностью. Тем не менее, не исключено действие неблагоприятных случайных факторов, которые могут привести к задержке прибытия круизного судна, а также возможность относительно небольших отклонений от расписания. На самом деле интенсивность движения может изменяться под воздействием различных факторов внешней среды. При моделировании в цифровой среде *Anylogic* за счет вычислительных мощностей можно рассматривать не только стационарный поток, но и стохастический, учитывающий последействие различных внешних факторов. В расчетах это можно учесть, рассматривая прибытие судов на основе гамма-распределения. Для этого можно использовать как значения интенсивности на выбранных временных интервалах, так и ее значения для каждой пары "сосед-

них" прибытий судов (в этом случае значение является обратным интервалу между ними). Получив функцию интенсивности, можно переходить к анализу нестационарного судопотока. Рассмотри предлагаемую математическую модель в следующем виде:

$$f(t_v) = \frac{\lambda(t_0 + t_v) \cdot (\Lambda_{t_0, t_0 + t_v})^{r-1} e^{-\Lambda_{t_0, t_0 + t_v.}}}{\Gamma(r)}, \qquad (2)$$

где $t_v \geq 0$ – интервал между приходами круизных судов; λ – интенсивность входящего потока судов; r – закон распределения ($r > 0$); $\Gamma(r)$ – гамма-распределение.

Результаты моделирование количества судозаходов с использованием вероятностных моделей

Для выполнения исследования была создана специализированная новая имитационная модель в программной среде *Anylogic* [11]. Данная модель характеризуется большой детализацией инфраструктры морского пассажирского порта. На основе исходных данных были проведены эксперименты с различными интенсивностями прибытий круизных и паромных судов в соответствии с различными типами математических распределений. Время швартовки судов распределено в соответствии с распределением. При реализации модели были использованы следующие варианты моделирования:

1) моделирование работы морского пассажирского порта на основе известного расписания прибытия круизных и паромных судов за прошедшие периоды (за основу были взяты данные открытых расписаний);

2) моделирование различных вариантов интенсивности прибытия круизных и паромных судов в порт. В данном случае использовались нормальный, экспоненциальный законы распределения и было предложено использовать Гамма-распределение.

Моделирование основано на известных месяцах навигации применяло для проверки работы модели. При таком подходе правильность модели сначала проверяется с использованием данных из известных расписаний работы портов, к примеру, в 2018 и 2019 годах. Проведение таких экспериментов подтвердило корректность модели.

Затем была проведена серия экспериментов с учетом вероятностных процессов прибытия круизных судов в порт. Например, время моделирования составляет 1 год, а для прибытия судов в 2019 году взята средняя интенсивность – 265 судов в год.

Результаты моделирования с учетом различных законов распределения приведены в табл. 1.

Чтобы оценить необходимость принятия решений для модернизации инфраструктуры и принятия решений, необходимо с достаточной точностью знать возможные колебания входного потока круизных и паромных судов. Наибольшую точность даст объединение доверительных интервалов всех

распределений, поэтому на выходе получится доверительный интервал, удовлетворяющий всем распределениям. Такой интервал будет наиболее точно предсказывать возможное количество судов, заходящих в морской пассажирский порт.

Таблица 1

Результаты моделирования различной интенсивности круизных судов

Количество экспериментов	Гамма распределение (общее количество судов)	Распределение Пуассона (общее количество судов)	Нормальное распределение (общее количество судов в год)
1	247	263	249
2	289	221	240
3	240	269	242
4	297	273	264
5	280	320	284
6	264	317	266

Результаты моделирования различных интенсивностей заходов судов в порт приведены на рис. 3.

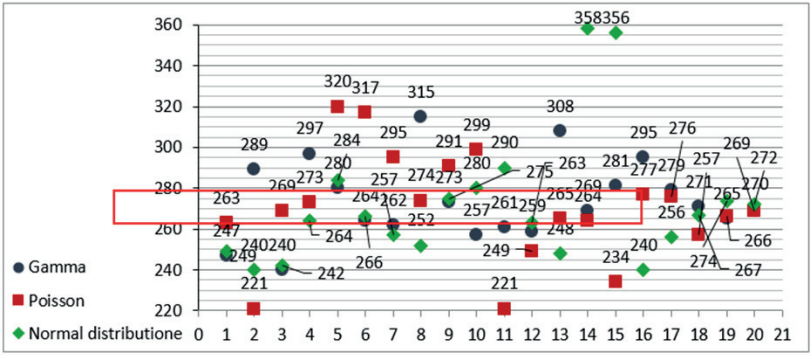


Рис. 3. Комбинированные экспериментальные результаты моделирования судозаходов круизных и паромных судов при использовании Пуассоновского распределения, Нормального распределения и Гамма распределения

На основе проведенной серии экспериментов выделен доверительный интервал, который отражает ситуацию загруженности причалов и интенсивностей работы для морского пассажирского порта. На основе полученных результатов открывается возможность произвести оценку загруженности причалов при различных вариантах влияния внешней среды.

Заключение

На основы выполненных экспериментов можно определить, что вероятности состояний порта близки к экспериментальным значениям загрузки. Наибольшая интенсивность круизных и паромных судов была достигнута при использовании гамма-распределения.

По результатам моделирования был спрогнозирован интервал возможных колебаний количества судов, прибывающих в пассажирский морской терминал в течение года. Прогноз был сделан с учетом фактической структуры судопотока за последние годы навигации по значению интенсивности 2019 года. Прогнозирование возможных колебаний потока судов, особенно в условиях современной эпидемиологической ситуации, позволяет снизить неопределенность и заранее подготовиться к принятию соответствующих управленческих решений, в том числе и по модернизации инфраструктуры, в морских пассажирских портах в настоящее время. Решение этой задачи является весьма актуальным для судоходства 2022 года и последующих лет, поскольку включает в себя стохастические процессы, обусловленные влиянием внешней среды. Практическая реализация разработанной модели может быть применена в других морских пассажирских портах и терминалах, что позволяет говорить о возможности широкого применения предлагаемого в работе исследования. Разработанная цифровая имитационная модель обладает качественной детализацией выполнения и точность воспроизведения операционных процессов морского пассажирского порта. Приведенное решение и разработанную модель можно применять для других транспортных терминалов.

Библиографический список

1. Maiorov N. N. Work analysis of maritime passenger terminals for particular region based on circos plot. / N. N. Maiorov, S. Krile // Naše more. 2019. Vol. 66. No 2. Pp. 57–61. DOI: 10.17818/NM/2019/2.2.

2. Maiorov N. N. Simulation of the route network and ferry traffic intensity based on the process of discretization and circos plot intensity diagram / N. N. Maiorov, V. A. Fetisov, S. Krile, D. Miskovic // Transport Problems. 2019. Vol. 14 (Issue 4). Pp. 21–31. DOI: 10.20858/tp.2019.14.4.2.

3. Krile S., Maiorov N., Fetisov V. Modernization of the Infrastructure of Marine Passenger Port Based on Synthesis of the Structure and Forecasting Development. Sustainability. 2021. Vol. 13. 3869. https://doi.org/10.3390/su13073869.

4. Bin K. L. Port development. New York. UNCTAD. 1985. 228 p.

5. Bird J. Seaports and Seaport Terminals; Hutchinson University Library: London, UK. 1980.

6. UNCTAD. Port marketing and the Challenge of the Third Generation Port. New York: UNCTAD. 1994. 55 p.

7. Пассажирский порт Санкт-Петербург «Морской фасад». URL: https://www.portspb.ru/O_porte/about (дата обращения 20.01.2022).

8. Chen M. J., Nijkamp P. Itinerary planning: Modeling cruise lines' length of stay in ports. International Journal of Hospitality Management, 2018. Vol. 73. Pp. 55–63. https://doi.org/10.1016/j.ijhm.2018.02.005.

9. Майоров Н. Н., Фетисов В. А. Практические задачи моделирования транспортных систем. СПб.: ГУАП, 2012. 186 с.

10. Бродецкий Г. Л. Системный анализ в логистике. Принятие решений в условиях неопределенности. М.: Academia. 2010. 336 с.

11. Anylogic. URL: https://www.anylogic.ru/ (дата обращения: 22.01.2022).

УДК 004.056.55

К. В. Епифанцев*
кандидат технических наук, доцент
М. М. Шишкова*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АСПЕКТЫ РАЗРАБОТКИ ВИРТУАЛЬНОГО ВОЛЬТМЕТРА НА БАЗЕ МИКРОКОНТРОЛЛЕРА ATMEGA 8

Возможность обеспечения высокой точности измерений напряжения является важной задачей, находящей множество прикладных применений в промышленности и науке. В настоящее время широко используются виртуальные приборы для моделирования различных электронных схем. Эти приборы обладают определенной точностью, которая исследуется в данной работе. Актуальность работы заключается в необходимости повышения качества измерений напряжения в средах создания моделей принципиальных электрических схем, оценки погрешностей этих виртуальных схем в сравнении с реальными прототипами.
Ключевые слова: виртуальный измерительный прибор, *Proteus*, *Multisim*, погрешность измерений

K. V. Epifantsev*
PhD, Tech., Associate Professor
M. M. Shishkova*
Student
*St. Petersburg State University of Aerospace Instrumentation

ASPECTS OF THE DEVELOPMENT OF A VIRTUAL VOLTMETER BASED ON THE ATMEGA 8 MICROCONTROLLER

The ability to provide high accuracy voltage measurements is an important task that finds many applications in industry and science. Currently, virtual instruments are widely used to simulate various electronic circuits. These devices have a certain accuracy, which is investigated in this paper. The relevance of the work lies in the need to improve the quality of voltage measurements in the environment for creating models of circuit diagrams, assessing the errors of these virtual circuits in comparison with real prototypes.
Keywords: virtual measuring instrument, Proteus, Multisim, measurement uncertainty.

В процессе разработки виртуальных измерительных приборов, необходимо проанализировать вопрос сходимости измерений между созданным прототипом и реально существующим прибором, необходимо рассчитать величину погрешности, чтобы впоследствии виртуальному прототипу присвоить класс точности, дать возможность прибору войти в реестр средств измерений.

В современном производстве, мы имеем проблемы с качеством работы приборов, которые зависят от ряда погрешностей (например, пыль, вибрация, влажность и т. д.). Использование виртуальных измерительных приборов решило бы данные проблемы.

Из приведенных выше типов вольтметра для реализации на макетной плате и создания виртуальной модели мною был выбран цифровой электронный вольтметр VOLTCRAFT MXD-4660A (рис. 1).

Мультиметр VOLTCRAFT MXD-4660A характеризуется высокой точностью измерений и большой разрешающей способностью. Разрядность данного мультиметра составляет 19 999 отсчетов, 10 ячеек памяти используется для фиксирования результатов измерений.

Погрешность при измерении постоянного напряжения в диапазоне от 200 мВ до 200 В составляет ±0,05%. Исходя из этого, можно предположить, что измерения данного лабораторного мультиметра очень точны и их можно принять за эталонные для сравнения с показаниями вольтметра. Созданный прибор показан на рис. 1. Он собран на макетной плате, смоделирован в программной среде *Proteus*.

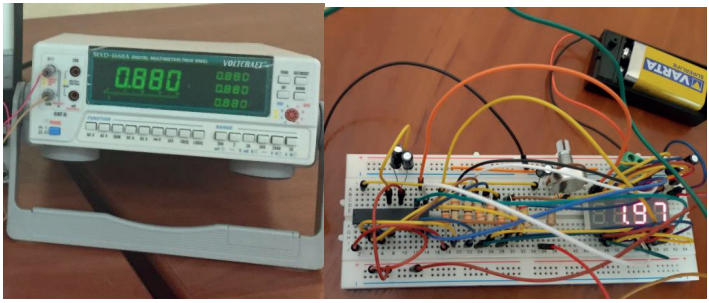


Рис. 1. Созданный макет мультиметра с прототипом в виртуальном виде (справа) и мультиметр лабораторный VOLTCRAFT MXD-4660A (слева)

При создании прототипа в качестве основного интеллектуального модуля используется микроконтроллер *ATmega*8 [2], представленный на рис. 2. Его выбор обусловлен низкой стоимостью и надежностью.

*ATmega*8 создан по технологии КМОП. Данная технология предполагает задействование биполярных транзисторов с изолированным затвором – это позволяет существенно уменьшить энергопотребление по сравнению с технологий ТТЛ. Быстродействие – 1 MIPS на 1 МГц рационально по отношению цена/энергоемкость.

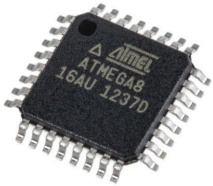


Рис. 2. Микроконтроллер ATmega8

Создание программного обеспечения (ПО) устройства осуществлялось на языке *C* в среде *Atmel Studio* 6 от компании *Atmel*. Это бесплатная интегрированная среда разработки (IDE) для создания программ для микроконтроллеров семейства ARM и AVR, функционирующая в операционной системе *Windows* 10. *Atmel Studio* включает в себя компилятор *C/C++* и симулятор, который дает возможность проверить работоспособность программы без загрузки в микроконтроллер. Интерфейс среды разработки *Atmel Studio* 6 приведен на рис. 3.

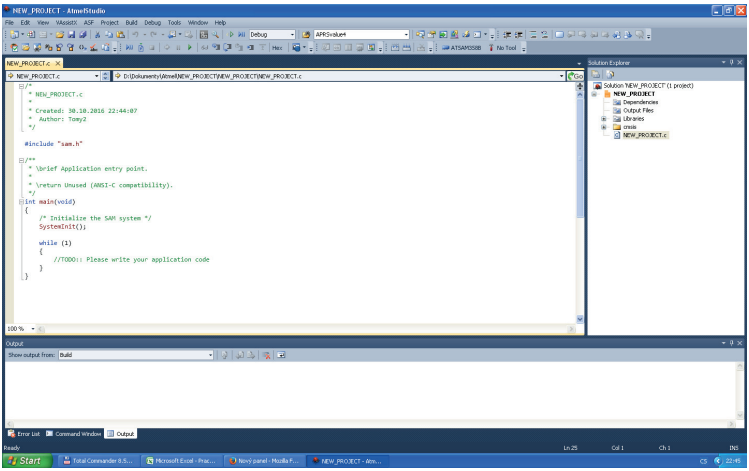


Рис. 3. Интерфейс среды разработки Atmel Studio 6

Созданная программа микроконтроллера позволяет проводить обработку сигнала, поступающего с делителя напряжения на порт PC4, и затем выводить информацию на экран семисегментного индикатора.

В программе *Proteus 8 Professional* была создана виртуальная модель исследуемого вольтметра [3]. После создания схемы и загрузки прошивки в микроконтроллер появляется возможность запустить симуляцию в *Proteus* 8 *Professional*. Процесс симуляции приведен на рис. 4.

Светодиодный индикатор показывает значение измеряемого напряжения 17,04 В, однако на встроенном вольтметре отображается 17 В. Это значит, что присутствует определенная погрешность. Для ее снижения используется переменный резистор RV2.

В процессе исследования были проведены измерения в лаборатории с использованием лабораторного мультиметра VOLTCRAFT MXD-4660A, источника питания GW Instek GPC – 6030D и вольтметра, собранного на макетной плате. Процесс измерений представлен на рис. 5. В процессе измерений была поставлена задача исключить метрологический отказ, который свойственен для подобного типа оборудования. Метрологический отказ – выход метрологических характеристик средства измерений за установленные пределы. В данной

методике метрологический отказ был исключен за счет применения электронных приборов [4].

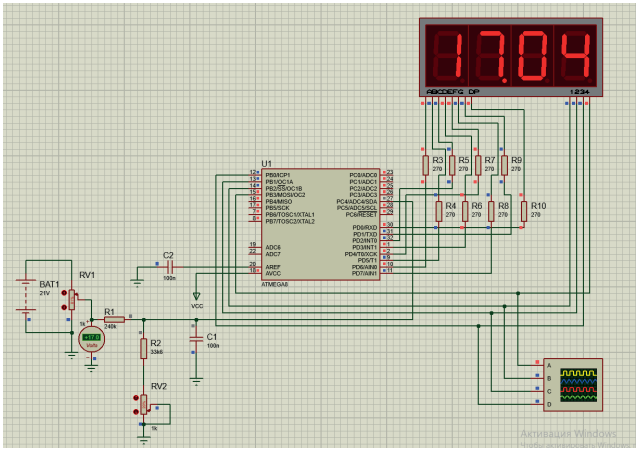


Рис. 4. Процесс симуляции

Рис. 5. Процесс измерений

Полученные результаты измерений, а также расчет погрешностей приведены на рис. 6 и 7.

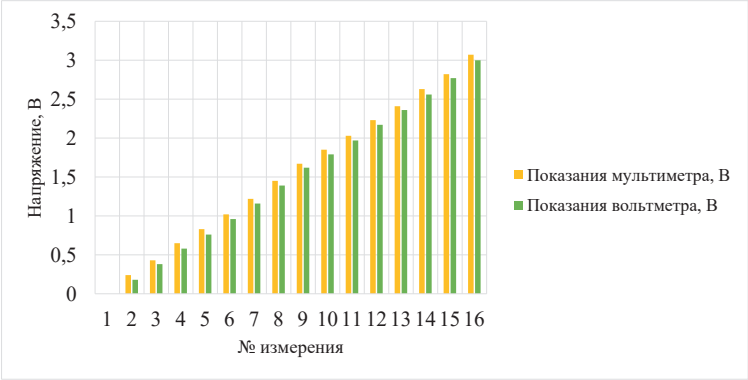


Рис. 6. Результаты измерений лабораторного мультиметра и собранного вольтметра

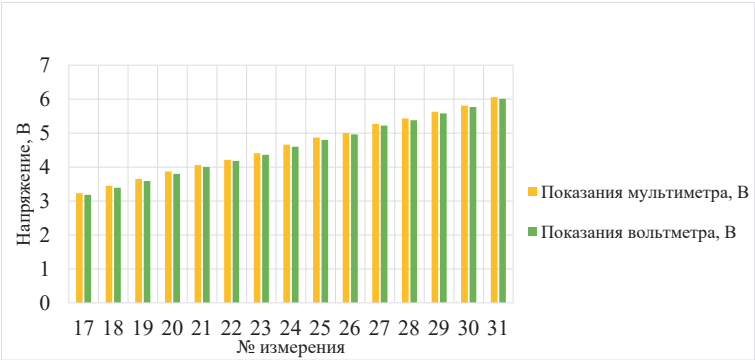


Рис. 7. Результаты измерений лабораторного мультиметра и собранного вольтметра

Всего было проведено 31 измерение в диапазоне 0–6 В с шагом 0,2 В. Второй столбец представляет собой напряжение на генераторе.

Пример расчета абсолютной погрешности в измерении № 3:

$$\Delta V = \left|V_{\text{ИЗМ}} - V_{\text{Д}}\right| = \left|0,38 - 0,43\right| = 0,05B.$$

В данном случае в формулу добавлен модуль, потому что интерес представляет величина погрешности, а не в какую сторону (отрицательную или положительную) она отклоняется.

Пример расчета относительной погрешности в измерении № 3:

$$\delta V = \frac{\Delta V}{V_Д} = \frac{0,05}{0,43} \cdot 100\% = 11,63\%.$$

В начале измерений относительная погрешность достаточно велика (25% в измерении № 2, 11,6% в измерении № 3), однако по мере увеличения значения напряжения эта погрешность начинает уменьшаться (0,83% в измерении № 31). Объясняется это тем, что среднее значение абсолютной погрешности 0,05 В с отклонением не больше 0,02 В, однако ее вклад в точность измерений при увеличении значения напряжения уменьшается.

Действия по измерению напряжения аналогично, были проведены для виртуальной модели вольтметра в программе *Proteus*8 *Professional.* Результаты представлены на рис. 8, 9.

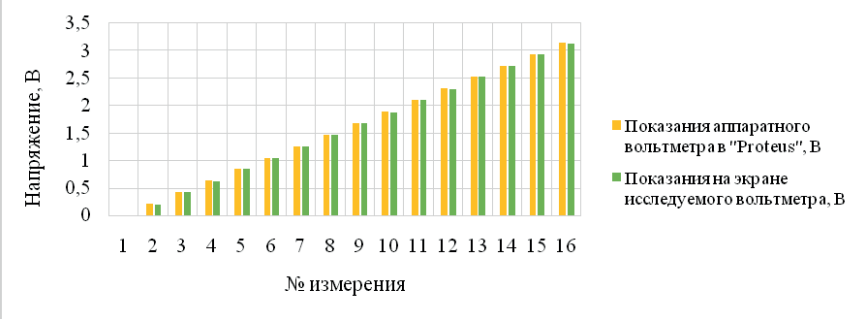


Рис. 8. Результаты измерений виртуального вольтметра и аппаратного вольтметра в Proteus

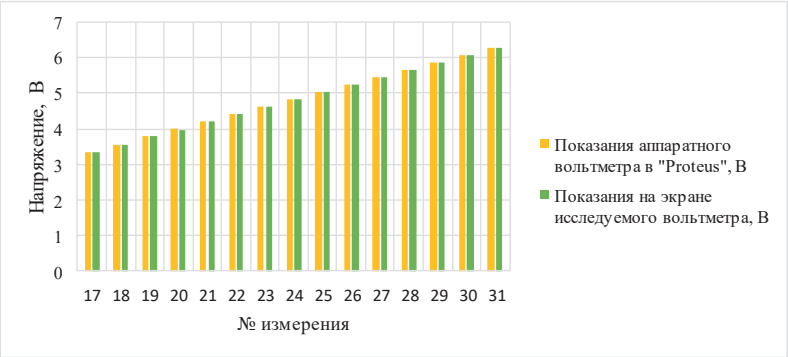


Рис. 9. Результаты измерений виртуального вольтметра и аппаратного вольтметра в Proteus

В качестве генератора сигнала использовалась виртуальная модель из батареи 21 В и переменного резистора, средством для измерения действительного значения напряжения выступил аппаратный вольтметр, встроенный в среду *Proteus*. Всего было проведено 31 измерение в диапазоне 0–6 В с шагом 0,2 В.

Пример расчета абсолютной погрешности в измерении № 4:

$$\Delta V = \left| V_{\text{ИЗМ}} - V_{\text{Д}} \right| = \left| 0,62 - 0,63 \right| = 0,01B.$$

В данном случае в формулу добавлен модуль, потому что интерес представляет величина погрешности, а не в какую сторону (отрицательную или положительную) она отклоняется.

Пример расчета относительной погрешности в измерении № 3:

$$\delta V = \frac{\Delta V}{V_{\text{Д}}} = \frac{0,0}{0,63} \cdot 100\% = 1,59\%.$$

Рассчитанные средние значения абсолютной погрешности соответственно равны 0,5 В для вольтметра и 0,01 В для модели. Можно сделать вывод, что показания виртуального прибора точнее в 5 раз! Были также вычислены средние значения относительной погрешности. Для вольтметра средняя относительная погрешность составила 3,53%, а для виртуальной модели – 0,37%. Следовательно, относительная погрешность виртуальной модели прибора меньше в 9,5 раз.

Анализ результатов измерений показывает, что виртуальная модель является более точной по сравнению с вольтметром, реализованным на макетной плате. Это происходит по некоторым причинам. Во-первых, сборка на макетной плате не способна обеспечить хорошее соединение между элементами. Из-за этого возникает переходное сопротивление, влияющее влияет на качество измерений. Во-вторых, устройство подвержено влиянию различного электромагнитного излучения, радиоволн и прочих помех, которые мешают получить нужное значение напряжения. В-третьих, благодаря современным вычислительным алгоритмам моделирование в программе *Proteus* 8 *Professional* позволяет измерить напряжение более точно, чем в случае с реальным прибором.

Однако определенная погрешность имеется также и в виртуальной модели. Это вызвано недостаточно точной настройкой калибровочного резистора RV2 в модели [1].

Библиографический список

1. Деярова Н. Я. Электрорадиоизмерения: учеб. пособие / Сост. преподавателем КС ПГУТИ Н. Я. Деяровой. Самара: КС ПГУТИ, 2016. 7,8 п. л.

2. Temirbekova Z. E. Programming microcontroller AVR ATMEGA8 / Под редакцией Б. М. Ибраева // В сборнике: Материалы XLI Международной научно-практической конференции. 2017. С. 102–104.

3. Основы метрологии: учеб. пособие / В. В. Окрепилов, Ю. А. Антохина, А. А. Оводенко, Е. Г. Семенова, В. Ш. Сулаберидзе, А. Г. Чуновкина. СПб.: ГУАП, 2019. 485 с.

4. Маркарян Л. В. Схемотехника цифровой электроники: лабораторный практикум. Москва: Изд. Дом НИТУ «МИСиС», 2018. 74 с. URL: https://znanium.com/catalog/product/1239510 (дата обращения: 20.05.2021).

УДК 656.073.2

О. А. Изотов*
кандидат технических наук
А. Л. Кузнецов**
доктор технических наук, профессор
*Санкт-Петербургский государственный университет аэрокосмического приборостроения
**Государственный университет морского и речного флота имени адмирала С.О. Макарова

МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ В СИСТЕМЕ ТРАНСПОРТИРОВКИ СБОРНЫХ ГРУЗОВ

Выявлены закономерности, влияющие на загрузку транспортной сети и представлена модель поведения транспортной системы, включающей в оборот новые средства укрупнения малых партий грузов. Показано, что в условиях внедрения новых средств укрупнения грузовых мест, грузы будут перевозиться по той же транспортной сети, но принципиально будет обеспечена возможность привлечения видов транспорта, способных расширить границы применения контейнерных технологий в глубину тыловых территорий. Целью моделирования транспортных потоков при организации перевозки сборных грузов с применением внутриконтейнерных модулей является установление связи между основными характеристическими и переменными: скоростью перевозок; плотностью перевозок; пропускной способностью участков. Связь между независимыми переменными обеспечивается через консолидированный транспортный поток. В качестве основного критерия оценки результатов моделирования выбрана совокупная стоимость передвижения грузов всеми видами транспорта. Расчет корреспонденций и их расщепление предлагается проводить последовательно, с опорой на известную загрузку сети. Полученные результаты показывают снижение нагрузки на транспортную сеть в результате применения новых средств укрупнения сборных грузов.
Ключевые слова: сборные грузы, моделирование транспортных процессов, загрузка транспортной сети, транспортный поток, распределение потока.

O. A. Izotov*
PhD, Tech.
A. L. Kuznetsov**
Dr. Sc. Tech., Professor
*St. Petersburg State University of Aerospace Instrumentation
**Admiral Makarov State University of Maritime and Inland Shipping

SIMULATION OF TRANSPORT FLOWS IN ASSEMLED CARGO TRANSPORTATION SYSTEM

The regularities affecting the loading of the transport network are revealed and a model of the behavior of the transport system is presented, which includes new means of enlarging small shipments into circulation. It is shown that in the conditions of the introduction of new means of enlarging cargo spaces, cargo will be transported along the same transport network, but in principle it will be possible to attract modes of transport that can expand the boundaries of the use of container technologies into the depths of the rear territories. The purpose of modeling traffic flows in the organization of transportation of combined cargoes with the use of container modules is to establish a relationship between the main characteristic and variables: the speed of transportation; the density of transporta-

tion; the capacity of sections. The connection between independent variables is provided through a consolidated traffic flow. The total cost of cargo transportation by all modes of transport is chosen as the main criterion for evaluating the simulation results. The calculation of correspondence and their splitting is proposed to be carried out sequentially, based on the known network load. The results obtained show a reduction in the load on the transport network as a result of the use of new means of consolidation of combined cargoes.
Keywords: combined loads, modeling of transport processes, loading of the transport network, traffic flow, flow distribution

Введение

В работе [1] было описано конструктивное решение, позволяющего расширить границы контейнерной транспортно-технологической системы в направлениях концевых участков консолидации/распределения (так называемой «последней мили») за счет введения новой транспортной единицы или «субконтейнера». Исследования авторов показывают, что внедрение в оборот новых средств укрупнения малых парий грузов повлечет изменение загрузки транспортной сети [2]. Оценка таких изменений представляет собой сложную комплексную задачу, решение которой требует не только расчетно-аналитических методов, но и моделирования поведения транспортной системы, задействованной под подобную перевозку [3].

В качестве цели моделирования транспортных потоков при организации перевозки сборных грузов с применением внутриконтейнерных модулей [4] выбрано установление взаимосвязи между основными характеристическими переменными соответствующего транспортного процесса:

V – скоростью перевозок;

P – плотностью перевозок;

q – пропускной способностью участков.

При этом, связь между независимыми переменными обеспечивается через совокупный транспортный поток Q.

Методы и материалы

Первый шаг в традиционном подходе к анализу транспортного потока состоит в поиске стационарных (независимых от времени) связей между q, P и V, который чаще всего принимает форму построения так называемых фундаментальных диаграмм. Как правило, решение задачи в такой постановке возможно лишь для малых промежутков времени, а получаемые результаты расчетов при этом сильно колеблются [5, 6].

Вторым шагом процедуры анализа транспортных потоков является оценка динамики перевозок, т. е. описание протекающих процессов в зависимости от затраченного времени [7].

В соответствии с этим, задача анализа транспортной сети как системы, в которой циркулируют транспортные потоки, так же разбивается на два основных этапа:

1. Оценка общих объемов прибытия и отправления грузов на терминалы и территории порта.

2. Распределение грузопотока по способам транспортировки грузов в глубь хинтерленда.

С внедрением новых средств укрупнения грузовых мест, грузы будут перевозиться по той же транспортной сети, поскольку ее конфигурация в первую очередь зависит от центров формирования спроса и предложения. В работах [8, 9] показано, что принципиально измениться только возможность привлечения видов транспорта, способных обеспечить применение контейнерных технологий в глубину территорий грузового тяготения (хинтерленда). Условно это показано на рис. 1.

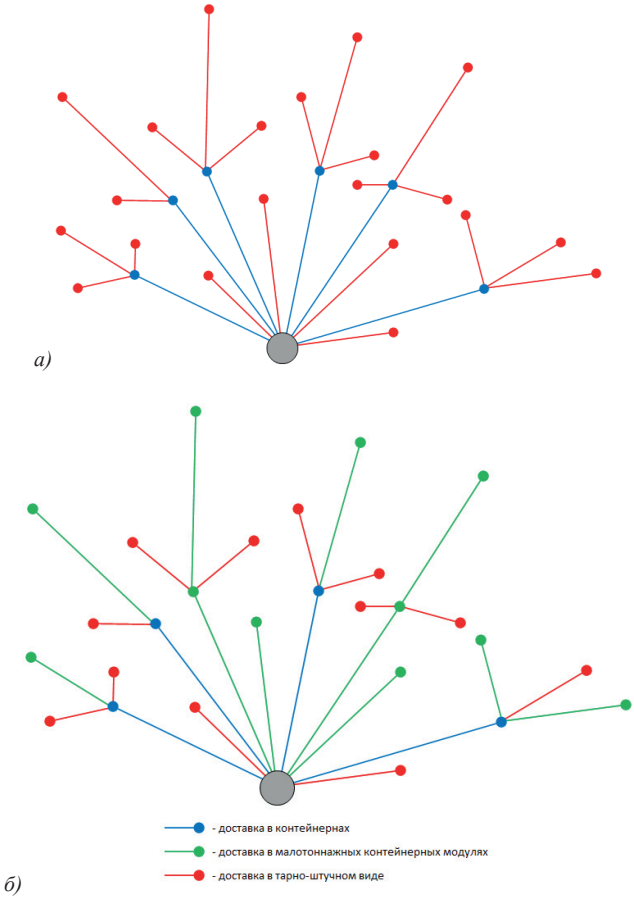


Рис. 1. Изменение способов организации транспортировки сборных грузов: а – существующими средствами укрупнения; б – с внедрением внутриконтейнерных модулей

Для формализации описания потоков введем следующие переменные и обозначения.

Доля (весовая) от объема перевозок грузов видами транспорта до внедрения новых средств укрупнения:

$$r = 1 - \gamma - g, \tag{1}$$

где g – доля перевозок грузов железнодорожным транспортам; γ – доля перевозок грузов автомобильным транспортом; r – доля грузов отправляемая территории морского термина в контейнерах.

Доля от объема перевозок грузов с применением новых видов укрупнения малых партий грузов может быть выражена через формулу:

$$r' = 1' - \gamma' - g', \tag{2}$$

где g' – доля грузов, перевозимых во внутриконтейнерных модулях; γ' – доля грузов, перевозимых в тарно-штучном виде; r' – доля грузов отправляемая с территории морского термина в контейнерах.

Третий шаг, это построение матриц корреспонденций, характеризующих объемы перевозок с применением различных видов укрупнения грузовых мест. Распределение грузопотоков по способам укрупнения грузовых мест при организации завоза в тыловые территории морского порта приведено в табл. 1.

Таблица 1

Распределение грузопотоков по способам укрупнения грузовых мест при организации завоза в тыловые территории морского порта

Доля от поступившего грузооборота	В контейнерах	Во внутри-контейнерных модулях	В тарно-штучном виде
	на 1–2 сутки нахождения груза на тыловой территории		
До внедрения новых средств укрупнения	0,8	–	0,2
После внедрения новых средств укрупнения	0,4	0,4	0,2
	на 3-4 сутки нахождения груза на тыловой территории		
До внедрения новых средств укрупнения	0,2	–	0,6
После внедрения новых средств укрупнения	0,2	0,4	0,2
	на 5–6 сутки нахождения груза на тыловой территории		
До внедрения новых средств укрупнения	–	–	0,4
После внедрения новых средств укрупнения	–	0,2	0,2

Четвертый шаг, это распределение корреспонденций по транспортной сети, т.е. определение путей и видов транспорта по участкам пути. Такое распределение задачи моделирования на рассматриваемые этапы носит условный характер, поскольку все этапы взаимосвязаны и не могут быть решены как отдельные задачи в силу описанных обратных связей. Так, в рассматриваемой модели расчета корреспонденций в качестве основного фактора может быть использована цена передвижения грузов видами транспорта. Отсюда, расчет корреспонденций и их расщепление может быть проведено последовательно с опорой на известную загрузку сети. При этом, задача может быть решена последовательными приближениями, повторяя шаги в итеративном режиме.

Обсуждение

Наиболее простая модель этого типа, а именно гравитационная модель, использует представление о системе материальных точек, масса которых отображает объем релевантного грузопотока. Все пары точек связаны между собой силами притяжения F_{ij}, величина которой зависит от их масс m_i и m_j, и разделяющего их транспортного расстояния l_{ij} друг от друга:

$$F_{ij} = k\frac{m_i m_j}{l^2_{ij}}, \tag{3}$$

где k – некоторая масштабирующая константа.

Полную транспортная гравитационная модель интенсивности перевозки партий грузов в тыловые территории порта, использующую идею гравитационной модели, предлагается построить с использование обобщенного притяжения:

$$N_{ij} = Q\cdot[(1-g-y)\frac{\text{Р}_{\text{конт}}T_{\text{конт}}V_{\text{конт}}}{S^2_{\text{конт}}} + g\frac{\text{Р}_{\text{мод}}T_{\text{мод}}V_{\text{мод}}}{S^2_{\text{мод}}} + \gamma\frac{\text{Р}_{\text{тшг}}T_{\text{тшг}}V_{\text{тшг}}}{S^2_{\text{тшг}}}], \tag{4}$$

где T – время перевозки грузов с применением различных средств укрупнения грузов; S – стоимость перевозки грузов между пунктами i и j с применением различных средств укрупнения грузов; Q – грузопоток.

Теперь модель распределения $\sum_{i=1}^{I}\sum_{j=1}^{J} N_{ij}$ можно рассматривать как функцию от плотности перевозок P_{ij}, дальности перевозок грузов L_{ij} и стоимости перевозки S_{ij}.

Если предположить, что плотность отправки грузов с территории морского терминала величина постоянная и не зависит от вида средств укрупнения грузовых мест, то в дальнейших расчетах ею можно пренебречь.

Собственно процесс моделирования состоит в расчете системы показателей для различных конфигураций точек образования и поглощения грузопотоков, призванного доказать преимущества использования новой системы и опре-

делить границы соответствующих областей. Для решения этой задачи было разработано специализированное программное обеспечение в среде VBA.

В качестве исходных данных для вариантов расчета использовались сгенерированные данные, отражающие топологические и массовые характеристики реальных грузопотоков. Пример таких данных приведен в табл. 2.

Таблица 2

Исходные данные для расчетов

Вид укрупнения груза	Исходные данные			Расстояние, на которое может быть доставлен груз, км				Стоимость перевозки груза на то же расстояние, руб. за 1 т			
	Вес, т	Цена, руб./т-км	Скорость перевозки, км/сут	2	4	6	8	2	4	6	8
ТШГ	1,5	10,0	400	800	1600	2400	3200	8000	16000	24000	32000
модуль	5,0	6,0	550	1100	2200	3300	4400	6600	13200	19800	26400
контейнер	20,0	6,0	550	1100	2200	–	–	6600	13200	–	–

Результаты

Проведенные расчеты показывают снижение нагрузки на транспортную сеть после применения новых средств укрупнения сборных грузов в зоне хинтерленда (рис. 2).

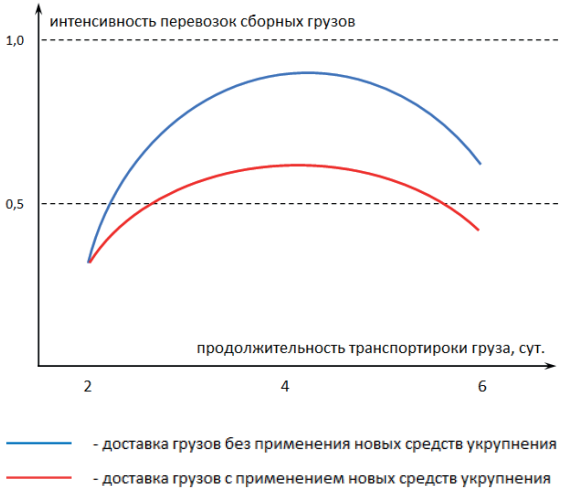


Рис. 2. Изменение интенсивности перевозок малых партий грузов в хинтерленде

Снижение нагрузки на транспортную сеть происходит за счет максимального приближения доставки сборной партии грузов с применением контейнерных технологий к пункту дислокации конечного потребителя товаров. В результате сокращается плечо подвоза таких грузов от тылового центра консолидации и распределения грузопотоков, в качестве которых с внедрением новых средств укрупнения сборных партий, смогут выступать не только грузовые станции и специализированные логистические центры способные принимать к обработке тяжеловесные контейнеры, но и малые станции, обеспечивающие обработку среднетоннажных и малых контейнеров. Приближение преимуществ контейнерных технологий к заказчику товаров сократит пробег автомобильного транспорта, количество погрузо-разгрузочных операций в промежуточных пунктах перевалки, что приведет и к сокращению общих издержек по транспортировке грузов.

В результате границы транспортных систем обеспечивающие оборот контейнеризированных грузов в тыловой зоне прибрежных терминалов могут быть существенно расширены без затрат на формирование или совершенствование транспортной инфраструктуры, участвующей в продвижении сборных партий товаров. Прогнозирование перевозок требует учета и других факторов, на что было обращено внимание в других статьях по данной теме [10, 11, 12].

Библиографический список

1. Изотов О. А. Определение сфер и границ применения новых средств укрупнения сборных грузов в контейнерных перевозках / О. А. Изотов, А. Л. Кузнецов // Транспортное дело России. 2020. № 2 (147). С. 164–166.

2. Изотов О. А. Перспективы развития технологий перевозки сборных грузов в контейнерах / О. А. Изотов, А. Л. Кузнецов // Вестник АГТУ. Серия: Морская техника и технология. 2020. № 1. С. 140–148.

3. Семенов В. В. Математическое моделирование динамики транспортных потоков мегаполиса. М.: ИПМ им. М.В. Келдыша РАН, 2004. 45 с.

4. Изотов О. А. Патент на полезное модель № 207180 «Складной грузовой контейнер» / О. А. Изотов, А. Л. Кузнецов. М.: ФСИС, 2021.

5. Agyemang-Duah K., Hall F. L. Some issues regarding the numerical value of free capacity, in Highway Capasity and Level of Service // edited by U. Brannolte. Balkema, Rotterdam, 1991.

6. Hall F. L., Allen B. L., Gunter M. A. Empirical analysis of freeway flow-density relationships // Transpn, Res. 1986.

7. Lighthill M. J., Whitham G. B. On kinematic waves // Proc. R. Soc. Lond. Washington, D. C. Highway Research Board, National Research Counsil, 1964. Vol. 1–3.

8. Изотов О. А. Технологические решения для организации отправок сборных грузов посредством контейнерных транспортно-технологических систем / О. А. Изотов, А. В. Кириченко, А. Л. Кузнецов // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. Т. 11. № 4. С. 609–620. DOI: 10.21821/2309-5180-2019-11-4-609-620.

9. Вильсон А. Дж. Энтропийные методы моделирования сложных систем. М.: Наука, 1978. 248 с.

10. Изотов О. А. Организация погрузо-разгрузочных работ новых единиц укрупнения сборных грузов // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. Т. 11. № 5. С. 813–822. DOI: 10.21821/2309-5180-2019-11-5-813-822.

11. Изотов О. А. Преимущества внедрения новых средств укрупнения сборных грузов в контейнерные перевозки // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. Т. 11. № 6. С. 1037–1043. DOI: 10.21821/2309-5180-2019-11- 6-1037-1043.

12. Изотов О. А. Перспективы экспедирования морских контейнерных перевозок / О. А. Изотов, А. Л. Кузнецов, А. В. Гультяев // Транспортное дело России. 2019. № 4. С. 130–133.

УДК 656.7

А. С. Костин*
аспирант
Ю. А. Силин*
студент
А. В. Бахмутская*
кандидат экономических наук
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

РАЗРАБОТКА ИЗОТЕРМИЧЕСКОГО КОНТЕЙНЕРА ДЛЯ РЕАЛИЗАЦИИ ДОСТАВКИ СПЕЦИАЛЬНЫХ ГРУЗОВ ПРИ ПОМОЩИ БЕСПИЛОТНОЙ АВИАЦИОННОЙ СИСТЕМЫ

В данной статье выполнен анализ существующих решений для доставки специальных грузов при помощи беспилотных авиационных систем, выведены основные требования к полезной нагрузке для беспилотной авиационной системы и выполнена практическая реализация устройства. На базе лаборатории беспилотных авиационных систем ГУАП выполнены лабораторные испытания изотермического контейнера, описаны полученные результаты.
***Ключевые слова*:** беспилотные авиационные системы, дрон, квадрокоптера, контейнер.

A. S. Kostin*
PhD Student
Y. A. Silin*
Student
A. V. Bahmutskaya*
PhD, Economic
*St. Petersburg State University of Aerospace Instrumentation

DEVELOPMENT OF AN INSULATED CONTAINER FOR THE IMPLEMENTATION OF THE DELIVERY OF SPECIAL CARGO USING AN UNMANNED AERIAL SYSTEM

This article analyzes existing solutions for the delivery of special cargo using unmanned aerial systems, derives the basic requirements for the payload for an unmanned aerial system, and performs a practical implementation of the device. On the basis of the laboratory of unmanned aerial systems of the SUAI, laboratory tests of an isothermal container were carried out, and the results obtained were described.
Keywords: unmanned aerial systems, drone, quadcopter, container.

Введение

Различные методы доставки грузов с помощью беспилотных авиационных систем постепенно внедряется в городские транспортные системы, прорабатываются как сами дроны и их системы навигации, так и разрабатываются законы и методы их регистрации и сопровождения в воздушном пространстве. Одной из важных особенностей беспилотных авиационных систем является

возможность доставить груз в труднодоступные районы за короткий срок. Таким грузом могут быть:

1. Биологические материалы, вакцины, медикаменты или питание в клиники, больницы или непосредственно пострадавшим от стихийных бедствий [1, 5].
2. Доставка почты, товаров и других небольших грузов [1, 5].
3. Доставка товаров из магазинов (включая еду и напитки).

Для реализации доставки медицинских грузов, помимо разработки беспилотной авиационной системы и ее систем навигации, необходимо разработать сам контейнер, внутри которого будут хранится медикаменты. При этом сам контейнер должен поддерживать определенную температуру и иметь возможность работать в автономном режиме, без использования бортовой сети дрона. В некоторых случаях требуется полная стабилизация контейнера во время доставки и отсутствие каких-либо вибраций [6, 7].

Медикаменты обычно доставляются в термоизоляционном пенопластовом контейнере, в некоторых случаях наполненном сухим льдом. Перед достижением точки назначения беспилотник снижается до 25–30 метров над землей и осуществляет сброс контейнера на бумажном парашюте. Погрешность приземления груза составляет не более пяти метров [1, 5, 8].

Данная система работы имеет следующие недостатки:

1. Низкая маневренность беспилотника самолетного типа, что делает невозможным его использование в городской среде.

2. Невозможность регулирования температуры медикаментов при транспортировке, что может привести к их порче. В случае с использованием сухого льда, при его таянии возникает большое количество углекислого газа, что так же может негативно сказаться на сохранности груза.

Для реализации проекта транспортировки медицинских грузов при помощи квадрокоптера, необходимо разработать контейнер, который будет отвечать следующим общепринятым в мире ключевым требованиям [1, 2]:

1) осуществление транспортировки в специальных контейнерах, поверхности которых подлежат очистке и обеззараживанию;

2) поддержание определенного температурного режима в процессе транспортировки от 2°C до 8°C;

3) валидация – проверка правильности монтажа конструкций и документального соответствия.

В рамках данной статьи рассмотрим пример реализации изотермического контейнера для доставки медикаментов.

На основании анализа проектов крупных компаний, а также опираясь на общепринятые правила транспортировки медицинских грузов, были сформированы следующие требования к разрабатываемому прибору [3]:

1) возможность вмещать в себя некоторое количество колб высотой 75 мм;

2) возможность поддержания заданной температуры в течение определенного времени. Нижняя допустимая граница 2°C;

3) использование вентиляторов во избежание нагревания от внешней среды частей груза, находящихся в отдалении от радиатора;

4) устойчивость к вибрациям;

5) наличие термоизоляционных стенок у грузового отсека;

6) герметичность.

Вопросы разработки конструкции грузового контейнера

Для повышения энергоэффективности, прибор для транспортировки крови должен работать в режиме теплокомпенсации и термоса второго рода. Режим теплокомпенсации будет активен до тех пор, пока температура внутри грузового отсека не достигнет нижней допустимой границы температуры 2°С. После ее достижения, охлаждающий элемент будет выключен и будет активен режим теплокомпенсации до тех пор, пока температура внутри грузового отсека не поднимется до верхней допустимой границы температуры 8°С, после чего охлаждающие элементы будут снова включены. Режим охлаждения не подходит, так как груз в контейнер будут помещать уже в кондиционном состоянии, т. е. охлаждать его не потребуется.

Конструкция должна быть разработана таким образом, чтобы охлажденный воздух от радиатора в первую очередь шел вдоль стенок грузового отсека и компенсировал их нагревание от внешней среды.

Далее рассмотрим компоненты разработанной полезной нагрузки:

Для наиболее оптимального соотношения веса и производительности были выбраны следующие электронные компоненты: микроконтроллер *Arduino nano*; элементы Пельтье TEC1-12703 – 2 шт.; элементы Пельтье TEC1-12703 – 2 шт.; DC-DC преобразователи – 2 шт.; вентиляторы – 4 шт.; датчик температуры DS18B20 – 1шт., транзистор IRF3205PBF – 1 шт.; OLED дисплей – 1 шт. На рис. 1 представлена принципиальная электронная схема контейнера.

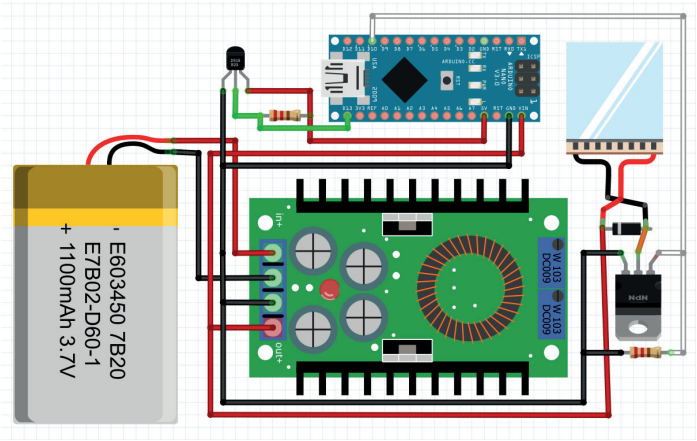


Рис. 1. Принципиальная электронная схема контейнера

Прибор состоит из двух основных частей – верхней и нижней. Верхняя часть включает в себя электронные компоненты и имеет конструкцию, позволяющую направлять холодный воздух от радиаторов на воздухораспределительную корзину, находящуюся в грузовом отсеке. Нижняя часть является грузовым отсеком. Обе части соединяются при помощи петли и замка. На верхней части установлен резиновый уплотнитель для герметичности.

Грузовой отсек напечатан с двойными стенками для создания внутри воздушной прослойки, которая улучшит термоизоляцию и уменьшит его вес.

Прибор имеет следующий принцип работы: на микроконтроллер с термодатчика приходит значение температуры и выводится на дисплей. Если оно выше нижней допустимой границы, то микроконтроллер подает сигнал на транзистор, включая тем самым элементы Пельтье. На каждом элементе Пельтье установлен радиатор с вентилятором на горячей части для ее охлаждения и повышения эффективности работы. На холодной части элемента так же установлен радиатор с вентилятором, для создания воздушного потока в грузовом отсеке. Питание прибора осуществляется через силовой разъем XT60 [1, 2].

Вентиляторы работают всегда. На горячей стороне элементов Пельтье для предотвращения нагрева радиаторов на холодной стороне, а на холодной стороне для перемешивания слоев воздуха в грузовом отсеке, что будет поддерживать одинаковую температуру во всех его частях.

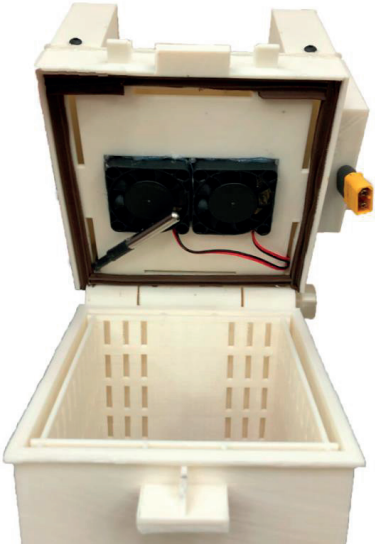


Рис. 2. Внешний вид контейнера в открытом состоянии

Для работы контейнера, а также для указания определенной температуры, был разработано программное обеспечение для микроконтроллера на базе Ar-

duino. Благодаря программному обеспечению поддерживается заданная оператором температура и есть возможность проверить температуру внутри контейнера в режиме реального времени. Ниже представлен фрагмент программного кода:

```
#include <GyverOLED.h>
#include <OneWire.h>
OneWire ds(9); //
GyverOLED<SSD1306_128x64, OLED_NO_BUFFER> oled;
void setup() { }
void loop() {
  byte data[2];
 ds.reset();
 ds.write(0xCC);
 ds.write(0x44);
 delay(1000);
 ds.reset();
 ds.write(0xCC);
 ds.write(0xBE);
  data[0] = ds.read();
 data[1] = ds.read();
 float temperature = ((data[1] << 8) | data[0]) * 0.0625;
 Serial.println(temperature);
 oled.init();
 oled.clear();
 oled.setScale(2);
 oled.home();
 oled.print("temp=");
 oled.print(temperature);
 if (temperature>7) {
  analogWrite(2, 255);
 }
 if (temperature<4) {
  analogWrite(2, 0);
  }
```

После окончательной сборки, отладки программного кода и настройки работы контейнера, были выполнены лабораторные испытания.

Исследование температурных режимов при выполнении полетов

Лабораторные испытания производились без груза и без подвешивания к квадрокоптеру. Данное исследование проводится в ГУАП на базе лаборатории беспилотных авиационных систем ГУАП при финансовой поддержке Министерства науки и высшего образования Российской Федерации (соглашение № FSRF-2020-0004 «Научные основы построения архитектур и систем связи бор-

товых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств»).

Прибор будет работать в режиме охлаждения для измерения полезной работы за 20 минут. Источником энергии служил блок питания с выставленным напряжением 16,8 В. Температура внешней среды 22°С.

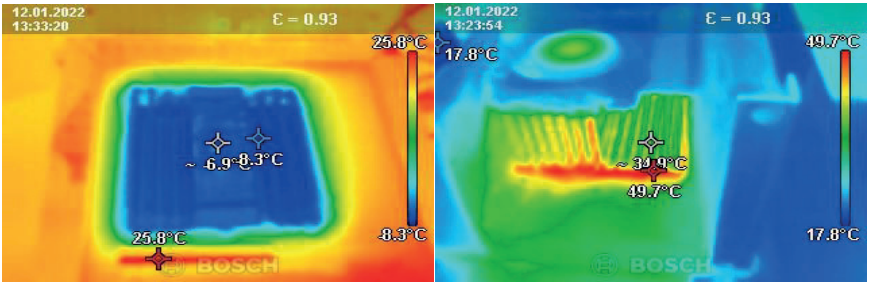


Рис. 3. Температуры работы холодной и горячей части элемента Пельтье

В условии полета на квадрокоптере, температура в грузовом отсеке будет опускаться быстрее, так как радиаторы с горячей стороны элементов Пельтье дополнительно будут охлаждаться сильным потоком воздуха от пропеллеров.

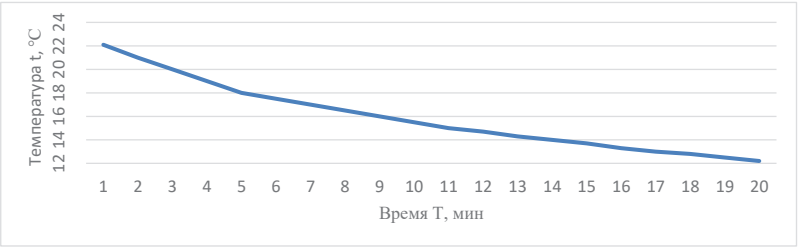


Рис. 4. График изменения температуры

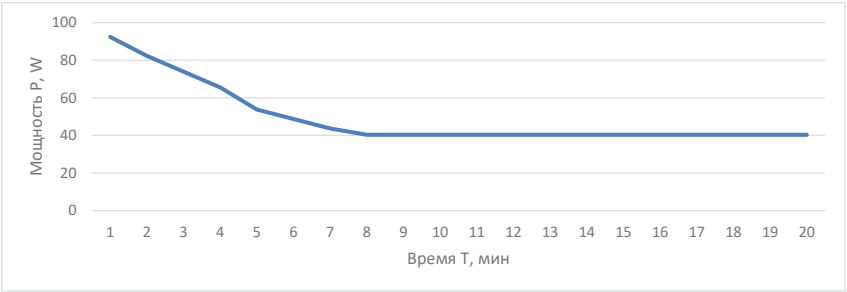


Рис. 5. График изменения потребляемой мощности

Замер изменения температуры в контейнере производился в течении T = 20 минут. Начальное значение температуры $t_н$ = 22°С, конечное значение $t_к$ = 12°С. Объем воздуха внутри контейнера принят m_1 = 0,01 м^3, при удельной теплоемкости c_1 = 1290 Дж/м^3. Объем пластика, учувствовавшего в охлаждении, принят m_2 = 0,4 кг при удельной теплоемкости c_2 = 1900 Дж/кг. Напряжение, потребляемое прибором U = 16,8 В, сила тока принята I = 2,5 А.

Для расчетов использовались следующие формулы:

1. Формула для измерения кол-ва теплоты при охлаждении:

$$Q = c \times m \times (t_н - t_к), \tag{1}$$

где Q – количество теплоты; c – удельная теплоемкость; m – масса или в случае с газами объем; $t_н$ – начальная температура; $t_к$ – конечная температура.

2. Формула расчета мощности:

$$P = U \times I, \tag{2}$$

где P – мощность; U – напряжение; I – сила тока.

3. Формула расчета КПД:

$$\eta = \frac{Q_1 + Q_2}{\frac{P \times 3600}{3}} \times 100, \tag{3}$$

где 3600 – количество работы, совершаемое 1 Вт за час;

Расчет по ф-ле (1) количества энергии, потребовавшейся для охлаждения воздуха: 1290 × 0,01 × (22 – 12) = 129 Дж.

Расчет по ф-ле (1) количества энергии, потребовавшейся для охлаждения пластика: 1900 × 0,4 × (22 – 12) = 7600 Дж.

Расчет по ф-ле (2) мощности, потребляемой прибором: 16,8 × 2,5 = 42 Вт.

Расчет КПД по ф-ле (3):

$$\frac{129 + 7600}{\frac{42 \times 3600}{3}} \times 100 = 15{,}3\%.$$

Полезная мощность прибора на данный момент равна 2,14 Вт. В безоблачную погоду солнечная энергия, учитывая площадь контейнера и коэффициент отражения пластика сможет разогревать поверхность контейнера с мощностью до 4 Вт, что означает, что контейнеру может не хватить мощности для осуществления теплокомпенсации. Следовательно, необходимо изменить коэффициент отражения света контейнера при помощи специальной краски или фольги.

Заключение

Для повышения эффективности прибора нужно уменьшить теплопроводность стенок, создав внутри вакуумные полости. Для повышения эффективности работы элементов Пельтье нужно установить большие по размерам и лучшие по качеству радиаторы на горячей части, что уменьшит ее температуру и

температуру холодной части. Можно изменить форму воздухораспределительной корзины, что улучшит циркуляцию воздуха в грузовом отсеке.

Использование небольшого количества хладагента, который будет храниться в холодильнике вместе с медикаментами и при необходимости транспортировки будет помещаться в прибор, поможет уменьшит энергопотребление прибора за счет аккумуляции холода и постепенной его отдачи.

Библиографический список

1. Силин Ю. А. Анализ аппаратных комплексов для доставки особо важных грузов с помощью беспилотных авиационных систем // Системный анализ и логистика: журнал. Вып. № 3 (29), ISSN 2077-5687. СПб.: ГУАП., 2021. С. 9–14. DOI: 10.31799/2077-5687-2021-3-9-14.

2. Силин Ю. А. Разработка охлаждающего контейнера способного поддерживать заданную температуру при транспортировке // Системный анализ и логистика: журнал. Вып. № 2 (28), ISSN 2077-5687. СПб.: ГУАП, 2021. С. 97–103. DOI: 10.31799/2077-5687-2021-2-97-103.

3. Требования к контейнеру для транспортировки донорской крови [gburospk]. URL: http://gburospk.ru/vracham/transportirovka-donorskoy-krovi-i-ee-komponentov.php (дата обращения: 01.02.2022).

4. Слободчиков Н. А. Грузоведение / Н. А. Слободчиков, Д. В. Кочнев, О. А. Диняк; ред. В. А. Фетисов. СПб.: ГУАП, 2013. 432 с.

5. Майоров Н. Н. Исследование маршрутизации полетных заданий беспилотных авиационных систем для операционных складских задач / А. С. Костин, Н. Н. Майоров, Е. А. Вознесенский, Н. В. Богатов // Сб. докл. второй Международной научной конференции «Аэрокосмическое приборостроение и эксплуатационные технологии». ГУАП. 2021. С. 130–137. DOI: 10.31799/978-5-8088-1554-4-2021-2-130-137.

6. Maiorov N. N. Control and analysis of quadcopter flight when setting a complex trajectory of motion / N. N. Maiorov, N. Bogatov, A. Kostin, // Journal of Physics: Conference Series 1925 (2021). 012043. IOP Publishing. DOI:10.1088/1742-6596/1925/1/012043.

7. Карпова Т. Ю. Эксплуатация беспилотных авиационных систем / Т. Ю. Карпова, А. С. Костин, Н. Н. Майоров. СПб.: ГУАП, 2021. 69 с.

8. Engel J. Accurate figure flying with a quadrocopter using onboard visual and inertial sensing / J. Engel, J. Sturm, D. Cremers // Proc. of the Workshop on Visual Control of Mobile Robots (ViCoMoR) at the IEEE/RJS Intern. Conference on Intelligent Robot Systems (IROS). Vilamoura, Algarve, Portugal, 2012. Pp. 43–48.

УДК 656.7

А. С. Костин*
аспирант
Ю. А. Силин*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОСОБЕННОСТИ ДОСТАВКИ СПЕЦИАЛЬНЫХ ГРУЗОВ В ИЗОТЕРМИЧЕСКОМ КОНТЕЙНЕРЕ ПРИ ПОМОЩИ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

В данной статье рассмотрены особенности реализации доставки специальных грузов в изотермическом контейнере при помощи беспилотной авиационной системы с учетом анализа существующих решений, были определены основные требования к беспилотной системе, а также описан алгоритм доставки груза. На базе лаборатории беспилотных авиационных систем выполнены лабораторные испытания доставки грузов на дронпоинты.
***Ключевые слова*:** беспилотные авиационные системы, дрон, квадрокоптер, доставка груза.

Исследование проводится в ГУАП на базе лаборатории беспилотных авиационных систем ГУАП при финансовой поддержке Министерства науки и высшего образования Российской Федерации (соглашение № FSRF-2020-0004 «Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств»).

A. S. Kostin*
PhD Student
Y. A. Silin*
Student
*St. Petersburg State University of Aerospace Instrumentation

FEATURES OF THE DELIVERY OF SPECIAL CARGOES IN AN INSULATED CONTAINER USING UNMANNED AERIAL SYSTEMS

This article discusses the features of the implementation of the delivery of special cargo in an isothermal container using an unmanned aerial system, taking into account the analysis of existing solutions, the main requirements for an unmanned system were determined, and the cargo delivery algorithm was described. On the basis of the laboratory of unmanned aerial systems, laboratory tests were carried out for the delivery of goods to drone points.
***Keywords*:** unmanned aerial systems, drone, quadcopter, cargo delivery.

Введение

При возникновении аварий или чрезвычайных ситуаций, в которых человек становится жертвой, очень часто может потребоваться доставка медикаментов и других специальных грузов пострадавшему. В машине скорой помощи, которая первая прибывает на место происшествия хранятся медикаменты для

оказания экстренной помощи, однако в машинах скорой помощи не перевозится, например кровь, так как в данных автомобилях нет соответствующего оборудования и неизвестна группа крови пострадавшего [1, 2].

Альтернативой может стать использование беспилотных летательных аппаратов, которые в течение короткого промежутка времени смогу доставить нужный груз прямо к месту происшествия, что может повысить скорость оказания первой помощи пострадавшим [1, 2].

В апреле 2019 года открылся первый распределительный центр в Гане, принадлежащий компании *Zipline*. Данная компания занимается беспилотной авиадоставкой медикаментов в труднодоступные места. На момент начала 2022 года компания совершила уже более двух миллионов успешных доставок. Для доставки используется беспилотник самолетного типа с грузоподъемностью 1,75 кг. Радиус охвата одного распределительного центра составляет 80 км [2].

Запуск беспилотника осуществляется с помощью пусковой установки, которая за секунду позволяет разогнать его до 110 км/ч, что позволяет сэкономить заряд аккумулятора. Для безопасности на беспилотнике продублированы все системы, а также установлен парашют для экстренных ситуаций.

Медикаменты доставляются в термоизоляционном пенопластовом контейнере, в некоторых случаях наполненном сухим льдом. Перед достижением точки назначения беспилотник снижается до 25–30 метров над землей и осуществляет сброс контейнера на бумажном парашюте. Погрешность приземления груза составляет не более пяти метров [2].

Данная система работы имеет следующие недостатки [3]:

1. Низкая маневренность беспилотника самолетного типа, что делает невозможным его использование в городской среде.

2. Невозможность регулирования температуры медикаментов при транспортировке, что может привести к их порче. В случае с использованием сухого льда, при его таянии возникает большое количество углекислого газа, что так же может негативно сказаться на сохранности груза.

Модели и методы формирования полетных заданий

Анализируя работу существующей компании, было принято решение использовать квадрокоптеры в качестве беспилотников, так как они могут маневрировать среди зданий на низких скоростях и имеют возможность вертикального взлета и посадки без специальных пусковых установок.

Предполагаемый принцип работы во время чрезвычайных происшествий, следующий:

1. Экипаж скорой помощи, прибывший на место происшествия, определяет необходимость доставки специальных медицинских грузов.

2. При необходимости доставки специальных медицинских грузов, экипаж создает запрос на доставку специальных медицинских грузов.

3. В ближайшем медицинском центре, при поступлении запроса, осуществляется комплектация квадрокоптера.

4. Квадрокоптер летит до места происшествия по наиболее оптимальному маршруту с учетом посадок в промежуточных пунктах для замены аккумулятора в случае необходимости. В случае если место чрезвычайного происшествия не входит в радиус покрытия доставки квадрокоптером, то маршрут строится таким образом, чтобы осуществить передачу в том месте, где скорая помощь будет входить в радиус покрытия воздушной доставки по пути в больницу [4].

5. Посадка квадрокоптера в месте чрезвычайного происшествия может осуществляться как автономно, так и при помощи дистанционного ручного пилотирования [4, 5].

6. После отгрузки специальных медицинских грузов, квадрокоптер возвращается в стартовую точку.

Когда дрон достигает места доставки, он исследует поверхность в нужном месте для безопасной посадки, производит посадку, затем отпускает груз, тем самым завершая доставку.

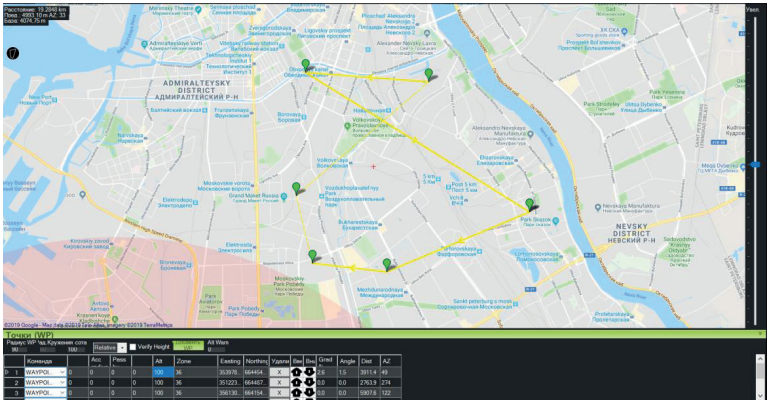


Рис. 1. Схема обработки заявки по доставке груза

Построение оптимальной полетной миссии для доставки груза можно осуществить при помощи теории графов с применением метода пути максимальной эффективности с учетом штрафов.

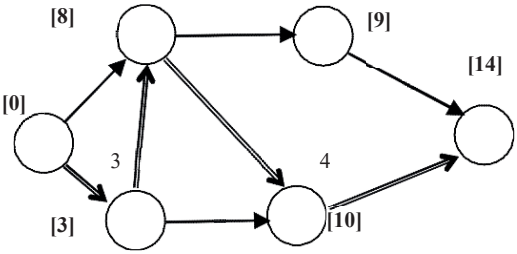


Рис. 2. Пример графа маршрута доставки

Пусть для каждой дуги (n + 1)-вершинной сети заданы два числа: эффект Эij и время tij. Каждый путь μ из начальной вершины в конечную вершину характеризует некоторый процесс доставки грузов беспилотной авиационной системой. Под продолжительностью пути будем понимать сумму времен его дуг. Если продолжительность доставки отличается от заданного времени T, то налагаются штрафы χ(μ), пропорциональные отклонению, т. е.

$$\chi(\mu) = \begin{cases} \alpha(T - T(\mu)), T(\mu) \le T \\ \beta(T(\mu) - T), T \le T(\mu) \end{cases},$$

где коэффициенты α и β могут быть как положительными, так и отрицательными.

Задача заключается в том, чтобы найти путь μ*, максимизирующий разность между эффектом и штрафами, т. е.

$$\mu^* = \arg\max\,[Э(\mu) - \chi(\mu)].$$

Обозначим $lij(\lambda)$ = Эij – λ tij, где λ – некоторый параметр, $T(\lambda)$ – продолжительность оптимального пути при параметре λ, т. е. пути, имеющего максимальную длину, измеряемую в $lij(\lambda)$. Легко показать, что с ростом λ величина $T(\lambda)$ не возрастает.

Обозначим $T(\alpha)$, $T(\beta)$ – продолжительности оптимального пути при λ равном α и, соответственно, β; μ(α), μ(β) – эти пути (для их нахождения необходимо решить две задачи на поиск пути максимальной длины). Рассмотрим шесть случаев (исходную задачу можно разбить на две подзадачи – поиска максимума Э(μ) – χ(μ) при $T(\mu) \le T$ и при $T(\mu) \ge T$).

Пусть α ≥ β, тогда $T(\beta) \ge T(\alpha)$ и:

если $T(\beta) \ge T(\alpha) \ge T$, то μ(β) – оптимальное решение;

если $T \ge T(\beta) \ge T(\alpha)$, то μ(α) – оптимальное решение;

если $T(\beta) \ge T \ge T(\alpha)$, то, сравнивая μ(α) и μ(β) по длинам l = Э – χ, выбираем путь, имеющий максимальную длину.

Пусть α ≤ β, тогда $T(\beta) \le T(\alpha)$ и:

если $T(\alpha) \ge T(\beta) \ge T$, то μ(β) – оптимальное решение;

если $T \ge T(\alpha) \ge T(\beta)$, то μ(α) – оптимальное решение;

если $T(\alpha) \ge T \ge T(\beta)$, то задача не имеет эффективных методов решения.

Для реализации проекта транспортировки медикаментов при помощи квадрокоптера, необходимо разработать контейнер, который будет отвечать следующим общепринятым в мире ключевым требованиям [1]:

1) осуществление транспортировки в специальных контейнерах, поверхности которых подлежат очистке и обеззараживанию;

2) поддержание определенного температурного режима в процессе транспортировки от 2°С до 8°С;

3) валидация – проверка правильности монтажа конструкций и документального соответствия.

В лаборатории беспилотных авиационных систем инженерной школы ГУАП на базе исследовательского летного поля была решена задача дистанционной доставки грузов с использованием специализированных точек доставки – дронпоинтов. Условия доставки заключались в формировании маршрута до двух дронпоинтов и реализации сброса определенного груза на каждой точке. Квадрокоптер должен был выполнить точную посадку на дронпоинт с последующим сбросом груза и осуществление световой индикации [6, 7]. Для решения задачи была написана программа на языке *Python* и выполнен код автономного полета с посадками, сбросами грузов, взлетами и возвращениями в начальные точки маршрута [7].

Необходимо было разработать новую приборную часть подвеса, схемы подключения и выполнить реализацию алгоритмов работы. На основе полученных решений необходимо было получить модель, которую можно применить и для других полезных нагрузок данного типа.

Для навигации квадрокоптера «Клевер» во время взлета, посадки и выполнения полетной миссии используется *frame_id* – система координат для значений x, y, z, v_x, v_y, v_z. Для взлета применяется система координат *body* – координаты относительно квадрокоптера без учета наклонов по тангажу и крену [8]. Во время использования данной системы координат считываются данные с датчиков, которые находятся в полетном контроллере без использования камеры, так как камера находится слишком близко к маркеру и распознать его не получится. Во время выполнения полетной миссии используется система координат *aruco_N* – координаты относительно маркера с $ID = N$ [8, 9].

Практическая реализация полетного задания беспилотной авиационной системы

В рамках проверки работы автономной навигации, в лабораторных условиях был выполнен автономный полет по заданным координатам с целью доставки грузов при помощи квадрокоптера на дронпоинты.

Рис. 3. Практическое решение логистической задачи доставки груза с помощью беспилотной авиационной системы

На рис. 3 представлен пример доставки груза беспилотной авиационной системой мультироторного типа на дронпоинт, ниже представлен фрагмент программного кода автономного полета с доставкой груза на дронпоинт.

Фрагмент программного кода:

```
import rospy
from clover import srv
from std_srvs.srv import Trigger
from mavros_msgs.srv import CommandBool
import math
import pigpio

rospy.init_node('flight')

get_telemetry = rospy.ServiceProxy('get_telemetry', srv.GetTelemetry)
navigate = rospy.ServiceProxy('navigate', srv.Navigate)
land = rospy.ServiceProxy('land', Trigger)
arming = rospy.ServiceProxy('mavros/cmd/arming', CommandBool)

pi = pigpio.pi()

MAIN_SERVO_PIN = 6
LEFT_SERVO_PIN = 13
RIGHT_SERVO_PIN = 19
CENTRAL_SERVO_PIN = 26

MAIN_SERVO_LEFT = 900
MAIN_SERVO_CENTRAL = 1600
MAIN_SERVO_RIGHT = 2200

HOOK_SERVO_CLOSE = 2100
HOOK_SERVO_OPEN = 800

pi.set_mode(MAIN_SERVO_PIN, pigpio.OUTPUT)
pi.set_mode(LEFT_SERVO_PIN, pigpio.OUTPUT)
pi.set_mode(RIGHT_SERVO_PIN, pigpio.OUTPUT)
pi.set_mode(CENTRAL_SERVO_PIN, pigpio.OUTPUT)

def navigate_wait(x=0, y=0, z=0, yaw=float('nan'), speed=0.5, frame_id='', auto_arm=False, tolerance=0.20):
    navigate(x=x, y=y, z=z, yaw=yaw, speed=speed, frame_id=frame_id, auto_arm=auto_arm)

    while not rospy.is_shutdown():
      telem = get_telemetry(frame_id='navigate_target')
```

```
    #print(telem.z)
    if math.sqrt(telem.x ** 2 + telem.y ** 2 + telem.z ** 2) < tolerance:
      break
    rospy.sleep(0.2)
```

На основе полученного положительного результата и успешного решения задачи доставки нескольких грузов в летном исследовательском поле лаборатории беспилотных авиационных систем получилось достигнуть следующих новых значимых результатов:

– получено новое решение аппаратного и программного комплекса для автономной доставки грузов,

– созданы алгоритмы и реализованы программы на языке Python для идентификации точек доставки и выполнения заданий по сбросу грузов,

– получены решения реализованы в полном цикле полетного задания без падений и потери груза,

– полученное решение формирования полетного задания можно масштабировать на большее количество точек доставки,

– полученное решение моделируется в среде Gazebo без ошибок, что подтверждает корректность полетных заданий,

– реализован алгоритм и программа идентификации точек доставки на основе данных от камеры (машинного зрения) позволяет реализовать вероятностные сценарии работы беспилотной авиационной системы.

Дальнейшим развитием разработки аппаратных комплексов стала разработка нового контейнера с возможностью поддержания заданной температуры.

Заключение

Для усовершенствования работы данной системы доставки в условиях городской среды возможно применение элементов искусственного интеллекта, который сможет корректно сформировать полетное задание и отслеживать состояние беспилотной системы на всем протяжении маршрута. Применение элементов искусственного элемента позволит улучшить обработку информации, поступающую с датчиков и систем машинного зрения для автономной системы избегания столкновения с статическими препятствиями и построения достаточно подробной карты местности для навигации по заданному маршруту при помощи различных датчиков на базе сонаров, лазерных дальномеров и стереокамер для построения модели местности. За счет данной системы возможно достаточно быстрое принятие решения для экстренной корректировки маршрута, хотя и требуется либо применять более простые нейронные сети из-за ограничений, связанных с вычислительной мощностью установленных бортовых систем, либо требуется крайне устойчивая и высокоскоростная беспроводная информационная сеть для передачи данных, поступающих в реальном времени в вычислительные центры, в которых происходит обработка больших данных и отправка на дрон предварительно обработанной информации, за счет которой дрон может принимать оптимальное решение для перестроения маршрута.

Библиографический список

1. Силин Ю. А. Анализ аппаратных комплексов для доставки особо важных грузов с помощью беспилотных авиационных систем // Системный анализ и логистика: журнал. № 3 (29), ISSN 2077-5687. СПб.: ГУАП, 2021. С. 9–14. DOI: 10.31799/2077-5687-2021-3-9-14.

2. Силин Ю. А. Разработка охлаждающего контейнера способного поддерживать заданную температуру при транспортировке // Системный анализ и логистика: журнал. № 2 (28), ISSN 2077-5687. СПб.: ГУАП, 2021. С. 97–103. DOI: 10.31799/2077-5687-2021-2-97-103.

3. Костин А. С. Классификация гражданских беспилотных летательных аппаратов и сферы их применения // Системный анализ и логистика. 2019. № 1 (19). С. 70–80.

4. Майоров Н. Н. Основы автономного управления беспилотными авиационными системами для решения транспортных задач / Н. Н. Майоров, Д. В. Еленин, А. С. Костин. СПб.: ГУАП, 2020. 71 с.

5. Dobrovolskaia A. Research the application of data from unmanned systems for the development of micromobility and modernization of urban infrastructure // Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) 2021. SUAI. Saint-Petersburg. 2021. 9470674. DOI: 10.1109/WECONF51603.2021.9470674.

6. Voznesenskii E. A. Automated battery charging system for multi-rotor aerial vehicles // Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) 2021. SUAI. Saint-Petersburg. 2021. 9470571. DOI: 10.1109/WECONF51603.2021.9470571.

7. Maiorov N. N. Control and analysis of quadcopter flight when setting a complex trajectory of motion / N. N. Maiorov, N. Bogatov, A. Kostin // Journal of Physics: Conference Series 1925 (2021). 012043. IOP Publishing. DOI:10.1088/1742-6596/1925/1/012043.

8. Карпова Т. Ю. Эксплуатация беспилотных авиационных систем / Т. Ю. Карпова, А. С. Костин, Н. Н. Майоров. СПб.: ГУАП, 2021. 169 с.

9. Wang Y. Adaptive time-varying formation tracking control of unmanned aerial vehicles with quantized input / Y. Wang, L. He, C. Huang // ISA Trans, 2019. Vol. 85. P. 76– 83.

УДК 656

Т. А. Менухова*
кандидат технических наук, доцент
А. В. Сумманен**
кандидат технических наук, доцент
А. А. Сивов *
кандидат технических наук, доцент
*Санкт-Петербургский горный университет
**Санкт-Петербургский государственный университет аэрокосмического приборостроения

ОПТИМИЗАЦИЯ ТРАНСПОРТНО-ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ПРИ ЭКСПЛУАТАЦИИ ЭКСКАВАТОРНО-АВТОМОБИЛЬНЫХ КОМПЛЕКСОВ

В статье предлагается вариант решения проблемы наличия простоев крупнотоннажной техники из-за разницы во времени оборота и простоя под погрузкой разнотоннажных карьерных самосвалов. При использовании разнотоннажных автомобилей-самосвалов для перевозок грузов горнодобывающей промышленности в карьерах возникают сложности при планировании ритма подачи подвижного состава под погрузку и при выполнении самой погрузки, поскольку у разнотоннажных автомобилей наблюдаются отличия как по времени оборота, так по времени простоя под погрузкой. Оцениваются альтернативные варианты организации совместной работы разнотоннажных автомобилей-самосвалов и экскаватора в зоне погрузки.
Ключевые слова: график совместной работы, экскаваторно-автомобильный комплекс, карьерный самосвал, экскаватор, перевозка грузов, погрузочно-разгрузочные работы.

T. A. Menukhova*
PhD, Tech., Associate Professor
A. V. Summanen ***
PhD, Tech., Associate Professor
A.A. Sivov*
PhD, Tech., Associate Professor
*St. Petersburg Mining University
**St. Petersburg State University of Aerospace Instrumentation

OPTIMIZATION OF TRANSPORT AND TECHNOLOGICAL PROCESSES IN THE OPERATION OF EXCAVATOR-AUTOMOBILE COMPLEXES

The article proposes a solution to the problem of the presence of downtime of large-tonnage equipment due to the difference in turnover time and downtime during loading of multi-tonnage mining dump trucks. When using multi-tonnage dump trucks for the transportation of goods in the mining industry in quarries, difficulties arise when planning the rhythm of the supply of rolling stock for loading and when loading itself, since multi-tonnage vehicles differ in both turnover time and idle time for loading. Alternative options for organizing joint work of multi-tonnage dump trucks and an excaator in the loading area are evaluated.
Keywords**:** excavator and automobile complex, mining dump truck, excavator, schedule of joint work, transportation of goods, loading and unloading operations.

Введение

При организации открытых горных работ выемка, погрузка и вывоз горной массы выполняются мощными экскаваторно-автомобильными комплексами. Грузоподъемность применяемых на таких работах автомобилей-самосвалов при этом достигает 150 т и более, на угольных разрезах в России имеется опыт эксплуатации БелАЗа-75710 грузоподъемностью 450 т. Один из способов повышения эффективности функционирования разреза – эксплуатация экскаваторно-автомобильных комплексов в оптимальных режимах. Современные решения в большей степени направлены на оперативное управление и контроль за работой техники [1 – 3], в то время как ключевым резервом для повышения эффективности работы техники является планирование с применением математического аппарата и алгоритмов, реализованных в программной среде, что и продемонстрируем на примере данного исследования [4].

Проблема

Эффективность работы экскаваторно-автомобильных комплексов зависит от простоев техники. При использовании на одном из участков автомобилей-самосвалов различной грузоподъемности возникают закономерные сложности в планировании ритмичности подачи подвижного состава под погрузку и при выполнении самой погрузки. У разнотоннажных автомобилей наблюдаются отличия, как по времени оборота, так и по времени простоя под погрузкой, что провоцирует сбои четкого ритма подачи подвижного состава под погрузку и простои техники в ожидании погрузки. Возникающие ввиду таких сбоев простои крупнотоннажной техники ведут к существенным финансовым потерям для предприятия, что делает особенно актуальной задачу организации совместной работы автомобилей-самосвалов и экскаваторов. Поставленная задача должна решаться путем составления и строгого выполнения графиков движения транспортных средств, оперативного диспетчерского руководства работой подвижного состава на линии, внедрения систем оперативной связи. При составлении графиков требуется высокая точность планирования и адекватный математический аппарат.

Альтернативные решения

Для исследования вариантов решения такой задачи были использованы данные одного из российских предприятий, осуществляющего добычу угля открытым способом, имеющего опыт эксплуатации разнотоннажных автомобилей-самосвалов. На примере частного случая, когда на одном из погрузочных пунктов работает один БелАЗ-75710 грузоподъемностью 450 т, шесть БелАЗов-75306 грузоподъемностью 240 т и экскаватор марки P&H-2800 с объемом ковша 33,2 м^3, были построены альтернативные графики подачи автомобилей под погрузку с целью повышения эффективности использования транспортной и погрузочной техники. В качестве альтернативы рассмотрена возможность прерывания погрузки БелАЗа-75710 при прибытии под погрузку

БелАЗа-75306 для сокращения временных простоев автомобилей-самосвалов и экскаваторов.

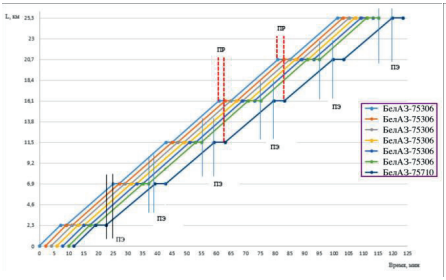
Математическая модель

Далее представлена модель оценки альтернативных вариантов совместной работы автомобилей-самосвалов и экскаватора:

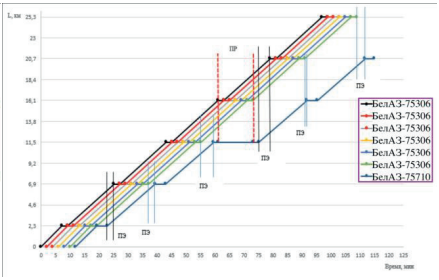
$$\frac{a_i \cdot q_i \cdot T}{t_i} = Q_i^{(j)};\ \sum_{i=1}^{n} Q = Q_i^{(j)};\ Q_i^{(j)} => max\ ;\ Q_i^{(j)} => {}^{max}_{j}Q,$$

где a – количество автомобилей, ед.; q – грузоподъемность транспортной единицы, т; T – время смены, мин.; t – время оборота, мин.; Q – объем перевезенной породы, т; i – количество марок автомобилей-самосвалов, i = 1, 2; n – количество вариантов по организации совместной работы, n = 1, …, 4. Наилучшим вариантом будет являться тот, которому соответствует максимальный объем вывезенной породы.

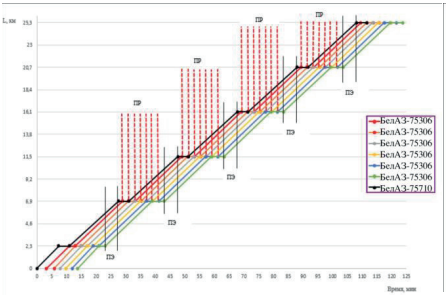
а) Базовый вариант



б) Альтернатива «А»



в) Альтернатива «В»



г) Альтернатива «С»

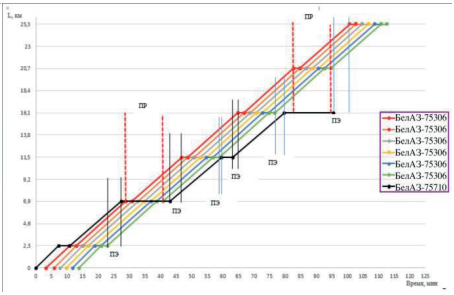


Рис. 1. Последовательность технологических операций в различных вариантах: ПР – простои БелАЗов; ПЭ – простои экскаватора

Рассмотрим организацию совместной работы автомобилей-самосвалов и экскаватора альтернативных вариантов.

Базовый вариант. Первыми загружаются БелАЗы-75306, после этого БелАЗ-75710 (рис.1, *а*).

Альтернатива «А». Первым загружаются БелАЗы-75306, после этого БелАЗ-75710. Если возникает ситуация, когда при погрузке БелАЗа-75710, подъезжает БелАЗ-75306, то экскаватор должен прервать погрузку первого и начать загружать второй, после этого возобновить погрузки при отсутствии очереди (рис.1, *б*).

Альтернатива «В». Первым загружают БелАЗ-75710, после этого БелАЗы-75306 в порядке очереди (рис.1, *в*).

Альтернатива «С». Первым загружается БелАЗ-75710, после этого БелАЗ-75306. Если возникает ситуация, когда при погрузке БелАЗа-75710, подъезжает БелАЗ-75306, то экскаватор должен прервать погрузку первого и начать загружать второй, после этого возобновить погрузки при отсутствии очереди (рис.1, *г*).

Результаты

В табл. 1 представлены сменные показатели совместной работы автомобилей-самосвалов и экскаватора для рассмотренных вариантов. Годовые показатели работы техники представлены на рис. 2.

Таблица 1

Сменные показатели совместной работы автомобилей-самосвалов и экскаватора

Наименование показателей, ед. изм.	Базовый вариант	Альтернативы		
		«А»	«В»	«С»
Простои экскаватора, мин.	143,1	117,75	145,6	129,5
Простои БелАЗов-75306, мин.	395,1	–	231,4	–
Простои БелАЗа-75710, мин.	–	123,85	–	124,1
Количество вывезенной породы БелАЗами-75306, т	45619,2	51148,8	45619,2	49766,4
Количество вывезенной породы БелАЗом-75710, т	13824	11664	13824	11232
Общее количество вывезенной породы, т	59443,2	62812,8	59443,2	60998,4

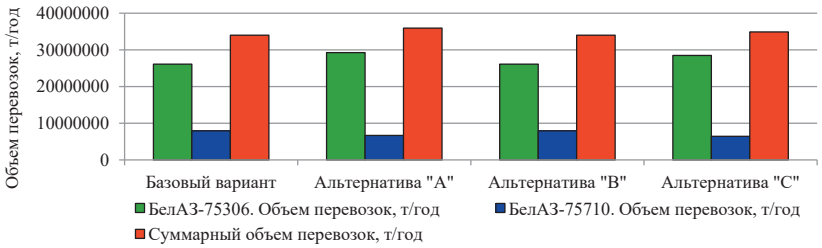


Рис. 2. Годовые показатели работы техники. Объем перевозок самосвалами

Вывод

При альтернативе «А» наименьший простой техники и больший объем вывезенной породы. Несмотря на увеличение эксплуатационных затрат происходит прирост прибыли за счет увеличения объема перевезенной породы в проектируемом варианте на 1 927 411 т/год относительно базового. Подобная оценка альтернатив может проводиться как при аналогичных условиях, когда эксплуатируются разнотоннажные автомобили-самосвалы при перевозке грузов горнодобывающей промышленности в карьерах, но также и в иных условиях при эксплуатации разнотоннажных автотранспортных средств и возникновении очередей при погрузке. Произвести расчеты по альтернативным вариантам и обработать результаты при эксплуатации данного количества автотранспортных средств представляется возможным с применением метода перебора вариантов и с использованием графоаналитического метода. Однако, при эксплуатации многократно большего количества разнотоннажного подвижного состава потребуется решение в программной среде.

Библиографический список

1. Клебанов А. Ф. Система диспетчеризации большегрузных автосамосвалов «КАРЬЕР» на разрезе "Черниговский": структура, функциональность, экономическая эффективность / Д. Я. Владимиров, JI. В. Рыбак // Горная промышленность, № 1, 2003, С. 52–56.

2. Kurganov V. M. Assessment of operational reliability of quarry excavator-dump truck complexes / V. M. Kurganov, M. V. Gryaznov, S. V. Kolobanov // Journal of Mining Institute. Vol. 241. 2020. С. 10.

3. Bol'shunova O. M. Пути повышения эффективности использования карьерного автотранспорта // Journal of Mining Institute. Vol. 157. 2004. С. 104.

4. Менухова Т. А. Повышение производительности экскаваторно-автомобильных комплексов за счет минимизации времени простоя крупнотоннажной техники / Т. А. Менухова, Ю. В. Бородина, А. А. Сивов // Инновации и перспективы развития горного машиностроения и электромеханики: IPDME-2021. Сборник тезисов VIII Международной научно-практической конференции. Санкт-Петербург. 2021. С. 435–439.

УДК 629.7.06

П. А. Назаренко*
ассистент
П. В. Попок*
студент
Д. А. Аблязов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ БАС В АРКТИЧЕСКИХ УСЛОВИЯХ

Рассмотрена актуальность использования беспилотных летательных аппаратов в арктических условиях, приведены примеры возможного использования.
Ключевые слова: беспилотный летательный аппарат, арктические условия, климатические условия, высокие широты Арктика.

P. A. Nazarenko*
Assistant
P. V. Popok*
Student
D. A. Ablyazov*
Student
*St. Petersburg State University of Aerospace Instrumentation

THE RELEVANCE OF THE USE OF UNMANNED AERIAL VEHICLES IN ARCTIC CONDITIONS

The relevance of the use of unmanned aerial vehicles in arctic conditions is considered, examples of possible use are given.
Keywords: unmanned aerial vehicle, arctic conditions, climatic conditions, high latitude, Arctic.

Введение

Беспилотные летательные аппараты особенно актуальны в использование в труднодоступных районах, где немногочисленные метеорологические и аэрологические станции располагаются на большом расстоянии друг от друга. Именно такая проблема существует сейчас в Арктике: точность прогноза погоды здесь оказывается существенно ниже, чем в средних широтах. В основном беспилотные авиационные системы (БАС) применяются для аэрофотосъемки, целей картографии, геологоразведки, осуществления разведки ледовой обстановки, и ряд других возможностей. Многие конструкторские бюро и предприятия занимаются проектированием и разработкой аппаратов пригодных для суровых арктических условий.

Интерес к исследованию арктической среды в последнее время возрос не только в арктических странах, но также в международных организациях и странах, которые не имеют территорий на полярном круге во внутренних

границах. Зачастую возникают разногласия из-за этих интересов. И для поиска компромиссов решаются вопросы следующего характера: теоретического, геополитического, экономического, а также технические, требующие использования современных технологий.

Применение БАС в арктических условиях

Арктика – это район Земли, примыкающий к Северному полюсу. Климатические условия этого региона являются одними из самых суровых на планете, и считаются неблагоприятными для исследований. Тем не менее к этому необычному краю ученые проявляют большой профессиональный интерес, так как изучение арктических особенностей поможет решить глобальные экономические, стратегические, а также экологические проблемы общества. Применение БАС в арктических условиях, а именно на высоких широтах характеризуется комплексом сложностей технической направленности, в основе которых можно увидеть проблемы, связанные с непростыми метеоусловиями, отсутствием наземной летной инфраструктуры, влиянием внешних помех на некоторые типы радионавигационного обеспечения, сложности могут возникнуть в процессе выполнения продолжительных полетов по времени.

Долгое время беспилотные летательные аппараты считались неподходящими для изучения Арктической местности из-за сложных климатических условий. С приходом современных технологий возможность использования БАС является одним из самых важных и необходимых инструментов для исследования Арктики. Продолжительность полета и сроки эксплуатации во многом зависят от силовых установок беспилотных аппаратов. В каждом виде элементов питания БАС есть свои как положительные, так и отрицательные стороны [1].

Существует два типа источников питания БЛА. Первый вариант – бензиновый двигатель, второй вариант – БАС с мощным аккумулятором. У каждого типа питания деталей летательных аппаратов есть свои сильные и слабые стороны. Бензиновый двигатель обеспечивает дальность полета, поэтому энергия, выделяемая при сгорании топлива, в несколько раз выше, чем у современных аккумуляторов. Но при этом применение двигателя имеет и ряд недостатков. Например, сложная конструкция, а также большое количество времени затрачивается на подготовку перед вылетом. К тому же, работа на бензиновом двигателе наносит вред экологии, так как при сгорании топливо выбрасывает в атмосферу углекислый газ, что приводит к загрязнению окружающей среды, а также – это уровень надежности, длительное время монтажа в начале сложной конструкции. Кроме того, БАС с бензиновым двигателем требует значительных затрат на транспортировку до места разработки и высокого уровня специалистов, работающих с этой техникой

Однако аккумуляторы не требуют высококвалифицированного технического персонала. Современные аккумуляторы могут питать БАС более 3 часов. Техническое обслуживание электрооборудования является коротким и простым. Единственным недостатком аккумуляторных батарей является воздей-

ствие окружающего климата Арктики на саму батарею, на ее работоспособность и срок службы, при которых снижается мощность аккумуляторной батареи, и тем самым это может привести к нарушению надежности работы беспилотника [2].

Рис. 1. Беспилотный летательный аппарат вертолетного типа

Немаловажным фактом является также географическое и стратегическое положение Арктической зоны. Экономика, наука и обороноспособность Российской Федерации тесно связаны с рассматриваемым регионом. Решение возникающих в данных сферах задач затруднительно без актуальных и обладающих информационной полнотой топографических карт. Преобладающим методом картографирования в современном мире является дистанционное зондирование земли со спутниковых космических аппаратов, однако получение топографических карт, необходимых для специфических задач требуемого масштаба за счет спутниковых данных на сегодняшний день невозможно. Кроме того, предварительную разведку местности на предмет полезных ископаемых предпочтительно проводить при помощи сканирующих устройств, устанавливаемых на летательные аппараты.

Решение огромного количества проблем в условиях Арктического холода оказывается доступным с помощью беспилотных летательный аппаратов:

- распознавание ледовой обстановки, мониторинг морского волнения, поиск косяков рыб;
- поиск и обнаружение морских судов;
- морской пограничный контроль;
- охрана важных объектов (километры трубопроводов топливно-

энергетических компаний);

– картография;

– контроль за гидрометеорологическими условиями и активными излучающими объектами;

– аэрофотосъемка;

– проверка соблюдения договорных обязательств (режим «открытого неба»)

– обнаружение малоразмерных воздушных и наземных объектов.

– тушение не только лесных пожаров, но и различных объектов могут быть использованы при исследовании арктических территорий.

Летательные аппараты средней дальности полета являются наиболее востребованными. Техника данного класса с вертикальным взлетом и посадкой в этом непростом крае незаменимы – беспилотникам вертолетного типа не нужна специальная полоса, у них большая маневренность и они могут зависать над объектом, что является несомненным достоинством в условиях арктического климата.

От уровня развития измерительной техники, зависит качество выполнения задач с помощью БАС. Выполнение задач в экстремальных условиях сильно зависит от совершенства бортового оборудования, в частности, от качества информационно-измерительных сигналов, которые используются в управлении. Источником данных сигналов о параметрах движения, таких как ориентация, местоположение, скорость, бортовая температура и другие, являются различные навигационные комплексы и измерительные системы [3].

При использовании БАС в условиях арктического холода наблюдаются ряд особенностей:

– Высокие значения магнитного склонения и его быстрые изменения на коротких расстояниях могут вызывать магнитные аномалии и бури. На Северном полюсе магнитное склонение очень велико из-за близости полюсов и наличия солнечной активности. Нестабильности показаний магнитного поля и гирокомпаса связаны с малыми значениями горизонтальной составляющей магнитного поля Земли.

– Из-за особенностей географического положения угол схождения меридиана становится большим, а долгота быстро меняется во время полета самолета. Из-за большого угла схождения меридиана лететь по маршруту с использованием магнитного компаса затруднительно. При полете с магнитным компасом линии фактического пути имеют большую кривизну, что значительно удлиняет путь с одной стороны и ослабляет качество работы навигационного оборудование с другой.

– Радиоволны, особенно коротковолновая нестабильность, и помехи от беспроводных устройств. Во время геомагнитной бури распространение радиоволн становится нестабильным, сокращается радиосвязь, ограничивается использование радиосредств (РТС). Помехи RTS возникают во время полета в среде, полной льда и снежного мусора. Он образуется в результате частичного разряда между противоположно заряженными частицами.

– Рельеф однообразен, и мало точек для радиолокационного или визуального наведения. Небольшое количество наземных навигационных средств беспроводной технологией. Нет радиолокационного контроля в высоких ши ротах, на море и в труднодоступных районах.

Благодаря высокому уровню развития измерительной техники решение поставленных задач становится реальным. Способы эксплуатации БАС напрямую связаны с оборудования, установленного на дроне. Очень важно чтобы информация доходила без искажений и управление беспилотного летательного аппарата было максимально точным и комфортным.

Решение вышеописанных вопросов требует модернизации существующих беспилотных летательных аппаратов для облегчения исследования земель Арктики. Заинтересованность в использовании БАС в исследованиях порождает конкретные задачи и требования, решая которые, исследования получаются максимально точными соответствуют параметрам изучения [4].

Заключение

В качестве ключевых задач, которые возможно решить при использовании БАС в арктических условиях можно выделить: поиск и обнаружения малоразмерных, средне размерных воздушных и наземных объектов, целей картографии, а также морского и речного транспорта, разведки ледовой обстановки, осуществление контроля за морскими границами, контроля за пожароопасной обстановкой в труднодоступных территориях.

Мониторинг труднодоступных участков, на высоких широтах, открывает новые возможности в изучении окружающей среды, позволяет получить качественную информацию о происходящих геоэкологических процессах и явлениях, что особенно важно во время глобального потепления.

Библиографический список

1. SCILEAD. URL: https://scilead.ru/article/341-primenenie-bespilotnoj-aviatsii-v-issledovaniy (дата обращения: 30.03.2022).

2. ELIBRARY. URL: https://elibrary.ru/item.asp?id=46392721 (дата обращения: 31.03.2022).

3. ELIBRARY. URL: https://www.elibrary.ru/item.asp?id=28910119 (дата обращения: 30.03.2022).

4. MAGAZINE. URL: https://magazine.neftegaz.ru/articles/tsifrovizatsiya/473748-bpla-v-usloviyakh-arkticheskogo-regiona/ (дата обращения: 31.03.2022).

УДК 629.7.06

П. А. Назаренко*
ассистент
П. В. Попок*
студент
Д. А. Аблязов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ИССЛЕДОВАНИЕ РАБОТЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ЭКВАТОРИАЛЬНОЙ ЗОНЕ

Проанализирована работа беспилотных летательных аппаратов в условиях повышенных температур. Сформулированы основные способы возможного решения проблемы перегрева источников питания. Определены актуальные варианты практического решения данной проблемы
Ключевые слова: беспилотный летательный аппарат, высокая температура, аккумулятор, охлаждение.

P. A. Nazarenko*
Assistant
P. V. Popok*
Student
D. A. Ablyazov*
Student
*St. Petersburg State University of Aerospace Instrumentation

INVESTIGATION OF THE OPERATION OF UNMANNED AERIAL VEHICLES IN CONDITIONS OF EXTREME TEMPERATURES

The work of unmanned aerial vehicles in conditions of high temperatures is analyzed. The main ways of a possible solution to the problem of overheating of power supplies are formulated. Actual options for a practical solution to this problem are identified
Keywords: unmanned aerial vehicle, high temperature, battery, refrigeration.

Введение

Все беспилотные летательные аппараты исторически имели исключительно военное применение. Но представление об этих машинах кардинально поменялось с развитием гражданской техники. Многие конструкторские бюро и предприятия занимались проектированием и разработкой подобных аппаратов. Теперь это уже не просто военные машины, а обыденная часть нашей современной жизни.

Квадрокоптер – беспилотная авиационная система (БАС), оснащенная четырьмя электродвигателями с воздушными винтами, вращающимися диагонально в противоположных направлениях. Наиболее распространенный беспи-

лотник, успевший зарекомендовать себя в различных областях гражданской сферы. Их рассматривают как полезное оборудование, которое значительно облегчает деятельность человека. Квадрокоптеры ценятся за их компактность, способность двигаться в трех плоскостях и “виснуть” над объектом, что позволяет применять их для различных задач (мониторинг и контроль объектов, разведка, сбор фото- и видеоинформации и т. д.).

Однако, при всех своих плюсах квадрокоптеры ограничены в работе условиями среды – это высокие и низкие температуры, песок, грязь, влажность. Находясь под прямыми лучами солнца квадрокоптер может перегреться, что очень опасно для аккумулятора, ведь есть вероятность его воспламенения.

Цель данной работы – проектирование и разработка устройств для эксплуатации беспилотных авиационных систем в экстремально высоких температурах.

Технология защиты аккумуляторных батарей

Функция литий-полимерного аккумулятора – преобразование энергии, образованной в ходе химической реакции, в электрическую. При эксплуатации АКБ скорость химической реакции может сильно возрастать и протекать более бурно. Это связано с тем, что при изменении температуры меняется вязкость электролита. При повышении температуры вязкость уменьшается, что в свою очередь приводит к уменьшению внутреннего сопротивления АКБ

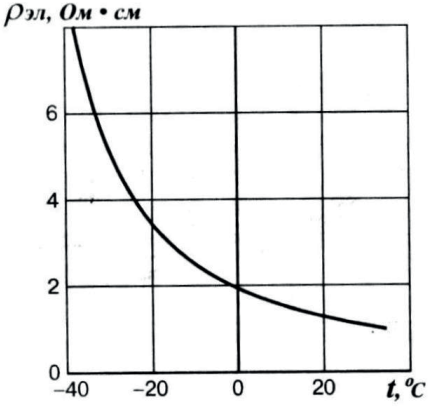


Рис. 1. Зависимость удельного сопротивления электролита АКБ от температуры

Из графика следует, что с повышением температуры внутреннее сопротивление АКБ уменьшается, а по закону Ома меньшее сопротивление означает больший ток, который дополнительно разогревает батарею за счет большей мощности цепи [1].

При заряде в АКБ накапливается тепло, выделяемое в процессе химической реакции. При разряде большими токами литий-полимерная батарея нагре-

вается за счет того самого накопившегося тепла. Нагрев выше 60°С ведет к необратимой химической реакции. Вся запасенная энергия преобразуется в тепло, что в свою очередь приводит к вздутию батареи за счет образовавшегося избыточного давления внутри оболочки, затем к резкому высвобождению этого тепла из-за разгерметизации корпуса, и, в конечном итоге, может закончиться возгоранием.

Литий-полимерный аккумулятор ни в коем случае нельзя перезаряжать. Перезаряд может произойти, когда вы пытаетесь зарядить аккумулятор быстрее, чем он способен принять этот заряд. В этом случае происходит та же ситуация: химическая реакция, генерация тепла, газ, набухание пакетов и взрыв. Граничными условиями для эксплуатации LiPo батарей считаются напряжения 2,7 В по нижней границе и 4,2 В по верхней.

В некоторые модели аккумуляторов встраивают защитную схему, предотвращающую аккумулятор от перезаряда, перегрева и токовых перегрузок. При достижении ячейками определенного уровня заряда схема отключает АКБ от зарядного устройства [2].

Технология защиты электронных компонентов

Надежность работы электронного оборудования напрямую зависит от условий эксплуатации – речь идет о влиянии окружающей среды. Агрессивные факторы могут привести к выходу из строя как отдельных компонентов системы, так и ЛА в целом. Например:

1. Загрязнение. Частицы пыли или песка электризуясь притягиваются к поверхности электронного оборудования и скапливаются на ней, что может вызвать, перегрев из-за отсутствия циркуляции воздуха или же, в купе с влажностью, короткое замыкание токопроводящих элементов.

2. Влажность. Влага способствует разрушению материала, вызывает деформацию или окисление.

3. Температура. Температурное воздействие увеличивает вероятность отказа работы оборудования в связи со спецификой их режима работы.

4. Пыль и песок, оседая на печатные платы, собирают и накапливают у поверхности оборудования вредные элементы, газы, влияющие на состояние соединений контактов. К тому же, частицы пыли имеют свой собственный заряд. При попадании и накоплении пыли увеличивается и общий заряд, что вредно для токопроводящих дорожек на печатных платах.

Для защиты от вредного воздействия используют лаковые покрытия. Требуется не допустить соприкасания поверхности микросхем и загрязнений. Для этой задачи подойдут эпоксидные или силиконовые лаки. У этих видов высокая термоустойчивость, отличные диэлектрические показатели и влагозащита [3].

Конструктивное решение для защиты от высоких температур

Лучшее решение для предотвращения от перегрева – разработка системы охлаждения для литий-полимерного АКБ. Система охлаждения будет состоять

из двух кулеров (рис. 2) для отвода тепла из корпуса для АКБ (рисунок 24). Основная задача – поддерживать оптимальную температуру внутри кейса и не дать АКБ нагреваться выше 60°С.

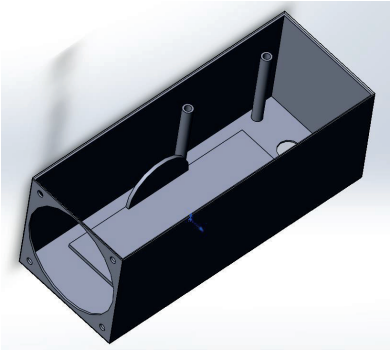


Рис. 2. Корпус для АКБ

В качестве материала для корпуса подойдет углепластик – прочный и жесткий, выдерживает высокие температуры, достаточно легкий, так как любой лишний вес сказывается на маневренности, скорости и управляемости квадрокоптера.

Кейс также нужен для того, чтобы предотвратить аккумулятор от повреждений, в случае падения. Снаружи кейс необходимо покрыть теплоизолирующим материалом.

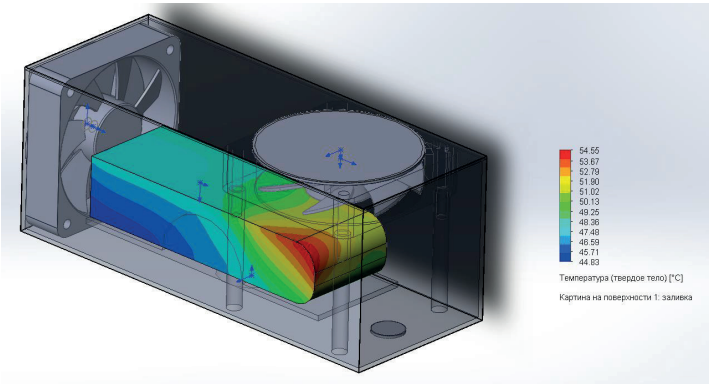


Рис. 3. Распределение температуры по поверхности АКБ

Верхнюю грань корпуса необходимо сделать съемной для более удобного монтажа АКБ и кулеров. На нижней грани присутствует отверстие для вывода

силовых кабелей. Внутри корпуса – держатель для АКБ, а также четыре стойки для крепежа одного из кулеров. Второй кулер крепится к боковой грани.

Моделирование проводилось на базе аккумулятора от учебного квадрокоптера «Клевер 4». Результаты моделирования приведены на рис. 3, 4.

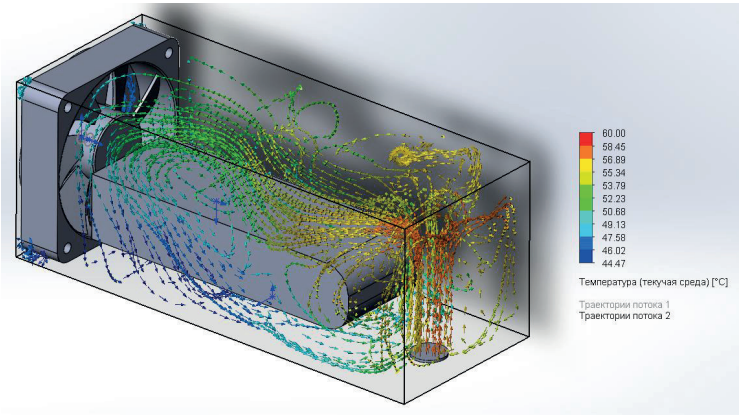


Рис. 4. Температура воздуха внутри корпуса АКБ

Заключение

Для решения задачи необходимо было провести анализ предметной области, связанной с беспилотными системами.

Проведен анализ его функциональной схемы, работы оборудования и составных элементов при повышенных температурах. Выяснилось, что самым слабым местом во всей системе является литий-полимерная АКБ, так как очень сильно подвержена влиянию высоких температур.

Также были рассмотрены возможные причины поломок АКБ – это короткое замыкание, повреждения, влияние окружающей среды, большие разрядные токи. Разработана защита от пыли и песка, попадающих на электронные компоненты системы, в виде покрытия их лаком.

В системе автоматизированного проектирования *SolidWorks* проведено моделирование системы охлаждения для литий-полимерной аккумуляторной батареи. Разработан специальный корпус, защищающий аккумулятор от повреждений.

Библиографический список

1. Orbyta. URL: https://orbyta.ru/sovet/sovet05.html (дата обращения: 03.04.2022).

2. Infoconnector. URL: https://www.infoconnector.ru/litij-polimernye-akkumulyatory-teoriya (дата обращения: 03.04.2022).

3. Fantozer. URL: http://fantozer.forumbb.ru/viewtopic.php?id=1007 (дата обращения: 03.04.2022).

УДК 629.7.06

П. А. Назаренко*
ассистент
К. А. Семенюк*
студент
Г. Ю. Анисимов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

АНАЛИЗ РАБОТЫ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ЭКСТРЕМАЛЬНО ВЫСОКИХ ТЕМПЕРАТУР И ВНЕШНИХ ЗАГРЯЗНЕНИЙ

На сегодняшний день квадрокоптеры применяются во многих отраслях. Однако эксплуатация данного летательного аппарата сильно ограничена температурой окружающей среды. Именно поэтому актуальной ставится задача создания устройств для эксплуатации беспилотных авиационных систем в экстремальных условиях при высоких температурах, которая сможет выдерживать данные погодные условия. Неблагоприятные внешние факторы существенно снижают качество выполнения полетного задания, поэтому принципиально важной задачей является повышение надежности беспилотного летательного аппарата.
Ключевые слова: беспилотная авиационная система, аккумулятор, высокие температуры.

P. A. Nazarenko*
Assistant
K. A. Semenuyk*
Student
G. U. Anisimov*
Student
*St. Petersburg State University of Aerospace Instrumentation

ANALYSIS OF THE OPERATION OF UNMANNED AERIAL SYSTEMS IN EXTREMELY HIGH TEMPERATURES AND EXTERNAL POLLUTION

Today, quadrocopters are used in many industries. However, the operation of this aircraft is severely limited by the ambient temperature. That is why the urgent task is to create devices for the operation of unmanned aircraft systems in extreme conditions at high temperatures, which will be able to withstand these weather conditions Unfavorable external factors significantly reduce the quality of the flight task, therefore, a fundamentally important task is to increase the reliability of an unmanned aerial vehicle.
Keywords**:** unmanned aircraft system, battery, high temperatures.

Введение

Беспилотные авиационные системы (БАС) – бурно развивающаяся область в авиации. Решение круга задач с помощью БАС объясняется их преимуществом перед пилотируемыми: низкая стоимость производства и эксплуата-

ции, и при этом эффективность выполнения поставленных задач не теряется. Беспилотники могут работать там, где есть вероятность вредного или опасного влияния на человека.

В целом, рынок гражданских БАС очень разнообразен. У производителя нет стандартов и ограничений: каждая модель разрабатывается под конкретный вид деятельности. Такая узкая специализация дает некоторую свободу в выборе функционала для создаваемых БАС, поэтому одни аппараты получаются более развитыми в технологическом плане по отношению к другим.

Одним из самых популярных представителей БАС считается квадрокоптер, так как он имеет оптимальные характеристики для использования в различных сферах, например, сельское хозяйство (контроль территории, обозначение маршрута и т. д.). Квадрокоптер уникален тем, что способен двигаться в трех плоскостях. Но несмотря на то, что он многофункционален и пользуется большим интересом на рынке у него есть проблемы, которые, к сожалению, ограничивают его применение. В основном эти проблемы заключаются во внешних факторах, которые способны нарушить комфортную эксплуатацию аппарата.

Например, использование квадрокоптера в пустыне, в этих условиях обнаруживается сразу две проблемы: высокая температура и песок. При высокой температуре аккумулятор квадрокоптера может перегреться, что в свою очередь негативно скажется на работе техники. Попадание песчинок в узлы управления квадрокоптера также нарушат его технические возможности (заклинит двигатель, перегрев двигателей).

Беспилотные авиационные системы

Беспилотная авиационная система – совокупность элементов, связывающих беспилотное воздушное судно, наземный пункт обслуживания и управления и каналы передачи данных между ними. Само по себе беспилотное воздушное судно функционировать не способно, поэтому полет и управление происходят по определенным полетным планам, алгоритмам, записанных в программное обеспечение беспилотника [1].

Создание БАС обусловлено решением некоторых задач: инженерных, научных и т. д. Современные беспилотные системы являются выдающимся достижением в авиации за последнее десятилетие. Разработанные перспективные технологии обеспечивают не только быстрые темпы роста рынка беспилотников, но и создают новые рынки и отрасли, способствуют повышению эффективности национальных экономик.

Особое внимание заслуживают технологии микроэлектромеханические системы (МЭМС) – их внедрение в БАС позволило беспилотникам выйти на новый уровень и значительно улучшить их возможности. Сейчас датчики положения, датчики давления стали в разы точнее, а размеры достигают крайне малых значений в несколько миллиметров, благодаря чему можно уменьшить масса-габаритные показатели и самих беспилотников. Сюда так же следует добавить о развитии микропроцессоров с мощной вычислительной способностью,

новых источников питания, позволяющих обеспечивать Беспилотное воздушное судно (БВС) энергией до нескольких часов непрерывной работы, и систем глобального позиционирования.

Специализация БАС определяется целевой нагрузкой БВС. В гражданской сфере большим спросом пользуются информационные, т. е. те, у которых полезная нагрузка (ПН) решает задачи поиска, идентификации, наблюдения, обмен данными с наземными средствами и т. д. Например, обследование экологической обстановки Земли. БАС, используя систему сбора и передачи информации, регистрирует данные окружающей среды в самых труднодоступных местах. Беспилотники способны работать непрерывно в любых погодных условиях, а также предоставлять информацию о состоянии своих бортовых систем. Человек-оператор не участвует лично, а значит, нет риска для жизни [2].

Отсутствие человека на борту летательного аппарата (ЛА) дает огромный плюс в проектировании конструкции. Это значит, что можно убрать системы жизнеобеспечения, что даст возможность сделать конструкцию ЛА много компактнее, а также даст больше пространства для ПН и оборудования. Снимаются так же ограничения по перегрузкам при выполнении маневров, требования надежности к конструкции в целом. Облегчается их транспортировка и хранение.

Решение для безопасной эксплуатации квадрокоптера в экстремальных условиях при высоких температурах

Для питания БАС используются литий-полимерные аккумуляторы. Такое решение позволяет уменьшить вес и объем батарей благодаря высокой удельной плотности заряда по сравнению с аккумуляторами других типов. Суть работы литий-полимерного аккумулятора заключается в преобразовании энергии, полученной в ходе химической реакции, в электрическую.

Нагрев аккумулятора может произойти в разных случаях, например, при подзарядке батареи, перегрузке по току, высокой температуре окружающей среды, длительном использовании. При достижении литий-полимерным аккумулятором критической температуры происходит необратимая химическая реакция, что приводит в лучшем случае к вздутию аккумулятора, а в худшем к его возгоранию [3].

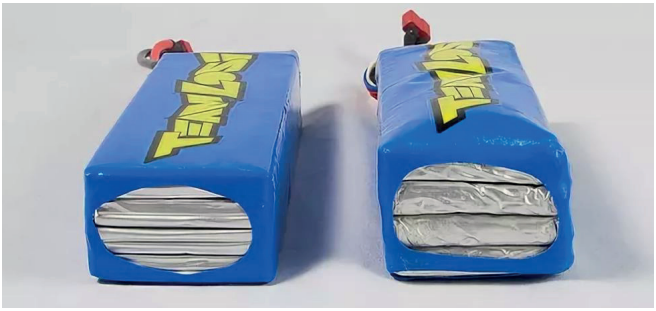


Рис. 1. Нормальный (слева) и вздутый (справа) аккумуляторы

Следует отметить, что в некоторых моделях аккумуляторов для избежание таких происшествий используют термозамыкатели.

Механическое повреждение также может сказаться на работе аккумулятора. Жесткие посадки или случайные удары от поверхности могут повредить оболочку аккумулятора, из-за чего контакты, исходящие из аккумулятора, могут оторваться и достать другие, что вызовет короткое замыкание. Прокол оболочки аккумулятора может вызвать воспламенение из-за реакции с воздухом, и большая часть энергии вырвется наружу в виде теплоты.

Двигатели квадрокоптера вынесены наружу относительно корпуса, поэтому подвергаются агрессивным климатическим условиям. При работе двигателей пыль и песок могут вздымаются потоками воздуха от воздушных винтов и оседают на магнитах или обмотках катушек. Попадание пыли в двигатель может пагубно сказаться на его работе. Слой пыли на обмотках катушки вызывает их перегрев, из-за чего обмотка может сгореть, вследствие чего двигатель выходит из строя. Дополнительный нагрев может вызвать и то, что забиваются вентиляционные каналы могут и перекрывают поступающий воздух для охлаждения двигателей.

Решением защиты аккумулятора от перегрева может стать пластмассовый короб с вентиляцией, в качестве охлаждения. Также короб будет защищать аккумулятор от механических воздействий и минимизировать попадание пыли и песка, что в свою очередь продлит службу аккумулятора.

Помимо очевидных защитных плюсов есть еще и финансовые. Себестоимость короба не сильно повлияет на цену квадрокоптера, потому что короб не имеет дорогих составляющих и не сложен в изготовлении, что также является большим плюсом.

Заключение

Слабым местом квадрокоптера является слабая защита от перегрева литий-полимерной АКБ. Пыль, песок, прямые лучи солнца, неправильный режим зарядки, длительное использовании все эти факторы тем или иным образом повышают температуру АКБ.

Проблему можно решить созданием пластмассового короба, которые будет способен охлаждать аккумулятор до приемлемых температур. Короб также будет служить защитой от механических повреждений аккумулятора.

Библиографический список

1. Беспилотные авиационные системы (БАС). URL: Cir. 328-AN/190/ ICAO. Монреаль: ICAO, 2011 (дата обращения: 25.03.2022).

2. Шилов К. Е. Разработка системы автоматического управления беспилотным летательным аппаратом мультироторного типа // Труды МФТИ. 2014. Т. 6. № 4. С. 142–143 (дата обращения: 25.03.2022).

3. Кибернетика. URL: https://cyberleninka.ru/article/n/otsenka-i-vybor-istochnikov-pitaniya-bespilotnyh-letatelnyh-apparatov/viewer (дата обращения: 27.03.2022).

УДК 629.7.06

П. А. Назаренко*
ассистент
К. А. Семенюк*
студент
Г. Ю. Анисимов*
студент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МОДУЛЬ ЗАЩИТЫ АККУМУЛЯТОРНОЙ БАТАРЕИ ДЛЯ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ ПРИ ОТРИЦАТЕЛЬНЫХ ТЕМПЕРАТУРАХ

Неблагоприятные внешние факторы существенно снижают качество выполнения полетного задания, поэтому принципиально важной задачей является повышение надежности беспилотной авиационной системы путем улучшения работоспособности его структурных элементов.
Ключевые слова: беспилотная авиационная система, мультикоптер, аккумулятор, низкие температуры.

P. A. Nazarenko*
Assistant
K. A. Semenuyk*
Student
G. U. Anisimov*
Student
*St. Petersburg State University of Aerospace Instrumentation

BATTERY PROTECTION MODULE FOR UNMANNED AIRCRAFT SYSTEMS AT LOW TEMPERATURES

Harmful external factors significantly reduce the quality of the flight mission, so an important task is to improve the reliability of an unmanned aerial vehicle by improving the performance of its structural elements.
***Keywords*:** unmanned aerial system, multicopter, battery, low temperature.

Введение

Беспилотные авиационные системы (БАС) – стремительно развивающаяся область промышленности, которая решает как гражданские, так и военные задачи. БАС получили широкое распространение во многих сферах деятельности человека. Наиболее примитивные и часто используемые – квадрокоптеры, которые представляют собой крестообразную конструкцию, имеющую четыре винта, вращающихся в противоположные стороны попарно. Данные беспилотники имеют ряд преимуществ: простота конструкции, малый вес в соотношении с перемещаемым грузом, маневренность и компактность.

Несмотря на то, что изготовители беспилотных авиационных систем ставят конкретный режим температур применения собственных приборов, пилотам время от времени нужно применять собственные дроны при отрицательных температурах воздуха. В данной работе рассматриваются основные проблемы эксплуатации БАС при низких температурах (от 0°С до –30°С), а также предлагаются решения модернизации беспилотников и анализ их работы.

Силовая установка БАС

Существует два типа источников питания беспилотной авиационной системы (БАС). Один вариант – бензиновым двигателем, а другой – мощным аккумулятором. У каждого типа питания деталей летательных аппаратов есть свои сильные и слабые стороны. Бензиновые двигатели обеспечивают дальность полета, поэтому энергия, выделяемая при сгорании топлива, примерно в 10 раз выше, чем у современных аккумуляторов, но такие технические устройства имеют множество недостатков: уровень надежности, огромное время монтажа в начале сложной конструкции. Кроме того, БАС с бензиновым двигателем требует значительных затрат на транспортировку до места разработки и множество высококлассных специалистов, работающих с этой техникой [1].

Однако аккумуляторы не требуют высококвалифицированного технического персонала.

Современные аккумуляторы могут питать БАС более 3 часов. Техническое обслуживание электрооборудования является коротким и простым.

Единственным недостатком аккумуляторных батарей является воздействие окружающей среды на саму батарею и физический процесс, который там происходит.

Вывод, который можно сделать из вышеизложенного: батарея является наиболее уязвимой частью беспилотной авиационной системы. Этот факт требует дальнейшего исследования [2].

Следующие факторы оказывают существенное влияние на производительность и срок службы батареи:

- Температура снаружи дрона.
- Состояние разрядки батареи.
- Состояние зарядки солнечных батарей.

Низкие температуры оказывают значительное влияние на работу дронов. Это влияет на производительность и срок службы батареи. Он имеет два температурных диапазона: жаркое лето и холодную зиму.

При температуре от 0°С до минус 10°С ухудшается процесс зарядки и разрядки АКБ. Но при работе потери энергии отсутствуют.

При температуре от минус 10°С до минус 20°С электропроводность уменьшается, откуда возникают нарушения в процессе зарядки.

При температуре ниже минус 20°С аккумулятор перестает функционировать и подавать на устройство необходимый ток, разрядное напряжение на контактах аккумулятора падает, что делает невозможным использование дрона.

Из ситуации, описанной выше, можно сделать вывод, что работоспособность батареи и БПЛА ухудшилась. Основной причиной такого изменения продуктивности является низкая температура. Основным элементом любого аккумулятора является электролит. Ток, протекающий по всей цепи, можно описать законом Ома. Где знаменатель этой формулы – сопротивление цепи. В результате вязкость электролита увеличивается с понижением температуры окружающей среды. Это, в свою очередь, увеличивает внутреннее со противление батареи, тем самым, общее сопротивление всей цепи БАС также увеличивается. Увеличение общего сопротивления цепи уменьшит ток в цепи. Это негативно сказалось на работе аккумулятора. Этого недостаточно для нормального функционирования БАС.

Для решения проблемы с быстрым разрядом АКБ беспилотника стоит все рассчитать, чтобы коэффициент полезного действия (КПД) был максимальным. В данном случае расстраивается КПД – продолжительность полета как при температуре, рекомендуемой к запуску БАС, так и при температурных режимах ниже 0°. Решений много: термокейс, нагревательные пленки, гибкие платы, но так как требуется максимальная легкая конструкция в плане веса, то возник интерес к гибким платам [3].

Также производителю или пользователю, непосредственно самого БАС, важно, чтобы устройство было максимально дешевым и не требовало серьезных изменений в конструкции корпуса.

Гибкая печатная плата – печатная плата, основа которой (диэлектрик) сделана из гибкого материала и может свободно изменять свою форму, что позволяет осуществлять монтаж в труднодоступных местах. Также гибкие платы позволяют минимизировать вес и объем конструкции, что и требуется в разработке мультикоптера.

Самый легкодоступный вариант разработки – термокейс, который сможет не только сохранять тепло, но и прогреваться при низких температурах, при этом контролируя подачу тепла так, чтобы не перегревать АКБ.

Конструкция кейса представляет собой проволоку определенного сопротивления, намотанную на экзоскелет. Экзоскелет вставляется в корпус, который сохраняет тепло – кейс. Разработка кейса и экзоскелета выполняется в программе *AutoCAD*.

Рис. 1. Медная нить

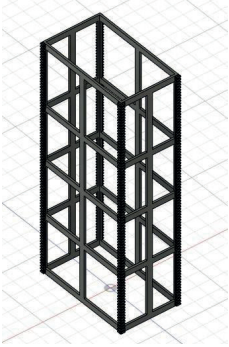


Рис. 2. Экзоскелет термокейса

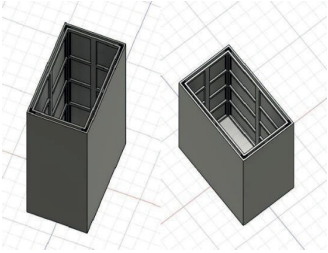


Рис. 3. Термокейс

Данная разработка не универсальна и разработана на основе квадрокоптера SYMA X8HG. В качестве тестов и создания конструкции использован АКБ от квадрокоптера SYMA X8HG.

Рис. 4. Квадрокоптер SYMA X8HG

Рис. 5. АКБ квадрокоптера

Данная сборка нуждается в питании и программном обеспечении, которое будет контролировать нагревание и температуру внутри корпуса.

Конструкция представляет из себя обогревательный элемент в виде катушки, которая питается от основного АКБ (блока питания), транзистора, регулирующего подачу тока с определенной периодичностью, термистора, измеряющего температуру в кейсе и передающего данные на контроллер *Arduino* UNO, питаемый от батарейки «Крона 9V». Программа, загруженная на контроллер, автоматически регулирует температуру внутри корпуса 20°С в зависимости от температуры окружающей среды.

Выбор *Arduino* UNO обоснован тем, что данный контроллер способен исполнять задачу максимально точно и быстро при любом изменении кода. Простейшая плата создана для изучения начальных принципов программирования

и создания проектов, которые дают развитие как таланту начинающего, так и техническому прогрессу в различных сферах наук.

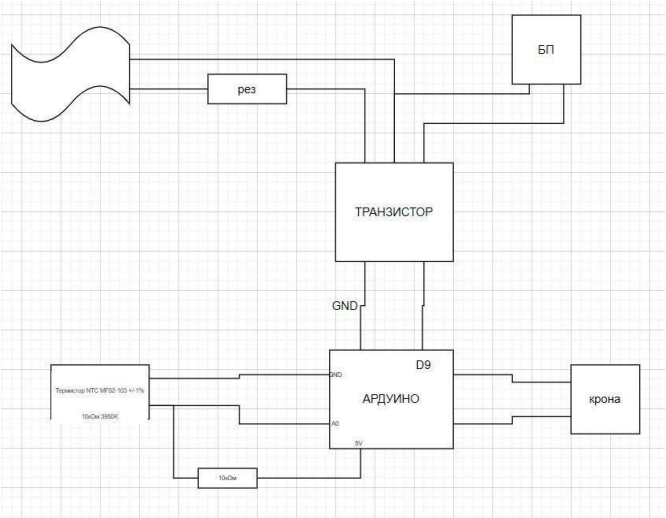


Рис. 6. Схема питания термокейса

Arduino UNO питается от USB или от внешнего источника питания, который выбирается автоматически. Внешнее питание подается через преобразователь напряжения AC/DC или АКБ. Работа контроллера возможна от внешнего питания 6–20 Вольт. При напряжении питания меньше 7 Вольт, на вывод соответственно поступает напряжение ниже 5 Вольт, что вызывает перебои в работе контроллера. Использование напряжения выше 12 Вольт перегревает регулятор напряжения, что способно повредить плату. Рекомендуемым диапазоном является напряжение 7–12 Вольт.

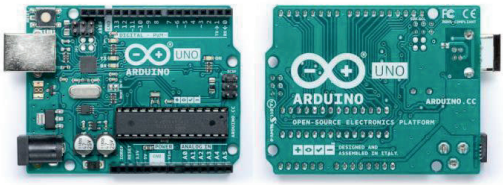


Рис. 7. Контроллер Arduino UNO

Физические характеристики

Габариты печатной платы UNO 6.9 и 5.3 см. Разъем USB и силовой разъем выходят за границы данных размеров. Четыре отверстия в плате позволяют

закрепить ее на поверхности. Расстояние между цифровыми выводами 7 и 8 равняется 0,4 см, хотя между другими выводами оно составляет 0,25 см [4].

Заключение

У беспилотных авиационных систем при температуре ниже минус 20°С аккумулятор перестает функционировать и подавать на устройство необходимый ток, разрядное напряжение на контактах аккумулятора падает, что делает невозможным использование дрона. Термокейс с контроллером *Arduino* UNO сможет не только сохранять тепло, но и прогреваться при низких температурах, при этом контролируя подачу тепла так, чтобы не перегревать аккумуляторную батарею. При наличии питания и программного обеспечения, сборка будет контролировать нагревание и температуру внутри корпуса, тем самым обеспечивая безопасный полет беспилотной авиационной системы при температурах до минус 50℃.

Библиографический список

1. GEOSCAN. URL: https://docs.geoscan.aero/ru/master/database/const-module/classification/classification.html (дата обращения: 02.03.2022).

2. ДроноМания. URL: https://dronomania.ru/faq/vsyo-o-lipo-batareyah-dlya-fpv-dronov.html (дата обращения: 27.02.2022).

3. ELIBRARY. URL: https://www.elibrary.ru/item.asp?id=28910119 (дата обращения: 27.02.2022).

4. Вольтик. URL: https://voltiq.ru/wiki/arduino-uno-review/#:~:text= (дата обращения: 02.03.2022).

УДК 629.735.33

В. В. Перлюк*
кандидат технических наук, доцент
В. А. Масталиева**
аспирант
М. А. Епринцев*
магистрант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения
**Академический университет имени Ж. И. Алферова Российской академии наук

СИСТЕМА КОНТРОЛЯ УТЕЧЕК И ЗОН НЕСАНКЦИОНИРОВАННОГО ОТБОРА ПРИРОДНЫХ ЭНЕРГОНОСИТЕЛЕЙ В ТРУБОПРОВОДАХ

Рассмотрены подходы к формированию комплекса пассивных беспроводных датчиков давления и блоков обработки информации для выявления неразрешенных подключений к трубопроводной системе газо- и нефтепроводов. Своевременное обнаружение несанкционированных врезок с использованием пассивных беспроводных датчиков позволит оперативно в режиме реального времени обнаруживать и локализовать места утечек в газо- и нефтетранспортной системе и предотвратить хищения нефти и нанесение непоправимого урона окружающей среде.
Ключевые слова: эксплуатация газотранспортной системы, датчики давления, контроль утечек, трубопроводы.

V. V. Perliouk*
PhD, Tech., Associate Professor
V. A. Mastalieva**
PhD Student
M. A. Eprintsev*
Postgraduate Student
*St. Petersburg State Marine Technical of University
**Alferov Academic University of the Russian Academy of Sciences

SYSTEM FOR MONITORING LEAKS AND ZONES OF UNAUTHORIZED SELECTION OF NATURAL ENERGY CARRIERS IN PIPELINES

Approaches to the formation of a complex of passive wireless pressure sensors and information processing units to identify unauthorized connections to the pipeline system of gas and oil pipelines are considered. Timely detection of unauthorized tie-ins using passive wireless sensors will quickly detect and localize leaks in the gas and oil transportation system in real time and prevent oil theft and irreparable damage to the environment.
Keywords**:** operation of the gas transmission system, pressure sensors, leakage control, pipelines.

Газотранспортная система является основой Единой системы газоснабжения России. То же можно сказать и о нефтетранспортной системе. Комплексная система обеспечения надежности трубопроводов основывается на си-

стеме диагностического обслуживания магистрального газопровода и нефтепровода, позволяя повысить эффективность эксплуатации и предотвратить возникновение техногенных катастроф.

Одним из важных элементов при эксплуатации газо- и нефтепроводов является ограничение хищения газа и нефти из трубопроводов. Предотвращение незаконных подсоединений к системе трубопроводов не только уменьшит потери нефти и газа при транспортировке, но и обеспечит безопасность функционирования.

Изначально рекомендуется сформировать стационарную систему из датчиков высокой точности определения давления и блоков обработки информации, которые связаны с единым информационным центром. Далее для увеличения масштаба действия системы должна быть реализована единая система контроля и обеспечения безопасности газо- и нефтепроводов в газонефтетранспортной системе России и стран-партнеров с использованием инновационной технологии сбора информации с беспилотных летательных аппаратов вертолетного типа. Применение беспилотных летательных аппаратов вертолетного типа позволит как увеличить масштаб зоны реализации мониторинга трубопроводов, но получить аудио- и визуальную информацию. Один из вариантов применения мониторингового комплекса с летательными аппаратами вертолетного типа в применении для топливно-энергетического комплекса продемонстрирован на рис. 1.

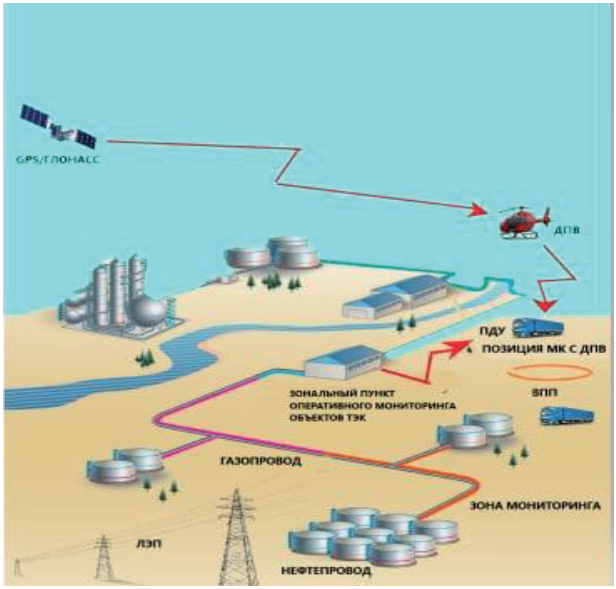


Рис. 1. Схема применения БЛА вертолетного типа

Существующие методы системы контроля утечек в газотранспортной системе требуют измерение давления газа. Разберем принцип обнаружения и локализации утечек газа с использованием бесконтактных пассивных датчиков. Наиболее перспективным представляется использование беспроводного датчика давления на поверхностных акустических волнах (ПАВ)

Конструкция датчика давления на основе линии задержки ПАВ предложена в патенте [1] и показана на рис. 2.

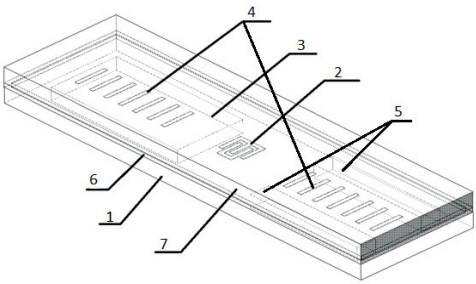


Рис. 2. Конструкция датчика давления на основе линии задержки на ПАВ

Чувствительный элемент на поверхностных акустических волнах для измерения давления содержит пьезоплату *1*. Линии задержки (ЛЗ) ПАВ-структуры, сформированные на поверхности, включают встречно-штыревой преобразователь *2*, размещенный на акустическом пути. На оборотной стороне пьезоплаты выполнено углубление, способствующее перекрытию акустического пути по апертуре. ЛЗ содержит минимум две отражающие структуры (ОС) *4*. Те, в свою очередь, состоят из массивов отражателей и расположены по обе стороны от ВШП *2*. В соответствии с принципами построения зеркальной топологии, отражающие структуры позволяют реализовывать знакопеременные зоны механических напряжений по разные стороны от ВШП. Выполнена дополнительная выемка на оборотной стороне пьезоплаты относительно поверхности с ПАВ-структурами со смещением относительно центральной оси акустического пути.

Полученный чувствительный элемент заключается в корпус для обеспечения необходимых свойств при расположении датчика в различных средах. Он состоит из рамки *6* и крышки *7*, и предназначен для герметизации устройства. ВШП *2* может быть подключен к антенне для беспроводной передачи данных. Сформированные на обратной относительно ПАВ-структур поверхности пьезоплаты выемки *3* и *5* представляют собой углубления прямоугольной формы, геометрические размеры которых определяются апертурой ВШП и протяженностью линии задержки.

Чувствительный элемент для измерения давления жидкостей и газов содержит, по меньшей мере, две контактные площадки, представляющие собой

слои металлизации, размещенные по краям пьезоплаты и предназначенные для подключения антенны или устройства опроса.

При попадании на отражающие структуры *4*, ПАВ отражается и возвращается на ВШП *2*, тем самым сформировав ответный сигнал. Воздействуя на ВШП посредством прямого пьезоэффекта, ПАВ преобразуется в электрический сигнал, который поступает на антенну датчика. С антенны датчика радиосигнал поступает на антенну считывающего устройства, в котором проводится обработка информации и принимается решение об оценке измеряемой величины. Значения механических напряжений вдоль акустического пути показаны на рис. 3.

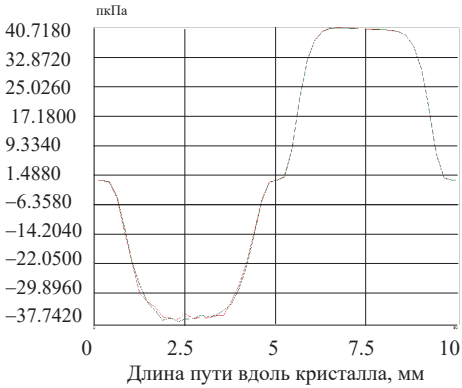


Рис. 3. Распределение механических напряжений вдоль акустического пути

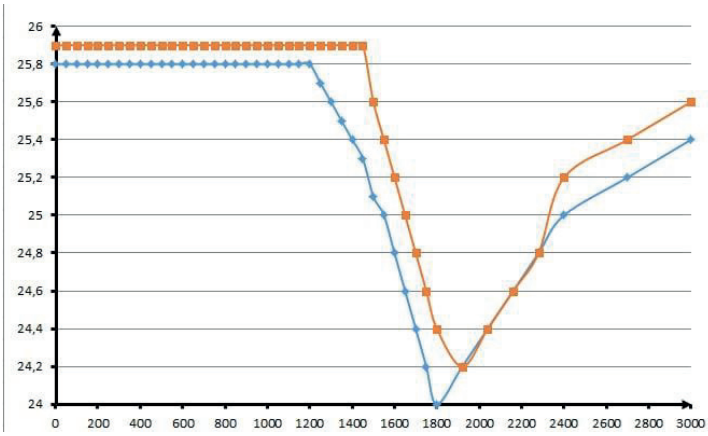


Рис. 4. Изменение давления в трубопроводе при утечке

Метод «давления волны» при использовании в трубопроводе датчика давления основан на анализе переходных процессов в трубопроводах при возникно-

вении утечки наиболее перспективен из-за своей точности и скорости определения места утечки. Метод заключается в том, что в момент повреждения трубопровода от местоположения утечки распространяются со скоростью звука волны разрежения в обоих направлениях трубопровода. Регистрируя волны в точках контроля участка трубопровода с помощью датчиков давления, появляется возможность своевременно и высокоточно обнаруживать место утечки. Пример зарегистрированной волны давления двумя датчиками системы обнаружения утечек приведен на рис. 4. Время появления утечки фиксируется спадом давления.

Математическое моделирование системы контроля утечек

Ниже приведен ряд формул, позволяющих провести моделирование системы контроля утечек.

Определение коэффициента местного сопротивления на боковое ответвление:

$$\xi_{б} = \xi_{с.б}\left(\frac{Q_{б}F_{с}}{Q_{с}F_{б}}\right)^{2}. \qquad (1)$$

Коэффициент местного сопротивления на проход:

$$\xi_{п} = \frac{\xi_{с.п}}{\left(1-\frac{Q_{б}}{Q_{с}}\right)^{2}}, \qquad (2)$$

где $\xi_{с.б}$ и $\xi_{с.п}$ – величина, взятая из кривых на рис. 5, исходя из соотношения расходов $\frac{Q_{б}}{Q_{с}}$, $Q_{б}$ – расход нефти на боковом ответвлении, в данном случае – в месте утечки, $Q_{с}$ – расход нефти на проходе, т. е. на выходе трубы.

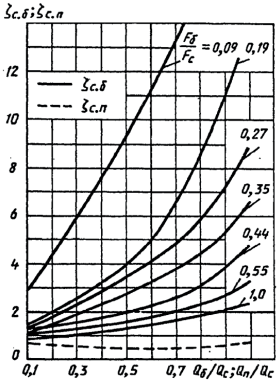


Рис. 5. Кривые $\xi_{с.б}$ и $\xi_{с.п}$ при различных значениях параметров диаметра трубы и щели [5]

Для проведения примера расчетов в *Ansys* были взяты следующие характеристики:

диаметр трубы: 200 мм,

диаметр повреждения трубы: 50 мм,

плотность нефти: 923 кг/м^3,

давление на входе: 100 кПА.

Расчет потерь давления из-за повреждения трубы:

$$S_б = \pi r^2 = 1963{,}4954\text{мм}^2 = 0{,}001963\text{м}^2,$$

$$S_п = \pi r^2 = 31415{,}9265\text{мм}^2 = 0{,}0314159\text{м}^2,$$

$$Q_б = S_б \cdot V = 0{,}001963 \cdot 0{,}162264 = 0{,}0003186048\frac{\text{м}^3}{\text{с}},$$

$$Q_c = S_c \cdot V = 0{,}0314159 \cdot 0{,}99315 = 0{,}0312\frac{\text{м}^3}{\text{с}},$$

$$\frac{Qб}{Qc} = 0{,}0102 \gg \xi_{с.п.} = 0{,}8,$$

$$\xi_п = 0{,}8 \cdot (1 - 0{,}0102) = 0{,}79184,$$

$$\xi_б = \frac{2}{0{,}0102 \cdot 16} = 12{,}21593464,$$

$$\Delta P_м = \sum \xi \frac{\rho w^2}{2} = \rho(\xi_б \frac{w_б^2}{2} + \xi_п \frac{w_c^2}{2}) =$$

$$= 932 \cdot (12{,}2159\frac{0{,}162264^2}{2} + 0{,}79184\frac{0{,}99315^2}{2}) = 514{,}5275.$$

Расчет потерь давления из-за повреждения трубы на основании данных моделирования в *Ansys:*

$$\xi_п = \frac{P_{т.вх} - P_{т.вых}}{P_{д.вх}} = 0{,}7601,$$

$$\xi_п = \frac{P_{т.вх} - P_{т.вых}}{P_{д.вх}} = 12{,}035,$$

$$\Delta P_м = 497{,}7585.$$

На основании математических вычислений было проведено моделирование в программной системе конечно-элементного анализа *Ansys*. Результаты моделирования распределения давления на участке нефтепровода приведено на рис. 6.

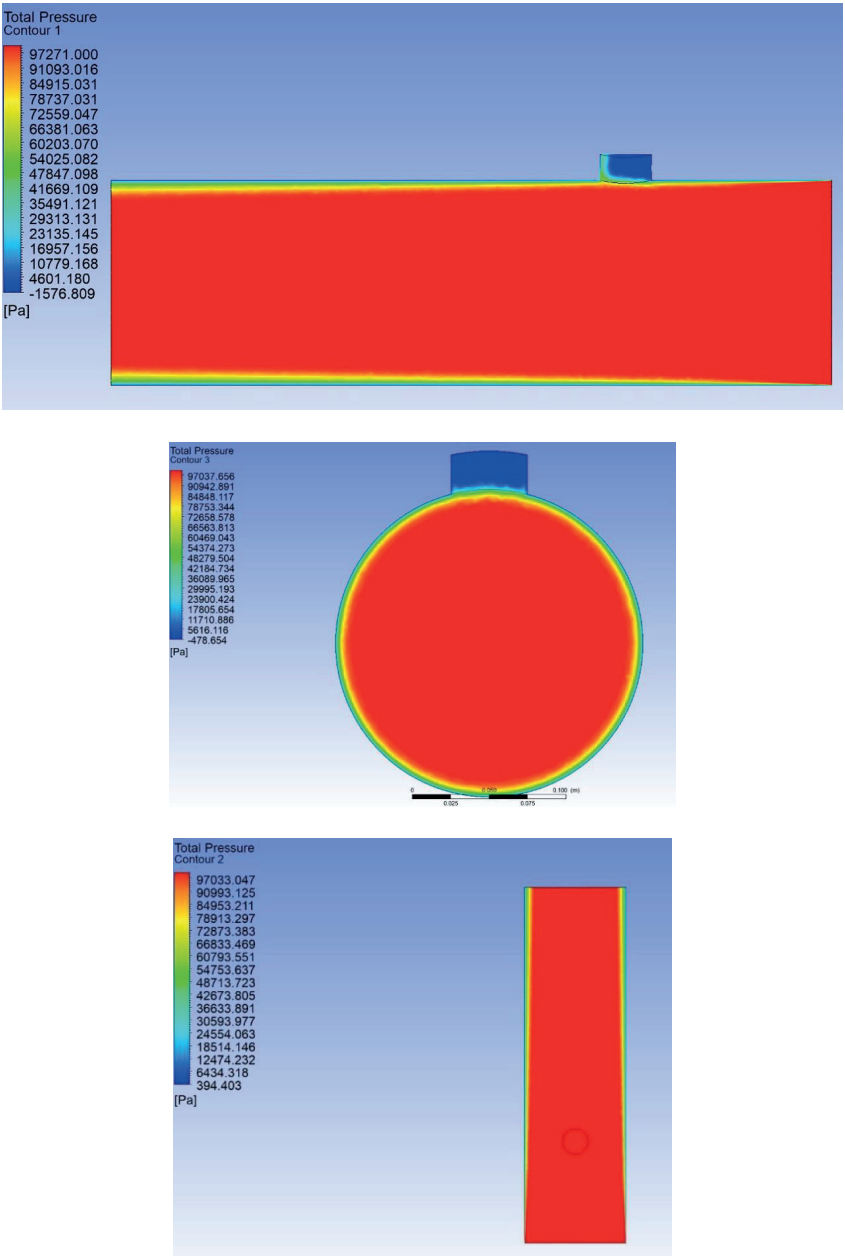


Рис. 6. Распределение давлений на участке нефтепровода с повреждением

Реализация математических расчетов в системе контроля позволяет выполнять сравнения временных маркеров и выявления смещения временных параметров давления в местах утечек трубопроводов. Визуализация полученных данных при контроле трубопровода может проводиться в цифровом и графическом виде. Таким образом можно выявлять утечки с газонефтепроводов.

Заключение

Проанализировав данный метод, можно заключить, что он позволяет с высокими скоростью и точностью обнаруживать месторасположение утечки. Обнаружение утечки происходит в течение нескольких минут, а погрешность определения места утечки меньше 100 метров. Максимальная дальность определения утечки и высокой чувствительности к малым утечкам определяет качество функционирования системы обнаружения.

Библиографический список

1. Анцев И. Г., Богословский С. В, Сапожников Г. А. Чувствительный элемент датчика давления на поверхностных акустических волнах // Вопросы радиоэлектроники. 2018. № 1. С. 93–97.

2. Анцев И. Г., Богословский С. В. Состояние и перспективы развития систем мониторинга на основе меток и датчиков на поверхностных акустических волнах // Радиопромышленность. 2015. Т. 4. С. 119–138.

3. Анцев И. Г., Богословский С. В, Сапожников Г. А. Датчик давления на поверхностных акустических волнах с зеркальной топологией // Наноиндустрия. 2020. Вып. 96. С. 389–391.

4. Состояние и перспективы развития систем мониторинга на основе меток и датчиков на поверхностных акустических волнах // Радиопромышленность. 2015. Т. 4. С. 119–138.

5. Альтшуль А. Д. Гидравлика и аэродинамика / А. Д. Альтшуль, П. Г. Киселев. М.: Стройиздат, 1975. 323 с.

УДК 62-50

В. К. Пономарев*
кандидат технических наук, доцент
В. Г. Буласова*
магистрант
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

РЕАЛИЗАЦИЯ ТИПОВЫХ ТРАЕКТОРИЙ ПОЛЕТА ВОЗДУШНОГО СУДНА В СИСТЕМЕ ЗОНАЛЬНОЙ НАВИГАЦИИ

Рассматриваются вопросы реализации ряда типовых траекторий полета воздушного судна в системе зональной навигации: вывод воздушного судна на линию пути из любой точки воздушного пространства при любом начальном курсе и подход к ней с заданным курсовым углом, вывод его в навигационную точку с заданным или произвольным путевым углом, управляемый разворот. Анализируется возможность использования для этой цели нелинейного алгоритма управления креном с функциями ограничения. Приводится методика выбора параметров нелинейного алгоритма и результаты моделирования процесса наведения, доказывающие работоспособность и эффективность рассматриваемого способа управления в спокойной атмосфере и при наличии ветра. Приводится модификация алгоритма, позволяющая решить задачу реализации управляемого разворота. Показано, что модифицированный алгоритм позволяет компенсировать влияние ветра на траекторию полета, что создает условия для программирования любой желаемой траектории полета в соответствии с общей целью технологии зональной навигации.
***Ключевые слова*:** зональная навигация**,** линия заданного пути, управление креном, нелинейный алгоритм, влияние ветра, управляемый разворот.

V. K. Ponomarev*
PhD, Tech., Associate Professor
V. G. Bulasova*
Postgraduate Student
*St. Petersburg State University of Aerospace Instrumentation

REALIZATION OF TYPICAL AIRCRAFT TRAJECTORIES IN THE AREA NAVIGATION SYSTEM

The issues of implementation of a number of typical aircraft flight paths in the area navigation system are considered: bringing the aircraft to the track from any point in the airspace at any initial heading and approaching it with a given heading angle, bringing it to a navigation point with a given or arbitrary track angle, controlled turn. The possibility of using for this purpose a nonlinear roll control algorithm with limitation functions is analyzed. A method for choosing the parameters of a nonlinear algorithm and the results of modeling the guidance process are presented, which prove the operability and efficiency of the considered control method in a calm atmosphere and in the presence of wind. A modification of the algorithm is presented that allows solving the problem of implementing a controlled turn. It is shown that the modified algorithm makes it possible to compensate for the effect of wind on the flight path, which creates conditions for programming any desired flight path in accordance with the general goal of area navigation technology.
Keywords: area navigation, set track, roll control, non-linear algorithm, wind effect, controlled turn.

Введение

Маршрут полета в воздушной навигации формируют в виде ломаной линии, состоящей из прямолинейных участков, которые сопрягаются друг с другом в точках воздушного пространства с известными координатами. Прямолинейные участки полета называют линией пути (ЛЗП). Переход от одной линии пути к другой осуществляют с помощью стандартного координированного разворота с рекомендованным для каждого воздушного судна креном. Опорные точки маршрута в классической навигации совмещают с маяками радионавигационных систем, что во многих случаях удлиняет путь и время полета воздушного судна. Кроме того, классический вариант организации воздушного движения существенно ограничивал возможности использования воздушного пространства для постоянно увеличивающегося количества воздушных судов в полете. В связи с этим в 80-х годах была разработана новая технология организации воздушной движения, которая получила название зональной навигации (*area navigation*, RNAV) [1, 2]. Эта технология позволяет воздушному судну выполнять полет по любой желаемой траектории, обеспечивающей сокращение длины пути. В RNAV базовые элементы полета (по прямой линии и разворот) сохраняются, но при этом траектория полета разбивается на ряд типовых участков, каждый из которых однозначно определен с помощью особого признака для унификации навигационных расчетов в бортовых навигационных вычислителях. Среди типовых навигационных задач в базовой (B-RNAV) и точной (P-RNAV) зональной навигации можно выделить:

– вывод воздушного судна на заданную линию пути из любого текущего места и любом значении его путевого угла;

– вывод воздушного судна в заданную точку пространства с заданным путевым углом;

– полет по линии пути, соединяющей две навигационные точки;

– разворот воздушного судна с фиксированным радиусом в условиях ветра (контролируемый разворот).

Решение типовых навигационных задач предполагает поиск и разработку законов управления креном воздушного судна, при формировании которых может использоваться только информация о текущем месте ВС относительно линии пути и скорости изменения этого параметра. Проектируемые законы управления должны быть достаточно просты. В то же время они должны обладать свойством универсальности, позволяющим их использовать при реализации большинства частных навигационных задач. В статье рассматривается возможность использования нелинейных алгоритмов формирования законов управления креном, обладающих указанными свойствами.

Нелинейный алгоритм реализации основных типовых навигационных задач

Во многих случаях типовые навигационные задачи могут быть решены при использовании нелинейного алгоритма формирования заданного значения угла крена с ограничениями [3, 4]:

$$\gamma_3^* = -k_z z^* - k_{\dot z}\dot z,$$

$$z^* = \begin{cases} z \text{ при } z < z_{\text{огр}} \\ z_{\text{огр}} \text{ при } z \ge z_{\text{огр}} \end{cases}, \ \gamma_3 = \begin{cases} \gamma_3^* < \gamma_{3\text{огр}}^* \\ \gamma_3^* \ge \gamma_{\text{огр}} \end{cases}, \qquad (1)$$

где $z_{\text{огр}}$ и $\gamma_{\text{огр}}$ – предельные значения линейного бокового отклонения и угла крена.

Коэффициенты передачи k_z, $k_{\dot z}$, а также $z_{\text{огр}}$ выбирают исходя из следующих условий:

– переходные процессы при управлении движением центра масс должны быть без перерегулирования;

– динамика системы управления креном ВС не должна существенно влиять на процесс управления траектории полета;

– при больших начальных отклонениях ВС от ЛЗП должна быть реализована траектория с постоянным углом подхода.

В первом приближении основные характеристики системы наведения с законом управления креном в форме (1) можно установить при использовании простейшей модели движения центра масс ВС в ортодромической системе координат [4]:

$$\ddot x = -\frac{g}{V}\left(\dot z - U_z\right)\sin\gamma, \ \ddot z = \frac{g}{V}\left(\dot x - U_x\right)\sin\gamma,$$

$$V = \sqrt{\left(\dot x - U_x\right)^2 + \left(\dot z - U_z\right)^2}, \ tgK = -\left(\dot z - U_z\right)/\left(\dot x - U_x\right), \qquad (2)$$

где x, z – ортодромические координаты, V – воздушная скорость, U_x и U_z – составляющие скорости ветра в проекциях на оси ортодромической системы координат, K – условный курс.

Систему управления креном можно считать идеальным динамическим звеном:

$$\gamma \equiv \gamma_3 . \qquad (3)$$

Уравнения (1) – (3) образуют замкнутую систему, описывающую движение центра масс ВС. При $V \approx \dot x - U_x, \sin \approx \gamma$ и работе алгоритма (1) в зоне линейности она преобразуется к виду:

$$\ddot z + gk_{\dot z}\dot z + gk_z z = 0. \qquad (4)$$

Методика выбора коэффициентов закона регулирования, обеспечивающая выполнение требований к траектории наведения представлена в [4].

При работе алгоритма (1) в зоне ограничения, ВС совершает разворот с постоянным углом крена до тех пор, пока не будет выполнено условие:

$$k_z z_{огр} + k_{\dot z}\dot z_п = 0, \qquad (5)$$

где $\dot{z}_п$ – линейная скорость бокового отклонения от ЛЗП на участке сближения.

Отсюда получаем:

$$z_{\text{огр}} = \frac{k_{\dot{z}} k_z \dot{z}_{\text{п}}}{k_z}. \qquad (6)$$

Величину $\dot{z}_п$ можно вычислить исходя из заданного курса подхода. При отсутствии ветра получаем:

$$\dot{z}_п = V \sin K_n. \qquad (7)$$

Таким образом,

$$z_{огр} = \frac{k_{\dot{z}} k_z V \sin K_n}{k_z}. \qquad (8)$$

Параметр $z_{\text{огр}}$, как видно, зависит и от выбранного угла K_n, и от скорости полета.

Работоспособности и характеристики системы наведения при выводе ВС на ЛЗП с законом управления креном (1) исследованы методом математического моделирования задачи по уравнениям (1) – (3).

В ходе моделирования изучалось:

– способность системы наведения вывести ВС из любой точки пространства ЛЗП при любом начальном курсе,

– влияние ветра на траектории и навигационные параметры полета,

– чувствительность к ошибкам системы управления креном.

Некоторые результаты моделирования представлены на рис. 1 – 4. Результаты получены при следующих параметрах модели: V = 200м/с, Ω_z = 0,05 c^{-1}, $K_n = 30^0$.

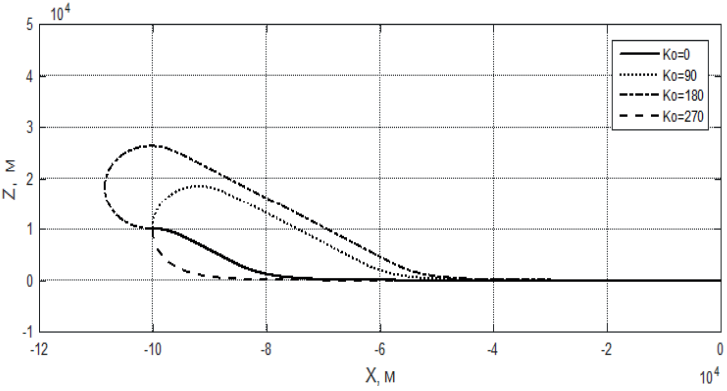


Рис. 1. Траектории ВС при выводе на ЛЗП

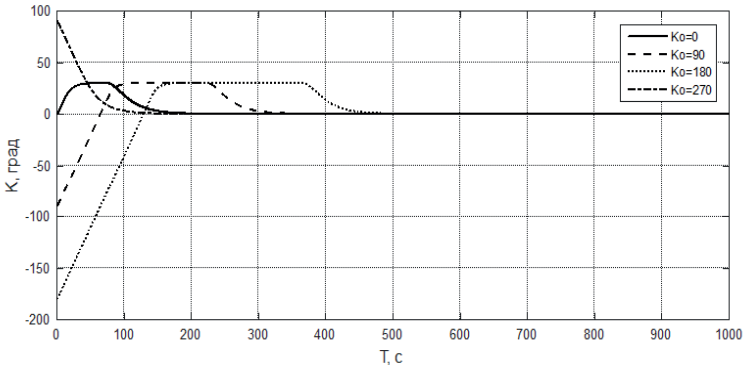


Рис. 2. Графики текущего курса при разных значениях начального курса ВС и отсутствии ветра

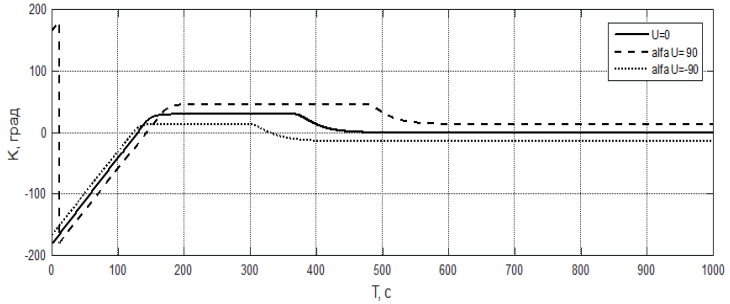


Рис. 3. Траектории ВС при наличии бокового ветра

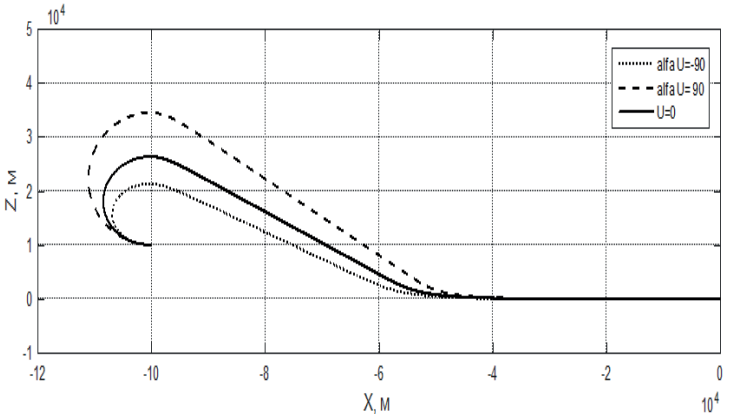


Рис. 4. Графики текущего курса при наличии бокового ветра

По результатам моделирования сделаны следующие выводы:

1. Закон управления траекторным движением в форме (1) обеспечивает вывод ВС на ЛЗП из любой точки воздушного пространства при любом начальном курсе и подход к ней с заданным курсовым углом.

2. При действии бокового ветра изменяется угол подхода ВС к ЛЗП. При этом, время выхода на ЛЗП практически не меняется, а ошибка по боковому отклонению после окончания маневра становится равной нулю. После окончания маневра выхода ВС на заданную линию пути курс ВС отличается от азимута ортодромии на угол ветра.

3. Основными причинами отклонения ВС от ЛЗП после завершения маневра являются ошибки измерения бокового смещения и ошибки системы управления креном при отработке заданного значения управляемого параметра.

Алгоритм (1) можно использовать и при решении задачи вывода ВС в навигационную точку с заданным путевым углом. В этом случае в навигационном вычислителе должны быть произведены расчеты, связанные с построением локальной ортодромии и определением бокового отклонения от нее. Локальная ортодромия при этом задается координатами навигационной точки и азимутом ортодромии, равном требуемому путевому углу прибытия ВС. Подобным образом решается и задача наведения ВС при полете на точку без задания конечного путевого угла.

Реализация управляемого разворота

Для уменьшения ошибок самолетовождения на всем протяжении маршрута помимо стабилизации на ЛЗП необходимо реализовать режим стабилизации воздушного судна и на криволинейных участках полета. При этом в навигационном вычислителе можно сформировать сигнал управления креном по алгоритму

$$\gamma_З = \gamma_{ПР} - k_z z - \dot{k}_{\dot{z}} \dot{z}, \tag{9}$$

где $\gamma_{ПР}$ – программное значение угла крена; z, $\dot{z}$ – текущие значения линейное отклонение воздушного судна вдоль нормали к траектории разворота и проекция текущей путевой скорости полета на нормаль к траектории разворота; k_z и $\dot{k}_{\dot{z}}$ – передаточные числа закона управления в режиме управляемого разворота.

Схема формирования текущих отклонений от заданной траектории разворота и скорости отклонения приведена на рис. 5.

На рис. 5 сделаны следующие обозначения: Rр – расчетный радиус разворота, D – дистанция ВС до центра разворота, ПУ – текущий путевой угол ВС, W – вектор путевой скорости ВС, A1 – пеленг (азимут) центра разворота, W_k – составляющая путевой скорости, касательная к траектории разворота.

В соответствии с рис. 5 величина z определяется по формуле:

$$z = F\left(R_P - D\right), \tag{10}$$

а составляющие путевой скорости на нормаль и касательную к траектории разворота с использованием выражений:

$$\begin{aligned} \dot{z} &= FW\cos\left(A1 - ПУ\right), \\ \mathrm{W_k} &= FW\sin\left(A1 - ПУ\right), \end{aligned} \tag{11}$$

где функция F учитывает направление разворота, которая формируется по условию:

$$F = \begin{cases} 1, & \text{если разворот вправо} \\ -1, & \text{если разворот влево} \end{cases}.$$

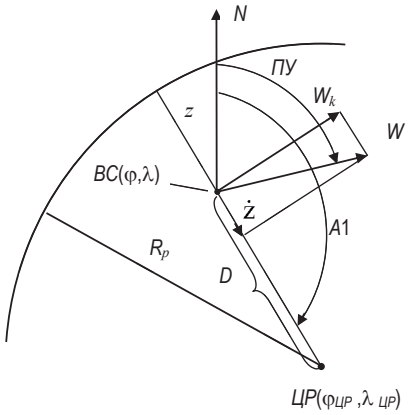


Рис. 5. Траектория и параметры полета при выполнении управляемого разворота

Программная составляющая заданного значения угла крена вычисляется по формуле:

$$\gamma_{\text{пр}} = F\ \mathrm{arctg}\frac{W_k^2}{R_\text{Р}\cdot g}, \tag{12}$$

где g – ускорение силы тяжести.

На рис. 6 – 8 представлены некоторые результаты математического моделирования полета воздушного судна при выполнении управляемого разворота. Сплошными линиями обозначены графики отклонения положения воздушного судна от траектории полета при управляемом развороте, а пунктирными – при простом развороте.

Моделирование выполнялось при следующих условиях: $R_\text{Р}$ = 20 000 м; V = 200 м/с; U = 20 м/с.

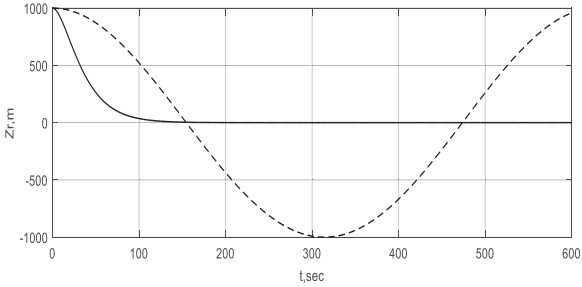


Рис. 6. Отклонение воздушного судна от расчетной траектории разворота при наличии ошибки вывода в точку начала разворота

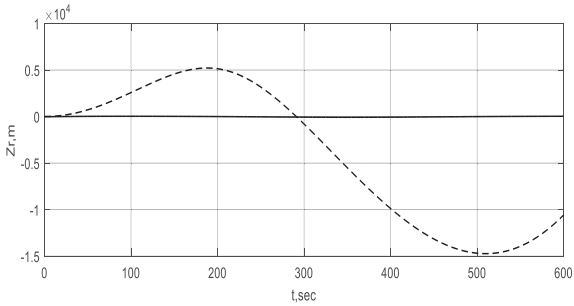


Рис. 7. Влияние попутного ветра в точке начала разворота

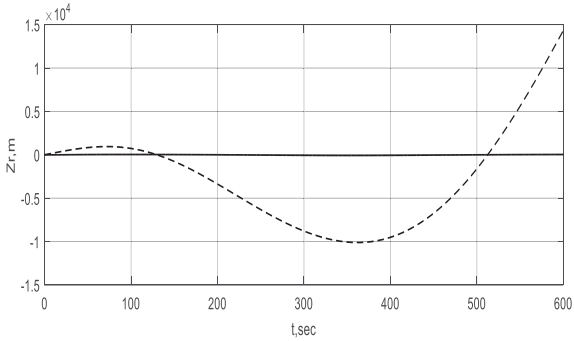


Рис. 8. Влияние бокового ветра в точке начала разворота

Представленные результаты моделирования подтверждают работоспособность и эффективность рассмотренного способа формирования сигнала

управления креном воздушного судна при выполнении им управляемого разворота.

Заключение

Представленные результаты исследования позволяют сделать следующие выводы:

1. Для решения задач реализации типовых траекторий полета в системе зональной навигации может быть рекомендован нелинейный алгоритм формирования сигнала управления креном воздушного судна в форме (1). Этот алгоритм обладает свойством универсальности и обеспечивает не только вывод воздушного судна на линию пути из любой точки воздушного пространства при любом начальном курсе и подход к ней с заданным курсовым углом, но и вывод его в навигационную точку с заданным или произвольным путевым углом;

2. Представленный в форме (12) алгоритм формирования сигнала управления креном воздушного судна в режиме управляемого разворота позволяет компенсировать влияние ветра на траекторию полета и может служить основой при разработке вопросов реализации полетов по любым желаемым траекториям, что является главной целью внедрения технологии зональной навигации.

Библиографический список

1. Navigation System Data Base. ARINC Specification 424.

2. Вовк В. И., Липин А. В., Сарайский Ю. Н. Зональная навигация: учеб. пособие. СПб.: АО Центр автоматизированного обучения. 2004. 126 с.

3. Автоматизированное управление самолетами и вертолетами / Под ред. С. М. Федорова. М.: Транспорт. 1977. 246 с.

4. Байбородин Ю. В., Драбкин В. В., Сменковский Е. Г. Бортовые системы управления полетом. М.: Транспорт, 1988. 336 с.

5. Буласова В. Г., Пономарев В. К. Нелинейный алгоритм управления креном при выводе воздушного судна на линию заданного пути // Системный анализ и логистика: журнал. Вып. № 2 (28). ISSN 2077-5687. СПб.: ГУАП, 2021. С. 3–8. DOI: 10.31799/2077-5687-2021-2-3-8.

УДК 629.7.08

С. Ф. Скорина*
кандидат технических наук, доцент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

МОДЕЛЬ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНТЕЛЛЕКТУАЛЬНОГО ТРАНСПОРТНОГО СРЕДСТВА ДЛЯ ПРОТИВООБЛЕДЕНИТЕЛЬНОЙ ОБРАБОТКИ САМОЛЕТОВ

Обоснована необходимость и рассмотрены подходы к формированию информационного обеспечения интеллектуального транспортного средства для противообледенительной обработки самолетов.
Ключевые слова: информационное обеспечение, интеллектуальное транспортное средство, противообледенительная обработка, самолет.

S. F. Skaryna *
PhD, Tech., Associate Professors
*St. Petersburg State University of Aerospace Instrumentation

MODEL OF INFORMANION SUPPORT OF AN INTELLIGENT VEHICLE FOR DE-AISING TREATMENT OF AIRCRAFT

Model information support of an intelligent vehicle for de-icing treatment of aircraft. The necessity is substantiated and approaches to the formation of information support for an intelligent vehicle for anti-icing treatment of aircraft are considered.
Keywords: information support, intelligent vehicle, anti-icing treatment, aircraft.

Повышение эффективности использования воздушного транспорта неразрывно связано с обеспечением его всепогодности и возможности выполнения плановых полетов в сложных метеорологических условиях. Одним из эффективных подходов к решению указанной проблемы является внедрение инновационных технологий в транспортную инфраструктуру аэропортов. Речь идет о построении и последующем использовании интеллектуальных специализированных транспортных средств (ТС). Эффективное функционирование умного транспортного средства требует существенного расширение номенклатуры позиций собственного информационного обеспечения, сбора, анализа и обмена информацией с другими подвижными объектами инфраструктуры аэропорта (самолеты, вспомогательные транспортные средства).

В Российской Федерации около 40% территории расположено в высоких широтах, для которых характерно короткое лето, продолжительная зима и достаточно длительные отрезки времени, приходящиеся на осень, зиму и весну. Для осенне-зимне-весеннего сезона характерны температурные «качели», сопровождающиеся не только частыми и значительными изменениями модуля температуры, но и неоднократные переходы температуры от плюсовых к минусовым значениям и обратно. Перечисленные обстоятельства усугубляют потен-

циальную опасность возникновения обледенения воздушных судов (ВС) в большинстве российских аэропортов, расположенных в высоких и средних широтах.

Метеоусловия в районе аэродрома, способствующие интенсивному обледенению, усугубляются и сложной аэрологической обстановкой. Последняя обусловлена отсутствием в районе стоянки ВС достаточного количества сооружений в виде функциональных зданий аэропорта и естественных препятствий в виде лесополос, переменного рельефа местности и т. п. Совокупность ветровых воздействий наряду с температурным фоном окружающей среды создают дополнительные предпосылки для возникновения обледенения. Следует также учитывать, что независимо от уровня автоматизации процессов проведения противообледенительной обработки соответствующие технические средства относятся к классу эргатических систем, функционирование которых происходит с участием человека-оператора, реализующего технологический процесс с помощью специализированной техники, расположенной на транспортном средстве (автомобиле).

Для специализированного ТС с размещенным на нем оборудованием для проведения противообледенительной обработки среди технических работников аэропортов сложилось устойчивое сленговое, но отражающее суть, короткое название англоязычного происхождения – деайсер. Участие человека в технологическом процессе обработки ВС определяет насущную необходимость учета так называемого человеческого фактора, со всеми характерными проблемами. Все это определяет целесообразность и актуальность использования комплексного, системного подхода к созданию специализированных средств, предназначенных для выполнения предполетной противообледенительной обработки ВС. Насущная необходимость проведения модернизации применяемых в аэропортах деайсеров и изменения технологии выполнения соответствующих работ подтверждает и произошедшее 2 декабря 2021 года в России летное происшествие с пассажирским ВС Airbus A321 авиакомпании S7, которое летело из Магадана в Новосибирск. Это происшествие могло закончиться катастрофой ВС, гибелью всех 199 пассажиров и 7 членов экипажа [1].

Расследование инцидента показало, что противообледенительная обработка была выполнена с рядом нарушений регламентированной технологии. Это привело к образованию льда во время взлета в приемниках полного воздушного давления информационного комплекса воздушно-скоростных параметров (ИК ВСП), нарушению ламинарного течения воздушного потока, к искажению информации о истинной воздушной скорости, отключению автопилота и автомата тяги. В результате угловые эволюции ВС по крену и тангажу в процессе полета достигали 40–45^0 градусов, самолет потерял 2700 метров высоты, заход на посадку и саму посадку пришлось осуществлять в ручном режиме.

Сегодня на рынке техники для предполетного обслуживания ВС представлены многочисленные образцы деайсеров импортного (*GLOBAL Ground Support*, *Safeatro, WESTERGAARD,* LAS-1) и отечественного производства (Гейзер, ПМ, МЕ) [2]. Из-за проблем, обусловленных санкционной политикой за-

падных стран, представляется целесообразным как с технических, так и с экономических позиций, рассмотреть основные направления проведения комплексной модернизации отечественной техники.

Анализ тактико-технических характеристик деайсеров отечественного и импортного производства выявил ряд характерных особенностей. В целом и те, и другие успешно выполняют возложенные на них функции по проведению противообледенительной обработке ВС [3]. При этом параметры, характеризующие процесс обработки с помощью импортных и отечественных систем, такие как объем баков с рабочей жидкостью, производительность, высота подъема кабины с форсунками и оператором и др., практически не отличаются.

Основные отличия касаются наличия, так называемых, сервисных функций, которые с одной стороны обеспечивают комфортные условия работы оператора, с другой – способствуют непосредственно повышению эффективности выполняемых работ и безопасности полетов в сложных метеоусловиях, уменьшают риски, обусловленные человеческим фактором. Реализуются эти сервисные функции за счет совершенствования структуры и состава информационного обеспечения деятельности оператора путем оснащения деайсера дополнительными сенсорами, которые позволяют контролировать параметры выполняемого технологического процесса. К таким датчикам относятся:

– датчики температуры окружающего воздуха, рабочей жидкости, воздуха в кабине оператора и водителя;

– датчики давления рабочей жидкости в баке и на входе распределительной форсунки;

– счетчики моточасов (наработки) транспортного средства, компрессоров и насосов в составе деайсера;

– сенсоры встроенной системы контроля и диагностики технического состояния основных агрегатов и систем:

– датчики системы аварийного оповещения при возникновении предотказового состояния основных агрегатов и возникновения опасного сближении ВС с распределительной форсункой.

Очевидно, что при таком многообразии источников разноплановой информации и необходимости ее дальнейшего эффективного использования деайсер должен быть оснащен бортовым вычислительным устройством обработки и представления информации оператору и водителю.

Анализ продукции современного отечественного приборостроения свидетельствует об отсутствии, как таковой, проблемы импортозамещения, поскольку все вышеупомянутые датчики, устройства обработки и отображения информации в достаточном количестве и необходимого качества выпускаются российскими предприятиями и могут найти применение при совершенствовании информационного обеспечения российских деайсеров [4]. При этом представляется целесообразным при проведении модернизации или при выпуске новых моделей дооснастить их следующими источниками информации:

– для осуществления текущего контроля соблюдения технологии обработки ВС необходим расходомер, позволяющий получать информацию о рас-

ходе используемой для обработки рабочей жидкости в единицу времени. Эта информация также позволяет контролировать оставшиеся в баках объемы рабочей жидкости и отказаться от непосредственного контроля уровня жидкости;

– плотномер, информация от которого необходима при входном контроле используемой рабочей жидкости для обработки ВС на соответствие заданной плотности и коррекции показаний расходомера;

– датчики стояночного курса ВС и деайсера. Информация от этих сенсоров необходима для остановки процесса противообледенительной обработки в случае, когда. курсовые углы ВС и деайсера отличаются на 180^0. При таком расположении объектов, возникает возможность попадания противообледенительной жидкости в приемники воздушного давления ИК ВСП и в компрессоры низкого давления двигателей ВС;

– подсистема контроля допустимой дистанции между распределительной форсункой деайсера и ВС на базе видеокомплекса с системой инцидентного анализа. В качестве источников информации о фактическом расстоянии между объектами могут найти применение как лазерные дальномеры, так и датчики машинного зрения. Одной из важных характеристик последних является простота и инвариантность к условиям применения.

– полезной для строгого соблюдения технологического процесса может быть и информация о фактической температуре обрабатываемых поверхностей ВС, которая может отличаться от температуры окружающей среды из-за использования экипажем штатных, встроенных систем предотвращения обледенения. Указанную информацию можно получить от тепловизора или более дешевых пирометров.

– датчик высоты распределительной форсунки деайсера по отношению к поверхности специализированной площадки для противообледенительной обработки самолетов.

Большинства упомянутых выше датчиков может быть выполнено на базе хорошо отработанной технологии производства микро-электромеханических систем, обеспечивающей микроминиатюризацию и исключительно низкую стоимость единицы продукции. Для обеспечения высокой надежности деайсера в целом могут быть применены принципы структурного резервирования сенсоров с наибольшими значениями интенсивностей отказов. Предложенные мероприятия будут способствовать роста эксплуатационной надежности аэродромной техники, повышению эффективности выполнения противообледенительной обработки ВС и, как следствие, обеспечат дополнительный вклад в повышение безопасности выполнения полетов.

Библиографический список

1. Федеральное агентство воздушного транспорта. URL: https://www.favt.gov.ru/ (дата обращения: 10.01.2022).

2. Руководство по прогнозированию метеорологических условий для авиации / ред. К. Г. Абрамович, А. А. Васильев. Л.: Гидрометеоиздат, 1985. 301 с.

3. Сторожук М. В. Наземное обледенение воздушных судов: Меры по предупреждению авиационных происшествий // Научный сборник МГТУ ГА, 2015. № 219. С. 93–100.

4. Онлайн журнал. Датчики и сенсоры: Практика использования, теоретические основы. Современные тенденции. URL: http://www.datchikisensor.narod.ru/ (дата обращения: 28.02.2022).

УДК 656.614.34

Е. С. Тимошек*
старший преподаватель
Т. Е. Маликова*
доктор технических наук, доцент
А. Ж. Радочинская*
аспирант
*Морской государственный университет имени адмирала Г. И. Невельского

МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЫГРУЗКИ СУДНА НА РЕЙДЕ С ИСПОЛЬЗОВАНИЕМ ВСПОМОГАТЕЛЬНОГО ФЛОТА

Рассмотрена одна из задач управления работой флота малой судоходной компании, осуществляющей перевозку грузов снабжения в районах Восточной Арктики, на уровне рейсового планирования, а именно, частная задача разгрузки транспортных судов на рейде. Предложено в качестве инструментария решения задачи формализации технологического процесса обработки судна использовать сетевое моделирование (сетевой график). Основными результатами исследования являются сетевой график выгрузки судна на рейде и логика его построения. Практическое применение сетевой модели «выгрузки судна на рейде» позволяет определить максимальную производительность технологических линий по вариантам работ и оптимальное время завершения грузовых работ в порту.
Ключевые слова: морской транспорт, рейдовый порт, моделирование, управление работой флота, перегрузочные операции.

E. S. Timoshek*
Senior Lecturer
T. E. Malikova*
Dr. Sc., Tech., Associate Professor
A. Zh. Radochinskaia*
PhD Student
*Maritime State University named after Admiral G. I. Nevelskoi

MODELING THE PROCESS OF UNLOADING A SHIP IN THE ROADSTEAD BY USING AUXILIARY FLEET

One of the tasks of managing the fleet of a small shipping company that transports supplies in the regions of the Eastern Arctic at the level of voyage planning, namely, a particular task of unloading transport ships in the roadstead, is considered. It is proposed to use network modeling (network diagram) as a tool for solving the problem of formalizing the technological process of ship processing. The main results of the study are the network schedule for unloading the vessel in the roadstead and the logic of its construction. The practical application of the network model of "ship unloading in the roadstead" makes it possible to determine the maximum productivity of technological lines according to the options for work and the optimal time to complete cargo operations in the port.
Keywords: sea transport, raid port, simulation, fleet management, loading operations**.**

Сбалансированное развитие инфраструктуры транспорта является одной из приоритетных задач любой из стран мирового сообщества. Решение этой задачи предполагает комплексное развитие всех элементов транспортной инфра-

структуры на основе всестороннего анализа статистики и использования математических методов прогнозирования потребностей рынка морских перевозок [1], построения транспортно-экономического баланса [2, 3], прогнозирования динамики грузовой базы, анализа моделей развития транспортной системы с целью выбора оптимально сбалансированных вариантов [4, 5], а также формирования рынка конкурентоспособных транспортных услуг [6]. Необходимо создать такие условия, в которых уровень предложения транспортных услуг был выше спроса на эти услуги, а также запуск в практику работы предприятий морского транспорта механизма «цена – качество», который обеспечит формирование конкурентной среды транспортных компаний.

Для больших и средних судоходных компаний в рамках оценочных средств механизма «цена – качество» есть возможность в процессе переходного периода использовать в своей работе в том числе и методику планирования и минимизации комплексных эксплуатационных расходов по флоту и по порту созданную еще в советский период, то для малых судоходных компаний каких-либо подобных методик просто не существует в силу отсутствия подобных компаний во временной период (50–90-х гг. прошлого века) разработки математического аппарата принятия управленческих решений на морском транспорте. В связи с этим и сложился замысел научного исследования отличительных особенностей управления флотом малой судоходной в процессе выгрузки судна на рейде [7], а затем разработки методики управления ее флотом на основе мониторинга и оценки значений по таким направлениям поиска как: резерв пропускной способности транспортной сети; скорость доставки грузов; гибкость транспортно-логистических технологий при обработке транспортного судна.

Немаловажными вопросами в любом научном исследовании являются абстрагирование конкретных свойств изучаемого объекта путем перехода на формализованный язык описания, например, к математической модели [8, 9], последующая реализация модели одним из известных методов решения и интерпретация полученных результатов для принятия управленческих решений [10]. В качестве инструментария описания процесса выгрузки судна на рейде с использованием вспомогательного флота было выбрано сетевое моделирование.

Моделируемые условия рейдовой выгрузки (постановка задачи). Судно выполняет несколько последовательных судозаходов в порты на побережье Восточной Арктики. В модели рассматривается два варианта выгрузки: в порту, оборудованном причалами и техническими средствами для производства грузовых работ; в поселках (портопунктах) выгрузка осуществляется на необорудованный берег с использованием самоходной баржи, доставленной на транспортном судне. Груз выгружается по двум последовательным вариантам работ: «судно – плавсредство (ПС)» и «плавсредство – берег».

Описание первого варианта выгрузки. Порт оборудован техническими средствами для производства погрузочно-разгрузочных работ (ПРР), но вследствие небольших глубин у причалов выгрузка осуществляется на рейде, а при неблагоприятных погодных условиях (волна, ветер) или загруженности причала

возможна выгрузка на необорудованный берег, где сооружается временный настил для перемещения тракторов. Перевалка груза осуществляется с использованием вспомогательного флота порта.

Технологическая схема по варианту «СУДНО – ПС»: палуба / трюм – СС (судовые стрелы / кран) – ПС. Вариативность в этом звене: выгрузка производится либо на две баржи большой грузоподъемности, либо на четыре баржи маленькой грузоподъемности.

Выгрузка груза из плавсредства («ПС – берег») может производиться по двум технологическим схемам. Первый случай, когда погодные условия благоприятны, и причал свободен, технологическая схема выгрузки: ПС –кран –склад. Второй случай, когда причал занят или погодные условия не позволяют подойти к пирсу. Технологическая схема выгрузки: ПС – трактор (волокуша) – кран – склад. Технологический процесс второго варианта: баржа двигается к точке выгрузки, где уже ждут тракторы, утыкается в берег, опускает аппарель, и тракторы вытягивают контейнеры на волокушах на складскую площадку для дальнейшей выдачи клиентам. Сетевой график для данного варианта представлен на рис. 1.

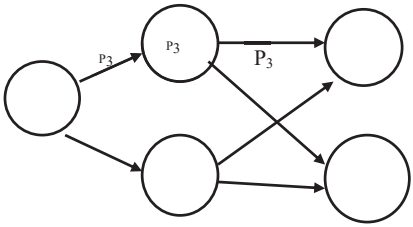


Рис. 1. Сетевой график выгрузки на рейде с использованием средств порта

Второй вариант сетевого графика (рис. 2) предназначен для поселков и портопунктов, в которых выгрузка осуществляется на необорудованный берег с использованием самоходной баржи, тракторов и оборудования, доставленных на транспортном судне.

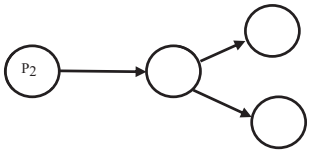


Рис. 2. Сетевой график рейдовой выгрузки на необорудованный берег

На рейде выгрузка осуществляется на самоходную баржу с использованием судового крана (судовых стрел). Предварительно с судна спускают баржу, на нее устанавливают тракторы и доставляют их к берегу. Баржа возвращается к транс-

портному судну, и начинается выгрузка контейнеров. Судовая операция выполняется по технологической схеме: палуба / трюм – СС (кран) – ПС. Организация работ по варианту «ПС – берег» возможна по двум технологическим схемам. Первая технологическая схема: ПС – трактор (волокуша) – кран –склад; вторая технологическая схема: ПС – трактор (волокуша) – кран – автомашина.

Объединим два построенных сетевых графика в единую транспортную сеть (рис. 3). При этом за источник транспортной сети примем транспортное судно (пункт P_0), последовательно обходящее порты выгрузки, а за сток – фиктивный пункт доставки P_9.

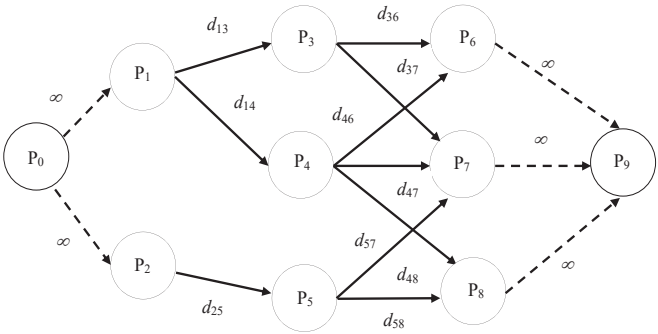


Рис. 3. Сетевая модель выгрузки судна на рейде: P_0 – транспортное судно; P_1 – порт, оборудованный техническими средствами для производства ПРР, имеет самоходные баржи; P_2 – портопункт, предполагающий выгрузку на необорудованный берег с использованием баржи транспортного судна; P_3 – погрузка больших барж на рейде; P_4 – погрузка малых барж на рейде; P_5 – погрузка самоходной баржи на рейде; P_6 – выгрузка на склад; P_7 – выгрузка на необорудованный берег – складская площадка; P_8 – выгрузка на необорудованный берег – автомашина, d_{ij} – пропускная способность соответствующей операции

Так как любая сетевая модель напрямую зависит от конкретного технологического процесса, и ее структура должна описывать строго этот процесс, то математическая модель выгрузки судна на рейде, представленная на рис. 3 является всего лишь одним из возможных вариантов. За основу в примере построения сетевой модели был взят реальный технологический процесс выгрузки грузов компании ООО «МаринТЭК» [11]. В сетевой модели выгрузки на рейде представлен вариант движения судна между двумя соседними портами: (P_1) – порт, оборудованный техническими средствами для производства ПРР, имеет самоходные баржи; (P_2) – портопункт, предполагающий выгрузку на необорудованный берег с использованием баржи транспортного судна. В данной модели главным является не сама математическая модель, а логика рассуждений, в результате которой и была она (модель) получена. Численная реализация сетевой модели возможна различными математическими методами. Например, в сетевой постановке (рис. 3) задача

решается методом Форда – Фалкерсона, а если перейти к записи модели на языке задачи линейного программирования – симплексным методом.

Вывод

Сетевая модель выгрузки транспортного судна с использованием вспомогательного флота раскрывает логику технологического процесса и позволяет определить максимальную производительность технологических линий по вариантам работ, которая в свою очередь может быть использована для определения времени выгрузки. На основе в том числе и данной модели авторами была разработана автоматизированная система управления флотом малой судоходной компании при доставке грузов снабжения на побережье Восточной Арктики.

Библиографический список

1. Изотов О. А. Прогнозирование перевозок грузов // Системный анализ и логистика. 2019. № 4 (22). С. 12–19.

2. Майоров Н. Н. Развитие морских паромных перевозок в балтийском море в контексте глобальных тенденций // Системный анализ и логистика. 2020. № 1 (23). С. 65–73.

3. Майоров Н. Н. Методологический базис организации сети морских пассажирских перевозок // Вестник астраханского государственного технического университета. Серия: морская техника и технология. 2018. № 2. С. 28–37.

4. Янченко А. А. Экспериментальные исследования влияния зонирования контейнерного терминала на эффективность его работы в условиях свободного порта Владивосток / А. А. Янченко, Т. Е. Маликова, Д. А. Оськин // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2019. Т. 11. № 1. С. 57–67. DOI: 10.21821/2309-5180-2019-11-1-57-67.

5. Tsvetkova A. Social responsibility practice of the evolving nature in the sustainable development of Arctic maritime operations // Arctic Marine Sustainability. Springer, Cham, 2020. С. 119–143.

6. Тимошек Е. С. Распределительная модель судов снабжения Арктического региона на участке транспортной сети / Е. С. Тимошек, Т. Е. Маликова // Вестник Волжской государственной академии водного транспорта. 2019. № 60. С. 213–222.

7. Худяков С. А. Технология перевозки грузов в порты с ограниченными глубинами / С. А. Худяков, Г. А. Зеленков, Т. Н. Тимченко // Эксплуатация морского транспорта. 2020. № 3 (96). С. 3–11.

8. Маликова Т. Е. Применение теории катастроф для классификации сценариев потери остойчивости судна при смещении груза // Вестник государственного университета морского и речного флота им. адм. С. О. Макарова. 2014. № 3 (25). С. 15–19.

9. Радочинская А. Ж. Обоснование возможности описания алгоритма разделения опасных грузов на языке конечных автоматов / А. Ж. Радочинская, Т. Е Маликова, А. Ю. Стрелков // Волновая электроника и инфокоммуникационные системы. Материалы XXIV Международной научной конференции. В 3 ч. СПб. 2021. С. 256–262.

10. Маликова Т. Е. Результаты численной реализации задачи расстановки флота малой судоходной компании / Т. Е. Маликова, Е. С. Тимошек // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2020. Т. 12. № 4. С. 654–665. DOI: 10.21821/2309-5180-2020-12-4-654-665.

11. Тимошек Е. С. Определение зоны эффективного использования транспортного флота в арктическом регионе на примере группы судов компании ООО «Маринтэк» / Е. С. Тимошек, С. Е. Чуйкова // Вестник Волжской государственной академии водного транспорта. 2019. № 61. С. 184–193.

УДК 62-503.56

А. Ю. Федоринов*
аспирант
В. В. Перлюк*
кандидат технических наук, доцент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ МАЛЫХ КОСМИЧЕСКИХ АППАРАТОВ В ГРУППЕ НА ОСНОВЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ РОЕВОГО ИНТЕЛЛЕКТА

Рассматривается задача математического моделирования оптимального метода группировки малогабаритных летательных аппаратов. Моделирование осуществляется в среде *Matlab*. В качестве примера выбран микро-спутник *Cubesat* (кубсет). Поставлена задача обеспечить безопасный и эффективный групповой полет для множества микро-спутников на низко-земной орбите, связь между спутниками осуществляется по средству радио-видео сигналов. В качестве метода группировки и управления будет использоваться алгоритм Роя.
Ключевые слова: *Cubesat,* микро-спутники, алгоритм Роя, групповая робототехника, моделирование, прогнозирование.

A. Y. Fedorinov*
PhD Student
V. V. Perlyuk*
PhD, Tech., Associate Professor
*St. Petersburg State University of Aerospace Instrumentation

DEVELOPMENT OF A MOTION CONTROL SYSTEM FOR SMALL SPACECRAFT IN THE GROUP BASED ON SIMULATION METHODS USING SWARM INTELLIGENCE

The problem of mathematical modeling of the optimal method of grouping small-sized aircraft is considered. Modeling is carried out in the Matlab environment. The micro-satellite Cubset is chosen as an example. The task is to provide a safe and efficient group flight for a variety of micro-satellites in low-Earth orbit, communication between the satellites is carried out by means of radio-video signals. The «Swarm» algorithm will be used as a grouping and control method.
Keywords: Cubesat, micro satellites, Swarm algorithm, group robotics, modeling, forecasting.

Введение

В настоящее время ведутся масштабные работы по освоению космоса, производиться запуск огромного числа спутников для решения всевозможных целей и задач, однако для группового полета мало просто вывести спутники на орбиту, необходимо иметь эффективные и надежные алгоритмы верного взаимодействия спутников между собой. Алгоритмы должны выстраивать летательные аппараты (ЛА) по определенным заданным параметрам, а при возникновении неисправностей оперативно перестраивать ЛА для продолжения мис-

сии. Таким методом в рассматриваемом случаи послужит алгоритм Роя, он отлично зарекомендовал себя в микро-робототехники, так с его помощью решаются задачи, в которых фигурируют десятки и даже сотни роботизированных единиц. Говоря о единицах спутников, в работе будут рассмотрены *CubeSat* – формат малых (сверхмалых) искусственных спутников Земли для исследования космоса, имеющих габариты 10×10×10 см при массе не более 1,33 кг. Для более эффективного использования такого подходя требуется решение комплексной научно-технической задачи взаимоориентации микроспутников друг с другом [1]. В статье будет рассмотрена задача внедрения разработанных алгоритмов Роя в систему спутников.

Постановка задачи

Рассматривается задача обеспечения полета группы малых космических аппаратов (микроспутников) с учетом небольших взаимных расстояний между ними. Моделирование будет проводиться в среде *Matlab.* Главной задачей исследования будет разработка и анализ алгоритмов по взаимной ориентации малых летательных аппаратов, а точнее управлением их движением и формирования определенной системы построения в групповом полете. Связь между отдельными объектами чаще все осуществляется по средству радио-видео связи [2]. Сформированная структура используемых каналов связи должна обеспечить высокую динамику в передаче данных, возможность оперативной реконфигурации каналов связи с помощью разделенных друг относительно друга космического и наземного сегмента. В качестве алгоритма обработки информации (позиционирование микро-спутников относительно друг друга) будет использоваться алгоритм Роя.

Одна из главных задач при групповом полете это распределение заданий и действий, которые производит каждый спутник. На протяжении всего полета микроспутники будут изменять свою позицию и ориентацию в пространстве и относительно друг друга, поэтому ориентация кубсета будет четко известна алгоритмы позиционирования [3].

Для определения относительного фазового состояния аппаратов в группе используется обработка видеоизображений, получаемых при съемке одного аппарата с помощью видеокамеры, установленной на другом аппарате. Используется метод, основанный на распознавании на снимке некоторых точек аппарата, положение которых известно в системе отсчета, связанной с этим аппаратом [4].

Широко известны методы выделения (идентификации) характерных признаков в изображении сцены, которые используются в системах машинного зрения [5]. Суть метода, применительно к формированию геометрической модели микроспутника по изображению, состоит в селекции из полученного входного массива точек изображения некоторых локальных признаков, определяющих отличительные особенности формы и геометрических размеров именно того реального объекта, для которого создается данная геометрическая модель. Данный метод относится к классу пространственно-временной селекции и

позволяет оперировать непосредственно с информацией, полученной тем или другим способом путем сканирования трехмерной сцены.

Следующим шагом становиться построения алгоритма обработки информации и принятия решений. Роевой интеллект отлично может справиться с этой задачей, так как описывает коллективное поведение децентрализованной самоорганизующейся системы, а также рассматривается в теории искусственного интеллекта как метод оптимизации. Актуальной задачей в этой области является разработка распределенных алгоритмов управления такого рода системами [6]. Проблема заключается в том, что требуется разработать алгоритм решения некоторой глобальной задачи, программируя локальное поведение многих таких спутников, действующих параллельно и взаимодействующих локально друг с другом. Заметим, что в рое частиц, частица представляет потенциальное решение проблемы. Поведение частицы в гиперпространстве поиска решения все время подстраивается в соответствии со своим опытом и опытом своих соседей [7]. Кроме этого, каждая частица помнит свою лучшую позицию с достигнутым локальным лучшим значением целевой функции и знает наилучшую позицию частиц – своих соседей, где достигнут глобальный на текущий момент оптимум. В процессе поиска частицы роя обмениваются информацией о достигнутых лучших результатах и изменяют свои позиции и скорости по определенным правилам на основе имеющейся на текущий момент информации о локальных и глобальных достижениях. При этом глобальный лучший результат известен всем частицам и немедленно корректируется в том случае, когда некоторая частица роя находит лучшую позицию с результатом, превосходящим текущий глобальный оптимум. Каждая частица сохраняет значения координат своей траектории с соответствующими лучшими значениями целевой функции (обозначим Y_i), которая отражает когнитивную компоненту. Аналогично значение глобального оптимума, достигнутого частицами роя, будем обозначать Y'_i, которое отражает социальную компоненту. Таким образом, каждая частица роя подчиняется достаточно простым правилам поведения, которые учитывают локальный успех каждой особи и глобальный оптимум всех особей (или некоторого множества соседей) роя [8].

Каждая i-я частица характеризуется в момент времени t своей позицией $X_i(t)$ в гиперпространстве и скоростью движения $V_i(t)$. Позиция частицы изменяется в соответствии со следующей формулой [9]:

$$X_i(t + 1) = Xi(t) + Vi(t + 1), \quad (1)$$

где $X_i(0)$ соответствует ($X_{\min}$, $X_{\max}$).

Заключение

Дальнейшее исследования и моделирование алгоритма позволит добиться эффективной оптимизации для группового полета микро-спутников. При успешной реализации такого подхода будет доступен огромный список задач, которых можно будет достичь с использованием данной технологией. Моделью динамической системы будет являться набор дифференциальных уравнений, который представляет динамику системы с использованием законов физики.

Использование в такой системе алгоритма Роя дает возможность решить проблему оптимизации, а также повышает надежность системы, так как даже при выводе из строя отдельных спутников система сможет адаптироваться к этому без особых трудностей.

Библиографический список

1. Небылов А. В., Перлюк В. В., Леонтьева Т. С. Исследование технологии взаимной навигации и ориентации малых космических аппаратов в группе // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2019. Т. 18. № 1. С. 88–93.

2. Потюпкин А. Ю., Данилин Н. С., Селиванов А. С. Кластеры малоразмерных космических аппаратов как новый тип космических объектов // Ракетно-космическое приборостроение и информационные системы. 2017. Т. 4. № 4. С. 45–56.

3. Салимжан Касым. Разработка и анализ системы наведения группировки малых космических аппаратов для дистанционного зондирования Земли // Молодой ученый. 2019. № 24 (262). С. 139–140.

4. Nebylov A., Panferov A., Brodsky S., Knyazhsky A. Relative navigation and positioning of nanosatellites in formation // AIRTEC 2017 Congress. Germany. 2018. Vol. 2. Issue 1. 4 p.

5. Panferov A., Nebylov A., Brodsky S. Synthesis of a control system for relative motion of closely spaced satellites // Journal of Aeronautics & Aerospace Engineering, 2017.

6. Sermpinis G., Theofilatos K., Karathanasopoulos A., Georgopoulos E. F., Dunis C. Forecasting foreign exchange rates with adaptive neural networks using radial-basis functions and Particle Swarm Optimization // European Journal of Operational Research.

7. Eberhart R., Kennedy J. A New Optimizer Using Particle Swarm Theory // Sixth International Symposium on Micro Machine and Human Science.

8. Kashan A. H., Karimi B. A discrete particle swarm optimization algorithm for scheduling parallel machines // Computers & Industrial Engineering.

9. Сорокин А. А. Роевой интеллект и групповая робототехника в решении различных задач / А. А. Сорокин, Р. А. Коваленко, Е. А. Яковлева // Технические науки: проблемы и перспективы: материалы VII Междунар. науч. конф. Казань, июль 2020 г. Казань: Молодой ученый, 2020.

ВСТРОЕННЫЕ МИКРОЭЛЕКТРОННЫЕ СИСТЕМЫ

УДК 623.74; 004.89

Е. Ю. Зыбин*
доктор технических наук
В. В. Косьянчук*
доктор технических наук
В. М. Новиков*
начальник сектора
Н. И. Сельвесюк*
доктор технических наук
А. Ю. Чекин*
кандидат технических наук
Д. А. Фофанов**
кандидат технических наук
*Федеральное государственное унитарное предприятие «Государственный научно-исследовательский институт авиационных систем»
**ООО «АРЛИ спецтехника»

АРХИТЕКТУРА ОТКАЗОУСТОЙЧИВОЙ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СЕТИ СКОРОСТНЫХ ВИНТОКРЫЛЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Рассмотрена архитектура отказоустойчивой информационно-измерительной сети скоростных винтокрылых летательных аппаратов. Приведены особенности реализации контура сбора информации на базе оптических систем. Сформулированы принципы интеграции оптической сенсорной сети с бортовой информационной сетью скоростных винтокрылых летательных аппаратов. Предложена архитектура интеррогатора волоконно-оптических датчиков, позволяющая интегрировать сенсорную сеть в комплекс бортового оборудования воздушного судна.
***Ключевые слова*:** интегральная фотоника, радиофотоника, волоконные оптические датчики, полностью оптическая бортовая сеть, системы WDM, интеррогатор, скоростной винтокрылый летательный аппарат, отказоустойчивая информационно-измерительная сеть.

Исследование выполнено за счет гранта Российского научного фонда №22-29-00186, https://rscf.ru/project/22-29-00186.

E. YU. Zybin*
Dr. Sc., Tech.
V. V. Kos'yanchuk*
Dr. Sc., Tech.
V. M. Novikov*
Head of Sector
N. I. Sel'vesyuk*
Dr. Sc., Tech.
A. YU. Chekin*
PhD, Tech.
D. A. Fofanov**
PhD, Tech.

*Federal State Unitary Enterprise State Research Institute of Aviation Systems (GosNIIAS)
**ARLI Spetstechnika LLC

ARCHITECTURE OF A FAULT-TOLERANT INFORMATION-SENSOR NETWORK OF HIGH-SPEED ROTORCRAFT

The architecture of a fault-tolerant information-measuring network of high-speed rotary-wing aircraft is considered. The features of the implementation of the information collection loop based on optical systems are presented. The principles of integration of the optical sensor network with the onboard information network of high-speed rotary-wing aircraft are formulated. The architecture of the interrogator of fiber-optic sensors is proposed, which makes it possible to integrate the sensor network into the complex of on-board equipment of an aircraft.
Keywords: integrated photonics, radio photonics, fiber optic sensors, all-optical on-board network, WDM systems, interrogator, high-speed rotorcraft, fault-tolerant information-sensor network.

Введение

Комплекс бортового оборудования (КБО) скоростных винтокрылых летательных аппаратов (СВЛА) можно охарактеризовать как систему со сложной многоуровневой иерархией, с динамической структурой и возможностью адаптации к изменениям функционирования и различным отказам [1, 2]. Неотъемлемой частью процесса поддержания подобных систем в работоспособном состоянии является непрерывный мониторинг технического состояния отдельных элементов, прогнозирование и предупреждение выхода их из строя [3]. Функционал реализующей на СВЛА системы ранней диагностики отказов (СРДО) базируется на мониторинге состояния систем СВЛА путем непрерывного измерения множества параметров, используемых для дальнейшей диагностики. Для мониторинга технического состояния систем СВЛА могут быть использованы как аппаратные решения, так и аналитические подходы.

Программно-аппаратные средства обеспечения отказоустойчивости реализуют совокупность алгоритмов диагностики систем. Они анализируют значения диагностических параметров воздушных судов (ВС) и формируют прогнозы работоспособности систем ВС, технического состояния ВС с целью предотвращения отказных ситуаций в полете.

Способы обеспечения отказоустойчивости включают в себя следующие этапы:

– непрерывный мониторинг состояния систем и формирование диагностических параметров;

– анализ диагностических параметров и формирование прогноза работоспособности систем и СВЛА в целом;

– выработка решения по устранению прогнозируемых отказов с целью предотвращение развития аварии СВЛА.

Процедуры обеспечения отказоустойчивости осуществляются в автоматическом режиме без непосредственного участия человека. Объектами диагностики на ВС являются:

– бортовое радиоэлектронное электронное оборудование (БРЭО);

– программное обеспечение (ПО) ВС;
– электрические системы;
– пневмо- и гидросистемы;
– двигательные/силовые установки;
– механические системы и т. д.

В работах [5 – 7] были рассмотрены способы обеспечения отказоустойчивости и их программно-аппаратное обеспечение на базе полностью оптической бортовой сети (ПОБС), а в материалах [8, 9] предложены решения по реализации ПОБС и разработаны прототипы программно-аппаратных средств поддержки принятия решения по реконфигурации комплекса бортового оборудования при отказах на базе нейросетевых вычислительных и экспертных системах.

Однако, вопросы архитектуры ПОБС с множеством волоконно-оптических датчиков (ВОД) не рассматривалась, хотя технология интеграции информационно-измерительных сенсорных сетей в бортовую оптическую сеть является важнейшей задачей [7].

В этой связи в данной статье будет рассмотрена архитектура построения отказоустойчивой информационно-сенсорной сети скоростных винтокрылых летательных аппаратов на базе волоконно-оптических датчиков (ВОД). Реализация ВОД на базе волоконно-оптических компонентов имеет целый ряд преимуществ по сравнению с сенсорами на других физических принципах. В число преимуществ входят высокая чувствительность и разрешающая способность, отсутствие потребности в электропитании, нечувствительность к электромагнитным помехам, электро- и пожаробезопасность, отсутствие механических движущихся частей, удобство монтажа и простота обслуживания, а также малые габариты и масса [10]. Вся совокупность ВОД, находящихся на борту ВС, объединяется в единую сенсорную сеть с использованием устройства опроса датчиков – интеррогатора, позволяющего интегрировать сенсорную сеть в комплекс бортового оборудования.

Архитектура отказоустойчивой информационно-сенсорной сети

Основными информационными средствами перспективных СВЛА являются датчики (сенсоры) разнообразных физических величин, таких как деформация, температура, давление, уровень жидкости, скорость потока, положение, вибрация, химический состав, электрические величины (ток, напряжение и др.). При реализации измерителей на базе ВОД измерение физических величин происходит за счет модуляции датчиком параметров излучения: спектрального состава, амплитуды (интенсивности), фазы, поляризации. По физическим эффектам, вызывающим модуляцию параметров излучения при изменении той или иной измеряемой величины, ВОД можно разделить на интерферометрические, решетчатые, а также основанные на эффектах рассеяния Рамана, Рэлея и Бриллюэна.

Интерферометрические ВОД используют эффект изменения фазы оптического излучения в волоконном световоде при механическом или тепловом

воздействии на световод. Изменение фазы световой волны, прошедшей по находящемуся под воздействием световоду, преобразуется в изменение интенсивности за счет интерференции, после чего интенсивность детектируется фотодиодом, через который протекает электрический ток, пропорциональный мощности оптического излучения. При этом используется четыре основных конфигурации интерферометров, схематически показанные на рис. 1.

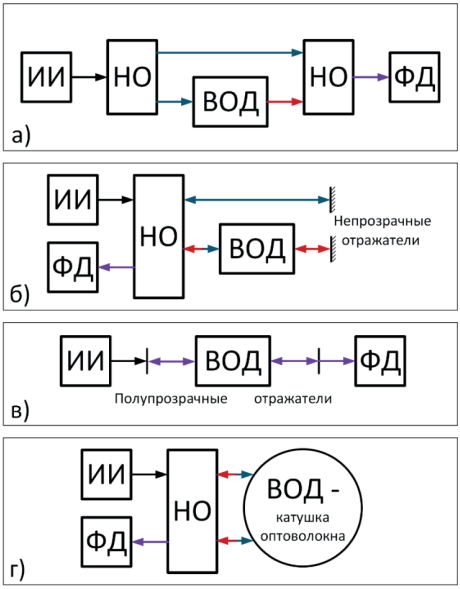


Рис. 1. Конфигурации интерферометров, используемые для получения информации от ВОД: а – Маха-Цандера; б – Майкельсона; в – Фабри-Перо; г – Саньяка. ИИ – источник излучения, НО – направленный ответвитель, ФД – фотодиод

Интерферометрические ВОД обладают крайне высоким разрешением, но одновременное измерение нескольких физических величин с помощью интерферометрических датчиков, размещенных в одном оптическом волокне, приводит к многочисленным техническим и технологическим трудностям. Аналогичным недостатком обладают и ВОД, использующие эффекты рассеяния. В этой связи для построения сенсорной сети ВС наиболее подходящими являются решетчатые ВОД, функционирующие за счет модуляции спектрального состава излучения (оптической фильтрации).

Центральным элементом сенсора с решетчатым ВОД является волоконная брэгговская решетка (ВБР), представляющая собой дифракционную решетку, сформированную за счет периодической модификации показателя преломления сердцевины оптического волокна [11]. Типовые структуры ВБР с различ-

ной конфигурацией профиля показателя преломления, используемые в ВОД, иллюстрируются рис. 2.

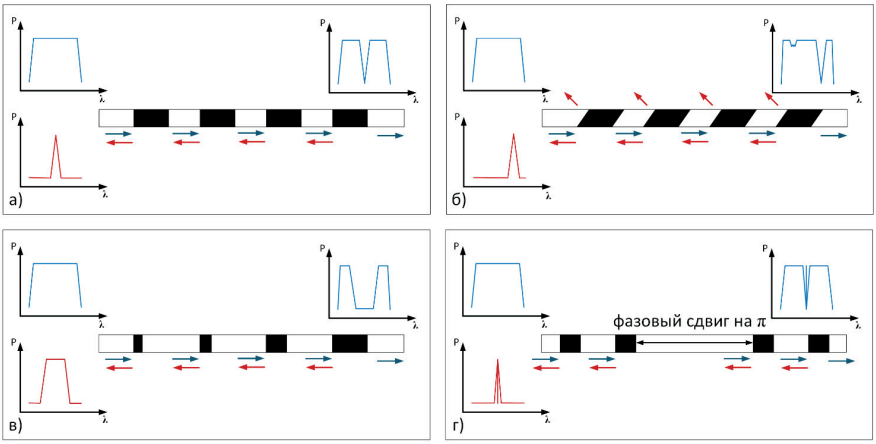


Рис. 2. Типы ВБР, используемых в ВОД и графики спектральной плотности мощности оптического излучения P в зависимости от длины волны λ на входе и выходе ВБР с различными конфигурациями профиля показателя преломления: а – однородный; б – наклонный; в – чирпированный; г – с фазовым сдвигом

Как видно из рис. 2, по отношению к излучению, попадающему на решетку, она играет роль полосового фильтра, спектральные характеристики которого, в первую очередь центральная длина волны пропускания или отражения, связаны функциональной зависимостью с измеряемым параметром среды, окружающей сенсор. ВБР делятся на точечные, квазираспределенные и распределенные. Первые два представляют собой датчики с прямым кодированием «длина волны-измеряемая величина». Последние представляют собой распределенные ВОД и не сильно отличаются от предыдущих двух, поскольку имеют схожую с решетками природу информативного контура. ВБР позволяют измерять практически весь требуемый для ВС перечень физических параметров.

Для измерения спектральных характеристик ВБР необходимо иметь либо широкополосный источник излучения, либо источник излучения с перестраиваемой длиной волны, а также оптический приемник, позволяющий оценить отклик решетки, измерить параметры отклика и пересчитать измеренные параметры в значение измеряемой физической величины. Источник и приемник излучения вместе с вычислителем объединяются в так называемый интеррогатор (опросчик).

Ключевой задачей для сенсорных сетей ВС является одновременное измерение нескольких физических величин с помощью датчиков, размещенных в одном оптическом волокне. Для решения данной задачи необходимо использовать ввод в волокно спектрально уплотненных оптических сигналов состоящий

из нескольких длин волн – λ, т. е. создать WDM-Сенсорную Сеть (WDM-СС). Мультиплексирование множества ВОД ВБР в единой сенсорной сети WDM-СС дает следующие преимущества:

– резервирование;

– мультиплексирование различных датчиков по разным объектам;

– мультиплексирование датчиков по измеряемой физической величине.

С учетом необходимости опроса многочисленных датчиков различных физических величин, из известных способов построения интеррогаторов наиболее перспективным является подход с применением упорядоченной волноводной решетки (AWG), имеющий потенциал для реализации в виде фотонной интегральной схемы [12]. Помимо общих преимуществ волоконно-оптических сенсоров, упомянутых выше, с их помощью удается получить дополнительные возможности, такие как встроенная автокалибровка и простое мультиплексирование нескольких датчиков, последовательно соединенных одним волокном. Эти дополнительные преимущества позволяют внедрять волоконные датчики в материалы для создания так называемых “умных структур”, мониторинг состояния которых возможен в режиме реального времени. Обобщенная схема интеррогатора на базе AWG во взаимодействии с ПОБС представлена на рис. 3. Как видно из рисунка, интеррогатор включает в себя следующие составные части:

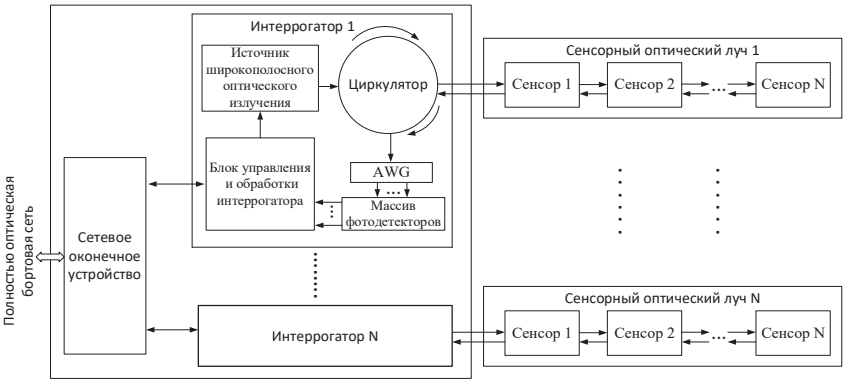


Рис. 3. Структурная схема интеррогатора

– полупроводниковый или волоконный источник оптического излучения, широкополосная работа которого достигается либо за счет усиленной спонтанной эмиссии (оптического шума), либо за счет перестройки по длине волны;

– оптический циркулятор, обеспечивающий разделение потоков излучения, направляемого на датчики, и отраженного излучения, содержащего информацию о физических параметрах;

– массив фотодетекторов, играющий роль спектрально-селективного элемента, позволяющего оценить зависимость мощности излучения от длины волны и извлечь информацию из потока излучения, отраженного от датчиков;

– блок управления и контроля, реализующий задание режимов работы системы под управлением вешних команд, поддержание оптимальных параметров, обработку результатов измерений, контроль технического состояния и взаимодействие с вышестоящим звеном СРДО;

– сетевое оконечное устройство для связи с полностью оптической бортовой сетью.

Отличительной особенностью предлагаемого решения построения интеррогатора является реализация многолучевой сенсорной схемы работы с ВОД. Где каждый сенсорный оптический луч может быт настроен на измерение отдельных физических величин, характеризующих состояние различных систем КБО.

Сенсорные сети как составная часть СРДО, включающие в себя интеррогатор и волоконно-оптические датчики, обеспечивают решение следующих задач:

– непосредственное измерение физических параметров самолетных систем;

– интеллектуальная обработка и передача параметров состояния самолетных систем в СРДО;

– повышение эффективности работы систем управления полетом ВС.

На сегодняшний день количество физических величин, характеризующих состояние ВС и влияющих на качество управления ВС, постоянно растет [13]. Это диктует необходимость создания комплексной измерительной системы, способной осуществлять высокоэффективный сбор, передачу и обработку данных о состоянии физических параметров ВС. В случае использования традиционных электронных измерительных средств это приводит к появлению значительного аддитивного шума вследствие использования длинных линий для передачи относительно слабых электрических сигналов, что снижает помехозащищенность системы. Кроме того, увеличение длины информационных каналов приводит к увеличению массы и стоимости всей измерительной системы в целом.

Для создания распределенной сенсорной сети ВС более всего подходят элементы волоконно-оптической системы обработки и передачи информации, которые позволяют увеличить скорость передачи данных до 10 Гбит/с, расширить полосу пропускания передаваемых сигналов до 10 Гбит/с, уменьшить потери для канализуемого излучения до уровня менее 0,2 дБ/км, обеспечить максимальную скорость ввода данных в электронную систему обработки и хранения информации. Данные оптические элементы имеют малые габариты, компактность, высокую помехозащищенность.

При включении интеррогатора в состав бортовой сети он выполняет функции:

– сетевого оконечного устройства ПОБС;

– блока управления ВОСС (волоконная оптическая сенсорная сеть)
– выдачи исходного оптического сигнала в ВОД;
– прием и преобразования оптического сигнала с ВОД;
– приема\передачи полученных от ВОД данных по единой бортовой сети.

Несмотря на то, что оптико-электронные интеррогаторы имеют определенные ограничения по разрешению и скорости интеррогации, а также трудности одновременного комплексированного измерения нескольких измеряемых величин, применение предложенного подхода позволяет создать высокоинформативную интегрированную бортовую оптическую сенсорную сеть на базе ПОБС, обеспечивающую отказоустойчивость сети и ее глубокую диагностику.

В результате проведенных исследований предложена архитектура отказоустойчивой информационно-сенсорной сети СВЛА, объединяющая два типа сетей ПОБС и WDM-СС, в результате чего образуется единое информационное пространство – бортовая информационная вычислительная среда, позволяющая осуществлять контроль и обеспечивать отказоустойчивость бортовых систем, построенных на различных принципах и использующих различные физические принципы измерений.

Библиографический список

1. Зыбин Е. Ю., Косьянчук В. В. Эволюция архитектуры комплекса бортового оборудования воздушных судов // IV Юбилейная Всероссийская научно-техническая конференция «Авиационные системы в XXI веке», посвященная 70-летию со дня создания ФГУП «ГосНИИАС»: сб. тезисов. 26–27 мая 2016 г. Москва. С. 198.

2. Желтов С. Ю., Косьянчук В. В., Зыбин Е. Ю. Перспективы развития комплексов бортового оборудования воздушных судов гражданской авиации // Гражданская авиация на современном этапе развития науки, техники и общества: сб. тезисов докладов Международной научно-технической конференции, посвященной 95-летию Гражданской авиации. 16–17 мая 2018 г. М.: Московский гос. технический ун-т гражданской авиации, 2018. С. 5–6.

3. Косьянчук В. В., Зыбин Е. Ю., Карпенко С. С., Бондаренко Ю. В. Резервированная интегрированная система мониторинга технического состояния воздушного судна // Девятый Международный Аэрокосмический Конгресс IAC18: тезисы докладов. 2018. С. 119–121.

4. Волоконнооптические датчики. Вводный курс для инженеров и научных работников / Под ред. Эрика Удда. М.: ТЕХНОСФЕРА, 2008.

5. Новиков В. М. Концепция применения полностью оптических бортовых сетей при решении задач динамической реконфигурации бортовой информационно-вычислительной среды на базе РМЭ // Сборник научных статей по материалам пятой Всероссийской научно-практической конференции. Воронеж: ВУНЦ ВВС «ВВА», 2017. С. 211–219.

6. Новиков В. М. Полностью оптическая бортовая сеть как средство построения бортового комплекса на принципах распределенной модульной электроники и технологии фотонных интегральных схем // V Международная науч-

но-практическая конференция «Перспективные направления развития бортового оборудования гражданских воздушных судов» М.: Типография ФГУП «ГосНИИАС», 2019. С. 51–56.

7. Новиков В. М. Решение задач интеллектуальной поддержки экипажа в части реконфигурации КБО при отказах // Актуальные вопросы исследований в авионике. Теория, обслуживание, разработки: сб. тезисов докладов VI Международной научно-практической конференции «АВИАТОР». 14–15 февраля 2019 года. Воронеж. 2019. С. 189–191.

8. Патент на изобретение № 2694137. Система передачи информации в реальном времени на базе полностью оптической спектрально-уплотненной бортовой сети реального времени. 2019.

9. Патент на изобретение № 2744517. Двухконтурная система передачи информации в реальном времени на базе полностью оптической спектрально-уплотненной бортовой сети.

10. Нуреев И. И. Радиофотонные амплитудно-фазовые методы интеррогации комплексированных датчиков на основе волоконных решеток Брэгга // Инженерный вестник Дона. 2016. № 2.

11. Васильев С. А., Медведков О. И., Королев И. Г., Божков А. С., Курков А. С., Дианов Е. М. Волоконные решетки показателя преломления и их применения // Квантовая электроника. 2005. 35:12, 1085–1103.

12. Marin Y. E., Nannipieri T., Oton C. J., Pasquale F. D. Current Status and Future Trends of Photonic-Integrated FBG Interrogators // Journal of Lightwave Technology. Vol. 36. No. 4. P. 946–953.

13. Зыбин Е. Ю., Косьянчук В. В., Сельвесюк Н. И. Отказоустойчивая архитектура комплексных систем управления перспективных самолетов транспортной категории на базе единой вычислительной платформы // Третья Всероссийская научно-техническая конференция «Навигация, наведение и управление летательными аппаратами»: тезисы докладов. М.: Научтехлитиздат, 2017. С. 227–229.

УДК 004.7; 004.9

Е. А. Суворова*
кандидат технических наук, доцент
*Санкт-Петербургский государственный университет аэрокосмического приборостроения

ПОДХОД, ОБЕСПЕЧИВАЮЩИЙ ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ КОЛИЧЕСТВОМ ПОДДЕРЖИВАЕМЫХ НЕЗАВИСИМЫХ ПОТОКОВ ДАННЫХ В ЗВЕНЕ ПЕРЕДАЧИ ДАННЫХ ДЛЯ СТАНДАРТА SPACEFIBRE

В данной статье предлагается подход, обеспечивающий возможность динамического управления количеством независимых потоков данных для стандарта *SpaceFibre*. Он ориентирован и на устранение ограничений по количеству поддерживаемых потоков данных на уровне спецификации стандарта, и на устранение ограничений, связанных с особенностями конкретных реализаций. Данный подход основан на динамическом перераспределении ресурсов между потоками данных. Он ориентирован на реализацию в ASIC.
Ключевые слова: *SpaceFibre*, управление потоком в звене передачи данных, качество сервиса передачи данных, динамическая реконфигурация, системы аэрокосмического назначения.

E. A. Suvorova*
PhD, Tech., Associate Professor
*St. Petersburg State University of Aerospace Instrumentation

THE APPROACH FOR DYNAMIC CONTROL OF THE NUMBER OF SUPPORTED INDEPENDENT DATA STREAMS IN THE DATA LINK FOR THE SPACEFIBRE STANDARD

This article proposes an approach that provides the ability to dynamically control the number of independent data streams for the SpaceFibre standard. It is oriented both to the elimination of restrictions on the number of supported data streams at the standard specification level, and to the elimination of restrictions associated with the features of specific implementations. This approach is based on the dynamic redistribution of resources between data streams. It is focused on ASIC implementation.
Keywords: SpaceFibre, data link flow control, QoS, dynamic reconfiguration, aerospace systems.

Введение

Количество независимых потоков данных, для которых необходимо обеспечивать различные механизмы качества сервиса (QoS) может очень существенно различаться в различных сетях аэрокосмического назначения. Поддерживаемое количество независимых потоков данных определяется выбором стандарта передачи данных с одной стороны (в большинстве современных стандартов максимальное количество потоков данных ограничено на уровне кодировок формата передаваемых пакетов/фреймов) и особенностями конкретных реализаций сетевого оборудования (маршрутизаторов и сетевых контроллеров терминальных узлов с другой стороны). В реализациях электронной компонентной базы (ЭКБ) ограничения на количество поддерживаемых потоков

данных, связаны с допустимыми аппаратными затратами, прежде всего, с размерами необходимого буферного пространства. При этом нередко большая часть буферного пространства простаивает в различных режимах функционирования устройств. Потенциально увеличить количество поддерживаемых потоков данных без увеличения аппаратных затрат можно за счет динамического перераспределения ресурсов между потоками данных (динамической реконфигурации). Однако эта возможность зачастую блокируется спецификой используемых стандартов. Кроме того, для реализаций оборудования аэрокосмического назначения, как правило, используется технология ASIC, которая исходно не предоставляет возможностей по динамической реконфигурации, в отличие от технологии FPGA. Использование же технологии FPGA очень ограничено в связи с тем, что эта технология существенно проигрывает технологии ASIC по быстродействию, площади, энергопотреблению, устойчивости к внешним воздействиям.

Современные сети аэрокосмического назначения могут очень существенно отличатся друг от друга по своей структурной организации, решаемым прикладным задачам. На разных этапах функционирования одной и той же системы могут выполняться разные задачи [3, 6]. Из-за этого количество и характеристики передаваемых между вычислительными узлами (терминальными узлами) потоков данных может очень существенно варьироваться от системы к системе и меняться в ходе функционирования одной системы. Соответственно, сетевое оборудование (маршрутизаторы и сетевые контроллеры терминальных узлов) должны обеспечивать передачу, маршрутизацию меняющихся наборов потоков данных с меняющимися характеристиками, обеспечивать для них требуемое качество сервиса (QoS). Реализация многих механизмов QoS, таких как гарантированная доставка данных, гарантированное время доставки данных связано с большими накладными расходами (аппаратными затратами). В значительной степени они связаны с необходимостью иметь довольно большие объемы памяти для промежуточного хранения принимаемых пакетов, фреймов данных [2]. Причем для разных потоков данных и на разных этапах функционирования системы может требоваться разное количество буферной памяти в зависимости от их характеристик (в частности, интенсивности) и требуемого QoS. Если ресурсы, в частности, ресурсы памяти, для каждого потока выделяются статически, это может существенно ограничить количество поддерживаемых потоков данных в маршрутизаторах и терминальных узлах. При этом довольно большая часть ресурсов может простаивать в течении длительного времени (использоваться не рационально).

Если для реализации ЭКБ используются FPGA, то их возможности по реконфигурации, в том числе и динамической, могут использоваться для перераспределения ресурсов между потоками. Однако, возможности использования FPGA по сравнению с ASIC для ЭКБ аэрокосмического назначения очень ограничены из-за того, что FPGA имеют существенно более высокое энергопотребление, меньшую степень интеграции, меньшее быстродействие, худшую устойчивость к внешним воздействиям [2].

Производство ЭКБ по технологии ASIC является экономически оправданным только в случае средних и крупных серий. Соответственно маршрутизаторы и терминальные узлы должны быть достаточно универсальными, для того, чтобы они могли использоваться в различных бортовых сетях. Должна существовать возможность динамически адаптировать их характеристики к изменениям наборов задач, решаемых в системе.

Возможности по динамической адаптации характеристик зависят как от особенностей реализации маршрутизаторов, терминальных узлов так и от особенностей используемого стандарта передачи данных.

В данной статье мы рассмотрим возможности по динамическому изменению количества независимо обрабатываемых потоков данных при использовании стандарта *SpaceFibre* [1]. Данный стандарт является современным стандартом, разработанным для бортовых сетей аэрокосмического назначения.

Механизмы обеспечения качества сервиса в стандарте SpaceFibre

В стандарте *SpaceFibre* возможность независимой обработки потоков данных, возможность поддерживать для каждого потока данных свои параметры QoS поддерживается в звене передачи данных и на сетевом уровне [1]. Для этого используется механизм виртуальных каналов и виртуальных сетей. В звене передачи данных может поддерживаться до 32 виртуальных каналов. Для каждого виртуального канала может быть задан уровень приоритета, доля пропускной способности физического канала и/или расписание (набор таймслотов, в которые разрешена передача данных). Для каждого виртуального канала используется отдельный механизм управления потоком, позволяющий исключить потерю принимаемых данных из-за переполнения буфера на приемной стороне. Для управления потоком используется механизм кредитования от приемника. Приемная сторона отправляет передающей стороне информацию о количестве свободного места в буфере – количестве «кредитов». Передающая сторона может отправлять приемной стороне количество данных в рамках полученного количества кредитов. На уровне звена передачи данных передача потока данных осуществляется в терминах фреймов. Максимальный размер фрейма (в отличие от максимального размера пакета) является фиксированным. Виртуальные каналы используют физический канал в режиме разделения времени. В физическом канале могут чередоваться фреймы, передаваемые от разных виртуальных каналов. Порядок передачи фреймов определяется параметрами QoS, заданными для виртуальных каналов и наличием кредитов.

В звене передачи данных реализован также механизм, обеспечивающий гарантированную доставку данных. Каждый фрейм снабжается порядковым номером и контрольной суммой. Контрольная сумма позволяет выявлять ошибки (искажения данных), которые могут возникать при передаче фреймов, а порядковые номера позволяют выявлять потерю (искажение) целых фреймов. Приемная сторона информирует передающую о возникающих ошибках. В этом случае выполняется повторная передача фреймов. Эти механизмы обеспечива-

ют возможность независимой передачи потоков данных по разным виртуальным каналам.

В стандарте *SpaceFibre* максимальное количество потоков данных, независимо обрабатываемых в звене передачи данных ограничено 32. Это количество зафиксировано в используемом формате фреймов. В заголовке фрейма данных и служебного фрейма, используемого для кредитования, под идентификатор (номер) потока отведено 5 битов [1].

В конкретных реализациях количество поддерживаемых виртуальных каналов может быть меньше 32. Для большинства современных реализаций оно не превосходит 8–12. Это ограничение обусловлено, прежде всего, достаточно большим объемом буферного пространства, необходимого для каждого виртуального канала, для реализации механизмов QoS (прежде всего, механизма управления потоком на базе кредитования). В [4, 5] нами было показано, что для того, чтобы исключить простои при передаче длинных пакетов (пакетов, длина которых в несколько раз превосходит максимальный размер фрейма) из-за отсутствия кредитов, буфер виртуального канала на приемной стороне должен вмещать не менее трех фреймов максимального размера (размер поля данных равен 256 байтов). Необходимо отметить, что приемный буфер виртуального канала будет задействован полностью только в том случае, если данный вириальный канал использует все ресурсы физического канала в течении достаточно продолжительного времени. Десятки фреймов передаются подряд (без передачи фреймов из других виртуальных каналов). Если в канале осуществляется чередование фреймов, относящихся к разным виртуальным каналам, то приемные буферы этих каналов большую часть времени будут использоваться лишь частично. Если, например, для виртуального канала разрешена передача данных только в одном таймслоте, то в остальных 63 таймслотах эпохи (продолжительность эпохи в стандарте *SpaceFibre* составляет 64 таймслота) буферное пространство этого виртуального канала будет простаивать.

Предлагаемый механизм

Мы предлагаем подход, позволяющий увеличить количество независимых потоков данных в звене передачи данных. В рамках данного подхода один виртуальный канал *SpaceFibre* может быть использован для передачи нескольких потоков данных. Фактически в звене передачи данных может быть реализован один виртуальный канал *SpaceFibre*, в рамках которого может передавать некоторое количество потоков данных.

В этом подходе используется двухуровневая система кредитования. На нижнем уровне используется система кредитования *SpaceFibre*. Для ее реализации достаточно буфера размером 3 фрейма [4, 5]. Данная система кредитования предназначена для исключения простоев канала, связанных с задержками при передаче кредитов.

Этот буфер используется для приема фреймов, относящихся к разным потокам данных. Для того, чтобы обеспечить независимость передачи данных, относящихся к разным потокам, необходимо обеспечить, чтобы данные, посту-

пающие в буфер виртуального канала, извлекались из него со скоростью не меньшей скорости их поступления. Это обеспечивается за счет верхнего уровня кредитования. На этом уровне осуществляется независимое кредитование для каждого потока данных. В отличие от базовой версии стандарта *SpaceFibre* на этом уровне используется переменный формат заголовков фреймов. Это обеспечивает возможность изменения разрядности полей, используемых для идентификации потока данных в соответствии с количеством потоков данных, которое необходимо поддерживать в звене передачи данных. Для обработки таких заголовков на приемной и передающей стороне может быть использован автомат с поддержкой динамической реконфигурации. По выполненным нами оценкам аппаратные затраты на реализацию такого автомата (на обработку заголовков фреймов второго уровня с переменным форматом) очень невелики. Они не превосходят 7–9% от площади буферного пространства, необходимого для размещения одного фрейма данных. На втором уровне используется физически единое буферное пространство для всех потоков данных. На логическом уровне оно разделено на сегменты. Размер одного сегмента соответствует размеру фрейма данных максимального размера. Каждый такой логический сегмент потенциально может быть использован для любого потока данных. В разные моменты времени он может использоваться для разных потоков данных. Механизмы кредитования (автоматы, в которых они реализованы) для отдельных потоков данных функционируют в зависимости от контекста, от режима (текущей конфигурации). Количество буферного пространства, которое может быть задействовано каждым потоком данных, зависит от параметров QoS, определенных для данного потока. Например, если используется расписание, то для каждого потока кредиты могут выдаваться только в тех таймслотах, в которых для него разрешена передача данных. Это позволяет сократить простои буферного пространства.

Заключение

В статье рассмотрены причины ограничений на количество независимых потоков данных, которые могут поддерживаться в одном звене передачи данных в соответствии со стандартом *SpaceFibre*.

В статье предложен подход, позволяющий увеличить количество поддерживаемых независимых потоков данных без увеличения количества буферного пространства, т. е. без сколько-нибудь значительного увеличения аппаратных затрат, сократить простои (неиспользование) отдельных частей буферного пространства.

В дальнейшем планируется оценить влияние различных стратегий распределения буерного пространства между потоками на характеристики системы.

Библиографический список

1. SpaceFibre – Very high-speed serial link. ECSS-E-ST-50-11C // ESA-ESTEC. Noordwijk, The Netherlands. 2019. 233 p.

2. International Roadmap for Devices and Systems (IRDS). 2021 Edition, 2021.

3. Khakhulin A., Orlovsky I., Sheynin Y. [et al.] Real Time Video Data Transmission in SpaceFibre Networks with the ESDP Transport Protocol // SpaceWire Conference, 2016.

4. Suvorova E. A. An Approach for Estimation of Packet Delivery Time on SpaceFibre Networks // Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2020.

5. Суворова Е. А. Оценка минимального времени доставки пакетов в виртуальных сетях SpaceFibre // Научная сессия. ГУАП. 2020. С. 26.

6. Zulkifli N. Development of small scale cluster computer for numerical analysis / N. Zulkifli, A. Sapit, A. N. Mohammed // CFDRI 2017, IOP Conf. Series: Materials Science and Engineering 243. 2017. 6 p.

СОДЕРЖАНИЕ

ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Бурлакова В. А. ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ВНУТРЕННЕЙ СТУПЕНИ КАСКАДНОЙ СХЕМЫ КОДИРОВАНИЯ ДЛЯ МНОГОУРОВНЕВОЙ ФЛЭШ-ПАМЯТИ 4

Волков В. Ю. ОБНАРУЖЕНИЕ И СЕЛЕКЦИЯ КОМПАКТНЫХ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ 11

Ерышов В. Г., Ильина Д. В. МАРКОВСКАЯ МОДЕЛЬ ПРОЦЕССА КОМПЬЮТЕРНОЙ РАЗВЕДКИ, ОСУЩЕСТВЛЯЮЩЕЙ НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП И ПОЛУЧЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ИЗ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНИЗАЦИЙ 17

Исаева М. Н., Овчинников А. А. ОБ ОДНОМ МЕТОДЕ ПОСТРОЕНИЯ КОДОВОЙ СИСТЕМЫ НА ОСНОВЕ КВАЗИЦИКЛИЧЕСКИХ КОДОВ 22

Коломойцев В. С., Баглаенко Е. Ю. СПОСОБЫ РАСПРОСТРАНЕНИЯ СЕТЕВЫХ ЧЕРВЕЙ И ПОСЛЕДСТВИЯ ДЛЯ СИСТЕМ, ЗАРАЖЕННЫХ ИМИ 28

Коломойцев В. С., Верхонина В. О. ОСОБЕННОСТИ ПОСТРОЕНИЯ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ ДЛЯ МЕССЕНДЖЕРОВ 33

Коломойцев В. С., Гринченко С. Р. СРАВНЕНИЕ АЛГОРИТМОВ ГЕНЕРАЦИИ ПРОСТЫХ ЧИСЕЛ И ПРЕДЛОЖЕНИЯ ПО ИХ УЛУЧШЕНИЮ 38

Коломойцев В. С., Грузденков Г. А. МЕТОД МНОГОУРОВНЕВОГО ДОСТУПА К ДОКУМЕНТАМ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 44

Коломойцев В. С., Ерышов Н. В. МЕТОД ОЦЕНКИ РИСКОВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ГОСТ Р 59339-2021 50

Коломойцев В. С., Калинина Е. А. ПРОТОКОЛЫ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ СООБЩЕНИЙ 56

Куров О. Ю., Исаева М. Н. СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ В ЗАГОЛОВКАХ TCP ПАКЕТОВ 61

Летуновская П. С., Шром Б. С., Пойманова Е. Д., Татарникова Т. М. МАШИННОЕ ОБУЧЕНИЕ В ВОПРОСЕ РАСПРЕДЕЛЕНИЯ ФАЙЛОВ ПО УРОВНЯМ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ 66

Овчинников А. А., Вересова А. М. СРАВНЕНИЕ ВЕРОЯТНОСТИ ОШИБКИ ДЕКОДИРОВАНИЯ КОДОВ РИДА – СОЛОМОНА И НИЗКОПЛОТНОСТНЫХ КОДОВ В КАНАЛЕ ГИЛБЕРТА – ЭЛЛИОТА 71

Овчинников А. А., Фоминых А. А. ДВУХСТУПЕНЧАТОЕ ДЕКОДИРОВАНИЕ НА ОСНОВЕ ИТЕРАТИВНОГО И СФЕРИЧЕСКОГО ПОДХОДОВ 76

Пастухова Е. В., Романова Ю. С. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ИССЛЕДОВАНИЯ В ЭПОХУ BIG DATA 81

Попов И. Д. О ПРИМЕНЕНИИ МЕТОДА НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ В MATLAB ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ НАБОРА ДАННЫХ KYOTO 2006 86

Попов И. Д. О РАЗМЕРНОСТИ ДАННЫХ KYOTO 2006 ПРИ ИСПОЛЬЗОВАНИИ МЕТОДА НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ 91

Савельева Д. Д., Татарникова Т. М. О СИСТЕМЕ КОНТРОЛЯ ЗА РАСХОДОМ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ 95

Сайганова Е. В. ЗАЩИТА ИНФОРМАЦИИ ОТНОСИТЕЛЬНО СОВРЕМЕННЫХ РЕАЛИЙ В ПРОЦЕССЕ СУДОРЕМОНТА 99

Сверликов А. В., Татарникова Т. М. МЕТОДИКА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ ПАТТЕРНОВ ПОВЕДЕНИЯ УМНЫХ УСТРОЙСТВ 104

Трофимов А. Н., Таубин Ф. А. АНАЛИЗ КАСКАДНОГО КОДИРОВАНИЯ ДЛЯ МНОГОУРОВНЕВОЙ ФЛЭШ-ПАМЯТИ С ИСПОЛЬЗОВАНИЕМ СМЕШАННОЙ NORMAL-LAPLACE МОДЕЛИ 109

Трофимов А. Н., Таубин Ф. А. ВЫЧИСЛЕНИЕ АДДИТИВНОЙ ГРАНИЦЫ ВЕРОЯТНОСТИ ОШИБКИ ДЕКОДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ ДЛЯ КАНАЛОВ С ПАМЯТЬЮ 114

Фомичева С. Г. ОПЕРАТОРЫ ТОФФОЛИ В АРИФМЕТИЧЕСКИХ ОПЕРАЦИЯХ С МНОГОРАЗРЯДНЫМИ КВАНТОВЫМИ РЕГИСТРАМИ 120

Фомичева С. Г. СИМУЛЯЦИЯ СОСТОЯНИЙ ЗАПУТАННОСТИ В КВАНТОВЫХ РЕГИСТРАХ 125

Шепета Д. А., Боженко В. В., Долгов Е. Н. АЛГОРИТМ МОДЕЛИРОВАНИЯ КОРРЕЛИРОВАННЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, РАСПРЕДЕЛЕННЫХ ПО ЗАКОНУ ВЕЙБУЛЛА 130

Шепета Д. А., Исаков В. И., Тюринова В. А. ПРЯМОЙ МЕТОД МОДЕЛИРОВАНИЯ ЛОГАРИФМИЧЕСКИ-НОРМАЛЬНОГО РАСПРЕДЕЛЕНИЯ 135

Щеголева А. А., Поляк М. Д. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ДИНАМИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ЛОТКИ-ВОЛЬТЕРРЫ С ВНУТРЕННЕЙ КОНКУРЕНЦИЕЙ 140

Юмашева Е. С. АРХИТЕКТУРА АГЕНТОВ, КАК СПОСОБ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ 146

Ястребов М. Ю., Ястребова А. Д. ОЦЕНКА ИРРЕГУЛЯРНОСТИ ХЕШ-КОДОВ 151

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

Анисимов Г. Ю., Семенюк К. А., Назаренко П. А. АЛГОРИТМЫ ДЕТЕКТИРОВАНИЯ ОСОБЫХ ТОЧЕК ИЗОБРАЖЕНИЯ ORB, BRISK, AKAZE В РАБОТЕ ТЕХНИЧЕСКОГО ЗРЕНИЯ БАС 155

Добровольская А. А., Майоров Н. Н., Язвенко М. Р. ИССЛЕДОВАНИЕ ВАРИАНТОВ МОДЕРНИЗАЦИИ ИНФРАСТРУКТУРЫ ТРАНСПОРТНОГО ТЕРМИНАЛА НА ОСНОВЕ ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ 162

Епифанцев К. В., Шишкова М. М. АСПЕКТЫ РАЗРАБОТКИ ВИРТУАЛЬНОГО ВОЛЬТМЕТРА НА БАЗЕ МИКРОКОНТРОЛЛЕРА ATMEGA 8 ... 171

Изотов О. А., Кузнецов А. Л. МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ В СИСТЕМЕ ТРАНСПОРТИРОВКИ СБОРНЫХ ГРУЗОВ 179

Костин А. С., Силин Ю. А., Бахмутская А. В. РАЗРАБОТКА ИЗОТЕРМИЧЕСКОГО КОНТЕЙНЕРА ДЛЯ РЕАЛИЗАЦИИ ДОСТАВКИ СПЕЦИАЛЬНЫХ ГРУЗОВ ПРИ ПОМОЩИ БЕСПИЛОТНОЙ АВИАЦИОННОЙ СИСТЕМЫ 187

Костин А. С., Силин Ю. А. ОСОБЕННОСТИ ДОСТАВКИ СПЕЦИАЛЬНЫХ ГРУЗОВ В ИЗОТЕРМИЧЕСКОМ КОНТЕЙНЕРЕ ПРИ ПОМОЩИ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ 195

Менухова Т. А., Сумманен А. В., Сивов А. А. ОПТИМИЗАЦИЯ ТРАНСПОРТНО-ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ПРИ ЭКСПЛУАТАЦИИ ЭКСКАВАТОРНО-АВТОМОБИЛЬНЫХ КОМПЛЕКСОВ 203

Назаренко П. А., Попок П. В., Аблязов Д. А. АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ БАС В АРКТИЧЕСКИХ УСЛОВИЯХ 208

Назаренко П. А., Попок П. В., Аблязов Д. А. ИССЛЕДОВАНИЕ РАБОТЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ЭКВАТОРИАЛЬНОЙ ЗОНЕ 213

Назаренко П. А., Семенюк К. А., Анисимов Г. Ю. АНАЛИЗ РАБОТЫ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ЭКСТРЕМАЛЬНО ВЫСОКИХ ТЕМПЕРАТУР И ВНЕШНИХ ЗАГРЯЗНЕНИЙ 218

Назаренко П. А., Семенюк К. А., Анисимов Г. Ю. МОДУЛЬ ЗАЩИТЫ АККУМУЛЯТОРНОЙ БАТАРЕИ ДЛЯ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ ПРИ ОТРИЦАТЕЛЬНЫХ ТЕМПЕРАТУРАХ 222

Перлюк В. В., Масталиева В. А., Епринцев М. А. СИСТЕМА КОНТРОЛЯ УТЕЧЕК И ЗОН НЕСАНКЦИОНИРОВАННОГО ОТБОРА ПРИРОДНЫХ ЭНЕРГОНОСИТЕЛЕЙ В ТРУБОПРОВОДАХ..... 228

Пономарев В. К., Буласова В. Г. РЕАЛИЗАЦИЯ ТИПОВЫХ ТРАЕКТОРИЙ ПОЛЕТА ВОЗДУШНОГО СУДНА В СИСТЕМЕ ЗОНАЛЬНОЙ НАВИГАЦИИ 236

Скорина С. Ф. МОДЕЛЬ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНТЕЛЛЕКТУАЛЬНОГО ТРАНСПОРТНОГО СРЕДСТВА ДЛЯ ПРОТИВООБЛЕДЕНИТЕЛЬНОЙ ОБРАБОТКИ САМОЛЕТОВ..... 245

Тимошек Е. С., Маликова Т. Е., Радочинская А. Ж. МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЫГРУЗКИ СУДНА НА РЕЙДЕ С ИСПОЛЬЗОВАНИЕМ ВСПОМОГАТЕЛЬНОГО ФЛОТА 250

Федоринов А. Ю., Перлюк В. В. РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ МАЛЫХ КОСМИЧЕСКИХ АППАРАТОВ В ГРУППЕ НА ОСНОВЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ РОЕВОГО ИНТЕЛЛЕКТА..... 256

ВСТРОЕННЫЕ МИКРОЭЛЕКТРОННЫЕ СИСТЕМЫ

Зыбин Е. Ю., Косьянчук В. В., Новиков В. М., Сельвесюк Н. И., Чекин А. Ю., Фофанов Д. А. АРХИТЕКТУРА ОТКАЗОУСТОЙЧИВОЙ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СЕТИ СКОРОСТНЫХ ВИНТОКРЫЛЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ 261

Суворова Е. А. ПОДХОД, ОБЕСПЕЧИВАЮЩИЙ ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ КОЛИЧЕСТВОМ ПОДДЕРЖИВАЕМЫХ НЕЗАВИСИМЫХ ПОТОКОВ ДАННЫХ В ЗВЕНЕ ПЕРЕДАЧИ ДАННЫХ ДЛЯ СТАНДАРТА SPACEFIBRE..... 270

Научное издание

XXV Международная научная конференция

ВОЛНОВАЯ ЭЛЕКТРОНИКА И ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ

Сборник статей

Часть 3

ISBN: 978-5-8088-1715-9

9 785808 817159

Ответственный за выпуск
В. И. Казаков

Редакторская подготовка *Е. В. Лазаревой*
Компьютерная верстка *А. Н. Колешко*

Подписано к печати 17.05.2022. Дата выхода в свет 27.05.2022. Формат 60×84 1/16.
Усл. печ. л. 16,3. Уч.-изд. л. 17,5. Тираж 150 экз. Заказ № 189.

Редакционно-издательский центр ГУАП
190000, Санкт-Петербург, Б. Морская ул., 67, лит. А

Распространяется бесплатно