ПРИКАСПИЙСКИЙ ЖУРНАЛ

УПРАВЛЕНИЕ И ВЫСОКИЕ ТЕХНОЛОГИИ

2022
№4 (60)

ISSN 2074-1707

16+

ISSN 2074-1707

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ В. Н. ТАТИЩЕВА

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 4 (60)

Журнал включен в перечень рецензируемых научных изданий, рекомендованных ВАК России для публикации основных научных результатов диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям.

Группа специальностей 1.2 «Компьютерные науки и информатика»:

1.2.2 – Математическое моделирование, численные методы и комплексы программ (технические науки).

Группа специальностей 2.2 «Электроника, фотоника, приборостроение и связь»:

2.2.4 – Приборы и методы измерения (по видам измерений) (технические науки);

2.2.11 – Информационно-измерительные и управляющие системы (технические науки);

2.2.12 – Приборы, системы и изделия медицинского назначения (технические науки).

Группа специальностей 2.3 «Информационные технологии и телекоммуникации»:

2.3.1 – Системный анализ, управление и обработка информации (технические науки);

2.3.4 – Управление в организационных системах (технические науки);

2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (технические науки);

2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки).

Журнал входит в базу данных Ulrich’s Periodicals Directory.

Астрахань
Астраханский государственный университет имени В. Н. Татищева
2022

ББК 30
П75

Рекомендовано к печати редакционно-издательским советом
Астраханского государственного университета имени В. Н. Татищева

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 4 (60)

Журнал выходит 4 раза в год
Все материалы, поступающие в редколлегию журнала,
проходят независимое рецензирование

ISSN 2074-1707

ASTRAKHAN STATE UNIVERSITY
NAMED AFTER V. N. TATISHCHEV

PRIKASPIYSKIY ZHURNAL:
Upravlenie i Vysokie Tekhnologii

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2022
No. 4 (60)

The journal is included in the list of the reviewed scientific journals recommended by VAK of Russia for the publication of the main scientific results of theses for the candidate of science degree, for the doctor of science degree on the following scientific specialties.

Group of specialties 1.2 "Computer science and informatics":

1.2.2 – Mathematical modelling, numerical methods and complexes of programms (technical sciences).

Group of specialties 2.2 "Electronics, photonics, instrument engineering and communication":

2.2.4 – Instruments and methods of measurement (by type of measurement) (technical sciences);

2.2.11 – Information-measuring and control systems (technical sciences);

2.2.12 – Medical devices, systems and products (technical sciences).

Group of specialties 2.3 "Information technologies and telecommunications":

2.3.1 – System analysis, information control and processing (technical sciences);

2.3.4 – Management in organizational systems (technical sciences);

2.3.5 – Mathematical software and software for computing systems, complexes and computer networks (technical sciences);

2.3.6 – Information security methods and systems, information security (technical sciences).

The journal is included into the database Ulrich's Periodicals Directory.

Astrakhan
Astrakhan State University named after V. N. Tatishchev
2022

Recommended by the Editorial and Publishing Board
of Astrakhan State University named after V.N. Tatishchev

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2022
No. 4 (60)

The journal is published four times a year
All materials that come to the Editorial Board of the journal
are subject to independent peer-review

СОДЕРЖАНИЕ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

УПРАВЛЕНИЕ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

CONTENTS

INSTRUMENT ENGINEERING, MEASUREMENT SCIENCE, INFORMATION AND MEASURING DEVICES AND SYSTEMS

INFORMATION-MEASURING AND CONTROL SYSTEMS

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

DOI 10.54398/20741707_2022_4_9
УДК 004.421.2

ВЕКТОРИЗАЦИЯ И РАСПАРАЛЛЕЛИВАНИЕ ПОЛНОСЛОВОВОГО ДЛИННОГО СЛОЖЕНИЯ

Статья поступила в редакцию 10.09.2022, в окончательном варианте – 29.09.2022.

Чусов Андрей Александрович, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
кандидат технических наук, доцент департамента электроники, телекоммуникации и приборостроения Политехнического института, ORCID: 0000-0002-7931-5368, e-mail: chusov.aa@dvfu.ru
Лычев Михаил Станиславович, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
студент, ORCID: 0000-0001-9120-5463, e-mail: lychev.ms@ students.dvfu.ru
Гайда Максим Алексеевич, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
студент, ORCID: 0000-0003-3362-5253, e-mail: gayda_m@mail.ru

В статье предложены алгоритмы для параллельного и векторного полнословового сложения длинных беззнаковых целых с переносом разрядов. Вследствие необходимости переносов, распараллеливание и векторизация программного обеспечения для неполиномиального сложения длинных целых традиционно считались непрактичными из-за зависимостей по данным между разрядами операндов. Представленные алгоритмы основаны на параллельном и векторном обнаружении источников переноса в частях векторных операндов с формированием битовых масок, которые в последующем скалярно прибавляются к векторной сумме исходных длинных операндов для получения их скалярной суммы методом, который является обобщением сумматора Когге-Стоуна на произвольную длину и гранулярность данных. Это отличает предложенные алгоритмы от существующих: действительно, известные и описанные в источниках сумматоры ориентированы на битовое представление данных ограниченной битовой длины, признается проблема отсутствия обобщенного описания сумматоров для операндов произвольной длины и используемого для их представления машинного слова. Поэтому в работе представлено формальное теоретическое и экспериментальное обоснование параллельной и векторной реализации сумматоров с опережающим переносом, применённой к произвольной гранулярности и произвольному размеру данных. Теоретически и экспериментально показано, что описанные алгоритмы обеспечивают заметный прирост производительности аддитивных операций с переносом при их реализации для многоядерных, многопроцессорных и векторных параллельных платформ, включая CUDA, что особенно заметно при использовании длинных векторных регистров, таких как AVX-512 с масочными регистрами и операциями над ними, а также в сравнении с существующими реализациями, такими как сумматор библиотеки GNU Multiprecision Library, построенной с включением флагов, задающих соответствующую векторизацию.

Ключевые слова: длинная арифметика, полнослововая арифметика, сумматоры с опережающим переносом, параллелизм, векторизация, SIMD, SMP, CUDA, GMP, AVX-512, регистры масок, высокопроизводительные вычисления

PARALLELIZATION AND VECTORIZATION OF FULL-WORD ADDERSCRITERIA

The article was received by the editorial board on 10.09.2022, in the final version – 29.09.2022.

Chusov Andrei A., Far-Eastern Federal University, FEFU Campus 10 Ajax Bay, Russky Island, Vladivostok, 690922, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-7931-5368, e-mail: chusov.aa@dvfu.ru
Lychev Mikhail S., Far-Eastern Federal University, FEFU Campus 10 Ajax Bay, Russky Island, Vladivostok, 690922, Russian Federation,
student, ORCID: 0000-0001-9120-5463, e-mail: lychev.ms@students.dvfu.ru
Gaida Maksim A., Far-Eastern Federal University, FEFU Campus 10 Ajax Bay, Russky Island, Vladivostok, 690922, Russian Federation,
student, ORCID: 0000-0003-3362-5253, e-mail: gayda_m@mail.ru

The paper proposes parallel and vector algorithms for performing full-word addition of long unsigned integers with carry propagation. Due to the latter, parallel and vectorized addition have long been considered impractical because of data dependencies between elements of two long addends. The presented algorithms are based on parallel and vectorized detection of carry origins within the digits of the addends, consequent construction of corresponding bit masks which, in turn, are added up to yield an adjustment to add to the vector sum of the addends using a generalization of the Kogge-Stone method upon arbitrary granularity of data as well as size of the problem. This solves the problem of poor generality of adders presented in literature which is well-known and described in multiple sources. Unlike the existing adders, the algorithms described in this paper are based upon a machine word based representation of data, rather than bit representation, and are agnostic to a definition of a word as well as size of addition. Therefore, the paper presents a formal theoretical and experimental justification of parallel and vectorized implementation of carry-lookahead adders applied to an arbitrary granularity of data of arbitrary size. The described approach is noticeably beneficial for implementation of high-performance adders using manycore, CUDA and SIMD-based parallelism, particularly using AVX-512 mask registers and the respective instructions, it significantly outperforms existing adders such as one implemented in the GNU Multiprecision Library built with the respective vectorization flags.

Keywords: long arithmetics, full-word arithmetics, carry-loookahead adders, SIMD, CUDA, parallel arithmetics, vectorization, AVX-512, high-performance computing

Введение. Использование длинной арифметики востребовано во многих областях науки и технологий, таких как криптография, обработка цифровых сигналов и высокоточные научные вычисления. Операции сложения предоставляют основание для большинства других операций длинной целочисленной арифметики. Вместе с тем аддитивные операции с переносом известны слабой распараллеливаемостью вследствие наличия зависимостей по данным, обусловленным переносами между разрядами длинных сумм. В частности, это препятствует векторизации сложения и реализации длинного сложения (например, библиотеки произвольной точности GNU Multiple Precision Arithmetic Library версии 6.2.0) предпочитают скалярное последовательное сложение (например, инструкции ADD/ADC в случае x86 и x86-64 архитектур) в пользу SIMD. Количество операций, требующихся, чтобы правильно переносить разряд и учитывать флаг переноса после сложения каждого элемента слагаемых, как минимум равно количеству элементов в слагаемых, и таким образом векторизация и распараллеливание могут не давать никаких улучшений производительности.

Однако вычисление разрядов операндов, которые при сложении генерируют установленный бит переноса, может быть частично выполнено параллельно, что предоставляет возможность увеличить производительность и энергоэффективность сумматоров ценой увеличения сложности реализации.

Подробный обзор методов создания сумматоров, основанных на битовой логике, приведен в [1]. Наиболее простой способ реализации сложения длинных целых основан на сумматоре с последовательным переносом, который складывает разряды слагаемых, поочерёдно перенося разряды. Большое количество реализаций полагаются на этот метод, потому что он простой, его легко реализовать как в виде программы, так и в виде системы логических элементов с минимальным количеством связей и соответствующих задержек. Этот сумматор легко может обойти по производительности другие более сложные методы, особенно при малых размерах операндов.

Однако обнаружение разрядов, которые оказываются источниками установленных бит переноса, распараллеливается относительно просто. Общий подход к такой операции показан в [2] и [3], в обеих работах приведены алгоритмы, широко известные как сумматоры с опережающим переносом. Эти сумматоры заранее вычисляют суммы без переноса разрядов, а затем выполняют параллельное уменьшение, циклически корректируя результат, чтобы учесть перенос разрядов. Такой подход широко используется в реализации сложения, когда важны производительность и энергоэффективность [4–6].

Недостатком методов с опережением переноса является сложность их реализации. Например, в [8] авторы совмещают два подхода, т.е. Когге – Стоуна [2] и Брент – Кунга [3], чтобы сбалансировать разреженность первого подхода с задержками второго, вызванными увеличенным количеством последовательных операций. Другим способом поиска баланса между производительностью и сложностью реализации сложения является использование древоподобной структуры алгоритма сложения, который при условии создания младшими разрядами ненулевого переноса исправляет соответствующие разряды суммы, полученной без учета переносов; если младшие разряды не создают такую необходимость, то исправление можно пропустить [6], и в этом случае может иметь место прирост производительности. Сумматоры с переключением переноса работают подобным образом, осуществляя параллельное вычисление суммы и ее инкрементированное значение и затем выбор одного из двух значений на основе значения вовремя поступившего бита переноса. В работах [9] и [10] предлагается метод реализации таких сумматоров с основной целью снижения схемотехнической сложности сумматоров.

Другим подходом к реализации параллельного сложения является выражение суммы в избыточной системе счисления, в которой данное значение может быть представлено больше, чем одним способом. Такими являются сумматор с сохранением переноса [1] и сумматор с сохранением заёма

[12] , оба похожи с точки зрения производительности. Они позволяют выполнять сложение без взаимосвязи между разрядами при условии, что представление хотя бы одного слагаемого и суммы остаётся в соответствующей избыточной системе счисления. Хотя они сами по себе быстрые и масштабируемые, преобразование между избыточной и неизбыточной системами счисления в лучшем случае сделает их производительность равной одному из сумматоров с последовательным сложением, потому что преобразование требует корректировки разрядов в неизбыточной системе счисления, что имеет сложность $O(n)$, а также дополнительной памяти (и операций ввода/вывода) для хранения значений в избыточной системе счисления.

Сумматоры, описанные в литературе, реализуются аппаратно с помощью логических вентилей, и для повышения производительности/энергоэффективности используют битовый параллелизм. Кроме этого, описанные в литературе существующие сумматоры работают с операндами достаточно (до 1 КиБ) ограниченной битовой длины, а реализации для данных произвольной длины описаны скудно [11]. Представленные в настоящей статье алгоритмы, напротив, не привязаны ни к длине, ни к машинному слову нижележащей вычислительной архитектуры, таким образом предоставляя возможность реализации параллельных и векторных полнослововых сумматоров с опережающим переносом для широкого набора вычислительных систем, используя набор распространенных арифметических инструкций, выполняемых над скалярами размером в машинное слово или векторными операндами фиксированного размера.

Для этого данная статья формализует и представляет два алгоритма параллельного сложения длинных полнослововых беззнаковых целых, используя широко распространённые скалярные многоядерные процессоры и векторизацию. Результатом является обобщение сумматоров с опережением переноса, в особенности сумматора Когге – Стоуна, чтобы складывать числа, представленные векторами произвольной длины, состоящими из машинных слов при допущении того, что пара слов может быть сложена аппаратно за постоянное время. Также исследованы функциональные требования к векторному процессору, чтобы реализовать такое сложение с приростом производительности.

На протяжении всей статьи использованы следующие обозначения. Векторы, которые представляют длинные целые длиной в n слов, находятся в группе $\langle Z_W, +\rangle$, изоморфной $\langle \mathbb{Z}_W, +\rangle$. В частности, каждый скаляр $v_i (0 \leq i < n)$ может быть либо беззнаковым целым из $\langle \mathbb{Z}_W, +\rangle$, либо знаковым целым в дополнении до W. Также представлен алгоритм без ветвлений, с помощью которого возможно обнаружение переноса для целых со знаком, который опирается на битовое представление v_i. В этом (и только в этом) случае предполагается, что W является степенью числа два.

Дополнительно представленными алгоритмами использованы раздельные b-битовые скаляры для выполнения переносов. Следовательно, предполагается, что лежащая в основе платформа предоставляет способы реализации целочисленной b-битовой арифметики, т. е. сложения в $\langle \mathbb{Z}_B, +\rangle$, где $B = 2^b$.

В этой статье использованы три операции сложения: обычное скалярное сложение «+», определённое в аддитивной группе $\langle \mathbb{Z}, +\rangle$; побитовое исключающее «или», обозначенное как $\oplus$, элементов в $\langle \mathbb{Z}_{2^n}, \oplus\rangle$ (т. е. сложение, гомоморфное полиномиальному сложению в $\{p \in \mathbb{Z}_2[x] \mid \deg(p) < n\}$) и векторное сложение $\boxplus$ векторов длины n в Z_W^n (с соответствующими скалярами, складываемыми по модулю W), образующее аддитивную группу $\langle Z_W^n, \boxplus\rangle$.

Обнаружение источников переноса. Началом алгоритма сложения является получение битовой маски, содержащей набор флагов переноса в результате сложения элементов векторов. Обнаружение легко выполняется путём сравнения значений векторов. Для этого необходимо рассмотреть два случая с учётом знакового и беззнакового сравнений, предоставляемых векторными процессорами. Например, SIMD расширения Intel AVX-512 и ARM предоставляют инструкции (к примеру, VPCMPUD и CMHS) для беззнакового сравнения. С другой стороны, некоторые процессоры позволяют сравнивать только знаковые целые, как в случае с SSE-SSE4.2 и AVX2.

Сложение двух беззнаковых скаляров x и y вызывает переполнение тогда и только тогда, когда $\forall x, y \in Z_W$: $x + y < x$ (где сложение выполняется по модулю W). Так как нет никаких других зависимостей кроме зависимости между x и y, то обнаружение, применённое к многослововым целым, может быть выполнено параллельно с применением поэлементного беззнакового сравнения. То есть, имея пару n-элементных векторов $V = (v_0 \cdots v_{n-1})^T$ и $U = (u_0 \cdots u_{n-1})^T$, а также функцию $\mathrm{CMPGT}(V, U) = ((v_0 > u_0) \cdots (v_{n-1} > u_{n-1}))$, которая отображает $(Z_W^n)^2 \to \mathbb{Z}_2^n$, обнаружение флага переноса выполняется с помощью вызова $C(V, U) = \mathrm{CMPGT}(V, V + U)$ (или $C(V, U) = \mathrm{CMPGT}(U, U + V)$).

В случае сравнения знаковых векторов, обнаружение немного более сложное, так как оно требует рассмотрения трёх случаев (рис. 1). Как указано выше, далее в настоящем разделе предполагается, что элементы векторов представлены в виде набора битов. При выполнении этого условия можно поступить следующим образом. Во-первых, если самые старшие биты обоих слагаемых x и y сбрасываются, то их сложение никогда не даст установленного флага переноса, потому что сложение младших разрядов даст перенос не более 1. Будучи добавленной к нулю самого старшего бита

суммы, эта единица никогда не даст нового ненулевого переноса. Во-вторых, если самые старшие биты обоих слагаемых установлены, то их арифметическая сумма всегда будет или 2 (двоичное 10), или 3 (двоичное 11) с левым битом, становящимся значением бита переноса, и с правым битом, равным значению переноса, получаемого в результате сложения младших бит. В противном случае, т. е. когда старшие биты x и y отличаются, получаемый флаг переноса всегда будет равен флагу, получаемому в результате сложения младших разрядов, а также противоположен сумме старших бит по модулю 2. Действительно, если самый старший бит одного из операндов установлен, а самый старший бит другого операнда сброшен, то результат арифметической суммы будет равен единице плюс флаг переноса более младших битов, т. е. 1 (двоичное 01) или 2 (двоичное 10) с левым битом, становящимся новым флагом переноса, значение которого противоположно правому биту. Полагая, что самый старший бит является битом знака, последняя проверка может быть совершена арифметическим сравнением суммы с нулём. Чтобы избежать ветвления, это обнаружение может быть представлено битовыми операциями над x и y: для знаковых целых x и y значение флага переноса равно $((0 > x)\ \mathsf{A}\ (0 > y)) \vee ((0 > x)\ \mathsf{A}\ (x + y \geq 0)) \vee ((0 > y)\ \mathsf{A}\ (x + y \geq 0)) \equiv (0 > x\ \mathsf{A}\ 0 > y) \vee (\neg(0 > x + y)\ \mathsf{A}\ ((0 > x) \vee (0 > y)))$. Аналогично случаю с беззнаковым целым, эти битовые операции не создают зависимостей данных и таким образом могут быть применены к векторам SIMD. В этом случае, имея аналогично заданное векторное сравнение CMPGT (но для целых со знаком),

$$C(V, U) = (c_1\ VAND\ c_2)\ VOR\ (c_s\ VANDN(c_1\ VOR\ c_2)), \quad (1)$$

где $c_1 = CMPGT(O,\ V)$; $c_2 = CMPGT(O,\ U)$; $c_s = CMPGT(O,\ V\ +\ U)$; O – нуль-вектор; VAND, VOR и VANDN – соответственно, поразрядные битовые И, ИЛИ и И-НЕ. И-НЕ дополняет первый операнд и вычисляет побитовую конъюнкцию результата со вторым операндом.

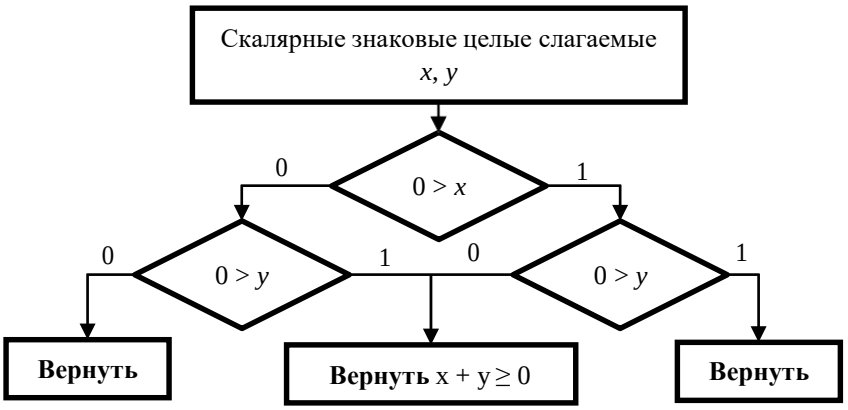


Рисунок 1 – Обнаружение флага переноса во время выполнения сложения целых со знаком в дополнении до двух

Реализация переноса. Основной проблемой, которая препятствует эффективному распараллеливанию и векторизации сложения, является необходимость переноса разрядов, потому что сложение раздельных пар разрядов может вызвать появление дополнительных переносов, что создает зависимость данных старших разрядов от результата сложения младших.

Тем не менее как только переносы, вытекающие из сложения элементов векторов (а также, возможно, перенос, возникший в результате предыдущего сложения младших частей исходных длинных целых, части которых представлены векторно) определены, можно использовать следующий подход, чтобы заменить n проверок и приращений элементов векторов на $\lceil n/b \rceil$ операций накопления битов, созданных функцией $C(V,\ U)$ (дана выше) в целочисленное значение, хранящееся в регистрах размером b бит, позволяющих выполнять арифметическое сложение и вычитание. Для этого могут быть использованы любые регистры общего назначения (или регистры битовых масок K0-K7 из AVX-512).

Для краткости в этом разделе предполагается, что $\lceil n/b \rceil = 1$, что справедливо для многих векторных процессоров. В противном случае, например, в параллельной реализации сложения, может быть использован метод Когга – Стоуна [2] для параллельной редукции b-битовых значений, как показано в разделе «Распараллеливание».

Так как результат сложения любого количества более младших разрядов числа никогда не даст значение больше, чем 1 (доказательство этого факта может быть найдено во многих классических источниках, например, в [13]), то битовая маска, созданная функцией $C(V,\ U)$, никогда не будет иметь биты, установленные в тех же позициях, что и элементы векторной суммы, которые нужно

инкрементировать в процессе учета переноса. Это позволяет объединить (используя битовое ИЛИ) маску, получаемую от $C(V,\ U)$, побитово сдвинутую на один бит влево, с маской, соответствующей позициям элементов суммы, которые создают флаги переноса в результате переноса разрядов, и при этом не будет возникать потеря данных.

Для этого нужно сначала определить те элементы векторной суммы $V\ +\ U$, разряды которой получены в результате целочисленного переполнения, то есть которые могут создать переносы. Так как максимальное значение переноса равно единице, такие элементы имеют значение $W\ -\ 1$. Следовательно, векторизованное сравнение суммы с вектором $I\ =\ (W\ -\ 1\ \cdots\ W\ -\ 1)^T$ с использованием подхода, аналогичного использованному выше, может быть применено здесь, чтобы получить маску

$$I(V,U) = CMPEQ(V+U, I), \tag{2}$$

где $\forall V,U \in Z_W^n : CMPEQ(V,U) = ((v_0 = u_0) \cdots (v_{n-1} = u_{n-1}))^T \in \mathbb{Z}_2^n$.

В целях задания формальной связи между скалярными значениями и их векторными эквивалентами мы вводим биекцию $\nu^n : \mathbb{Z}_W^n \to \mathbb{Z}_2^n$ (вместе с ее инверсией ν^{-n}) между соответствующими натурально изоморфными множествами, а также инъекцию $\gamma_W^n : \mathbb{Z}_W^n \to \mathbb{Z}_W^m$.

Теорема 1. Сумма $S = \sum_{k=0}^{n-1} s_k W^k$ двух беззнаковых целых $\nu_W^n(V) = \sum_{k=0}^{n-1} v_k W^k$ и $\nu_W^n(U) = \sum_{k=0}^{n-1} u_k W^k$, заданных векторами $V, U \in \mathbb{Z}_W^n \subset \mathbb{Z}_W^{n+1}$, где W^k – степень основания системы счисления, задающая значимость разряда длинного скаляра, а также бита $\zeta \in \mathbb{Z}_2$, равна

$$S = \nu_W^n(V) + \nu_W^n(U) + \zeta = \nu_W^{n+1}(V \boxplus U \boxplus (\gamma_W^{n+1} \circ \nu_2^{-(n+1)})(\varepsilon)), \tag{3}$$

где

$$\varepsilon = (i + 2c + \zeta) \oplus i \in \mathbb{Z}_{2n+1}, \tag{4}$$

$i = \nu_2^n(I(V,U))$ и $c = \nu_2^n(C(V,U))$.

Доказательство. Положим в качестве базы индукции $n = 1$. Тогда, чтобы учесть возможный флаг переноса, положим, что $\nu_W^1(V) = v_0$ и $\nu_W^1(U) = u_0$ находятся во множествах $\mathbb{Z}_W \times \{0\} \subset \mathbb{Z}_W \times \mathbb{Z}_2$. Тогда сложение $\nu_W(V)$ и $\nu_W^1(U)$ даёт сумму

$$S' = \nu_W^1(V) + \nu_W^1(U) = v_0 + u_0 = (v_0 + u_0) \bmod W + \left\lfloor \frac{v_0 + u_0}{W} \right\rfloor W == \nu_W^2 \begin{pmatrix} (v_0 + u_0) \bmod W \\ \left\lfloor \frac{v_0 + u_0}{W} \right\rfloor \end{pmatrix}$$

$$= \nu_W^2 (V \boxplus U \boxplus \begin{pmatrix} 0 \\ c \end{pmatrix}),$$

в которой вектор $(0 \quad c)^T = (\gamma_W^2 \circ \nu_2^{-2})(2\nu_W^1(C(V,U)))$.

Тогда прибавление ζ к сумме даёт

$$S = S' + \zeta = \nu_W^2 (V \boxplus U \boxplus \begin{pmatrix} 0 \\ c \end{pmatrix} \boxplus \begin{pmatrix} \zeta \\ i' \end{pmatrix}), \tag{5}$$

где i' является битом переноса, получаемого при прибавлении ζ к первому элементу $s'_0 \in \mathbb{Z}_W$ из S' и равно $\zeta \mathbin{\mathsf{A}} (s'_0 = W - 1) = \zeta \mathbin{\mathsf{A}} i$. Здесь $c + i' \in \mathbb{Z}_2$, так как или $c = 1$, т. е. $s'_0 \leq v_0$ и $s'_0 < u_0$, или $\zeta \mathbin{\mathsf{A}} (s'_0 = W - 1)$, потому что в $\mathbb{Z}_W$ не существует значений больших, чем $s'_0 = W - 1$, т. е. $c \mathbin{\mathsf{A}} i' = c \mathbin{\mathsf{A}} i = 0$.

Следовательно,

$$\begin{pmatrix} 0 \\ c \end{pmatrix} \boxplus \begin{pmatrix} \zeta \\ i' \end{pmatrix} = \begin{pmatrix} \zeta \\ c \oplus i' \end{pmatrix} = \begin{pmatrix} \zeta \\ c \oplus (\zeta \mathbin{\mathsf{A}} i) \end{pmatrix}. \tag{6}$$

Фиксируя имеющиеся значения s'_0 и W (и таким образом $i = (s'_0 = W - 1)$), рассмотрим аддитивную группу G_1 с множеством

$$\{t | (\exists \zeta, c \in \mathbb{Z}_2)[\neg(i \mathbin{\mathsf{A}} c) \mathbin{\mathsf{A}} (t = (i + 2c + \zeta) \oplus i)]\} \subseteq \mathbb{Z}_2^2,$$

дополненным групповой операцией – битовой суммой по модулю 2.

Заметим, что

$$\forall c, \zeta, i \in \mathbb{Z}_2 \ \mathsf{A} \neg \begin{pmatrix} i \\ c \end{pmatrix} \begin{pmatrix} i + 2c + \zeta \end{pmatrix} \oplus i = \left\lfloor \frac{(i+2c+\zeta) \oplus i}{2} \right\rfloor \cdot 2 + \left(\begin{pmatrix} i + 2c + \zeta \end{pmatrix} \oplus i\right) mod\ 2 =$$

$$\left\lfloor \frac{i+2c+\zeta}{2} \right\rfloor \cdot 2 + ((\zeta \oplus i) \oplus i) = (c \oplus \zeta \mathbin{\mathsf{A}} i) \cdot 2 + \zeta.$$

Поэтому операция замыкает G_1:

$$((i + 2c + \zeta) \oplus i) \oplus ((i + 2c + \zeta) \oplus i) = ((c_1 \oplus \zeta_1 \mathbin{\mathsf{A}} i) \cdot 2 + \zeta_1) \oplus ((c_2 \oplus \zeta_2 \mathbin{\mathsf{A}} i) \cdot 2 + \zeta_2) =$$

$$((c_1 \oplus c_2) \oplus (\zeta_1 \oplus \zeta_2) \mathbin{\mathsf{A}} i) \cdot 2 + (\zeta_1 \oplus \zeta_2) = (i + 2(c_1 \oplus c_2) + (\zeta_1 \oplus \zeta_2)) \oplus i,$$

где $(\neg(i \mathbin{\mathsf{A}} c_1) \mathbin{\mathsf{A}} \neg(i \mathbin{\mathsf{A}} c_2)) \Rightarrow \neg(i \mathbin{\mathsf{A}} (c_1 \oplus c_2))$, и таким образом G_1 изоморфна группе G_2 линейных полиномов из $\mathbb{Z}_2[x]$ с множеством

$$\{t | (\exists \zeta, c \in \mathbb{Z}_2)[\neg(i \mathbin{\mathsf{A}} c) \mathbin{\mathsf{A}} (t = (c \oplus \zeta \mathbin{\mathsf{A}} i)x + \zeta)]\} \subseteq \mathbb{Z}_2[x]$$

и отображением $G_1 \to G_2$: $a \cdot 2 + b \mapsto ax + b$, которое является биективным гомоморфизмом, потому что $(a_1 x + b_1) + (a_2 x + b_2) = (a_1 \oplus a_2)x + (b_1 \oplus b_2) \mapsto 2(a_1 \oplus a_2) + (b_1 \oplus b_2)$, а нули

возможны только, когда c и ζ оба равны нулю, потому что $(c \oplus \zeta \mathbin{\mathsf{A}} i)x + \zeta = 0 \Leftrightarrow (\zeta = 0) \mathbin{\mathsf{A}} ((c \oplus (\zeta \mathbin{\mathsf{A}} i)) = 0) \Leftrightarrow (\zeta = 0) \mathbin{\mathsf{A}} ((c \oplus 0) = 0) \Leftrightarrow (\zeta = 0) \mathbin{\mathsf{A}} (c = 0)$ и $(2c + \zeta + i) \oplus i = 0 \Leftrightarrow 2c + 2(i \mathbin{\mathsf{A}} \zeta) + \zeta = 0 \Leftrightarrow \zeta = 0 \mathbin{\mathsf{A}} c = 0$.

Следовательно, применение биекции $\nu_2^{-2} = \gamma_2^2 \circ \nu_2^{-2}$ к ε в (4) даёт (5), и таким образом (3) справедливо для $n = 1$.

Тогда из (5) и (6) следует, что $S \bmod W = (v_0 + u_0 + \zeta) \bmod W = \nu_W^1(V \boxplus U \boxplus \zeta)$, и $\lfloor S/W \rfloor = c \oplus (\zeta \mathbin{\mathsf{A}} i) = \lfloor \frac{i+2c+\zeta}{2} \rfloor \in \mathbb{Z}_2$.

Теперь, если $n > 1$, доказательство может быть получено с помощью индукции: если (3) и (4) справедливы для n, то они также справедливы для $n + 1$.

Представление слагаемых $\nu_W^{n+1}(V)$ и $\nu_W^{n+1}(U)$, соответственно, как $v_1 W + v_0$ и $u_1 W + u_0$ (где $v_0, u_0 \in \mathbb{Z}_W$ и $v_1, u_1 \in \mathbb{Z}_{W^n}$), даёт сумму $S = (v_1 + u_1)W + (v_0 + u_0 + \zeta) = (v_1 + u_1 + \lfloor \frac{v_0+u_0+\zeta}{W} \rfloor) W + (v_0 + u_0 + \zeta) \bmod W = (v_1 + u_1 + \lfloor \frac{i0+2c0+\zeta}{2} \rfloor) W + (v_0 + u_0 + \zeta) \bmod W$, где $i_0 = \nu_2^1(I(v_0, u_0))$ и $c_0 = \nu_2^1(C(v_0, u_0))$.

Заметим, что $\forall v \in \mathbb{Z}_W\ [\nu_W(v) \cdot W = \nu_W(v)]$, и $\forall \varepsilon \in \mathbb{Z}_{2^n}$: $(\gamma_\omega^n \circ \nu_2^{-n})(\varepsilon) = \gamma_W(\nu_2^{-n}(\varepsilon)) = (\gamma_W^{n+1} \circ \nu_2^{-(n+1)})(2\varepsilon)$.

Тогда, на основании индукционного предположения и доказательства начального случая при $n = 1$,

$$S = W \cdot \nu_W^{n+1}(\nu_W^{-(n+1)}(v_1) \boxplus \nu_W^{-(n+1)}(u_1) \boxplus (\gamma_W^{n+1} \circ \nu_2^{-(n+1)})(\lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor) \oplus (i_1 + 2c_1 + \lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor) \oplus i_1)) + \nu_W^1(\nu_W^{-1}(v_0) \boxplus \nu_W^{-1}(u_0) \boxplus (\gamma_W^1 \circ \nu_2^{-1})(((i_0 + 2c_0 + \zeta) \bmod 2) \oplus i_0)) =$$

$$\nu_W^{n+2}(\nu_W^{-(n+1)}(v_1) \boxplus \nu_W^{-(n+1)}(u_1) \boxplus \gamma_W^{n+2}(\nu_2^{-(n+1)}((i_1 + 2c_1 + \lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor) \oplus i_1) \oplus \nu_2^{-1}(((i_0 + 2c_0 + \zeta) \oplus i_0) \bmod 2)) =$$

$$\nu_W^{n+2}(V \boxplus U \boxplus (\gamma_W^{n+2} \circ \nu_2^{-(n+2)})(2((i_1 + 2c_1 + \lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor) \oplus i_1) + (v_0 + u_0 + \zeta) \oplus i_0) \bmod 2))). \quad (7)$$

Так как $\forall a, b, k \in \mathbb{N}_0$: $(a \oplus b) \cdot 2^k = a \cdot 2^k \oplus b \cdot 2^k$ и $\forall a, b \in \mathbb{N}_0, \forall d, c \in \mathbb{Z}_{2^n}, \forall k \geq n$: $(a \oplus b) \cdot 2^k + (c \oplus d) = (a \cdot 2^k + c) \oplus (b \cdot 2^k + d)$, последняя часть (7) может быть перегруппирована:

$((i_1 + 2c_1 + \lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor) \oplus i_1) \cdot 2 + ((i_0 + 2c_0 + \zeta) \oplus i_0) \bmod 2 = (2i_1 + 2 \cdot 2c_1 + 2\lfloor \frac{i_0+2c_0+\zeta}{2} \rfloor + (v_0 + u_0 + \zeta) \bmod 2) \oplus (2i_1 + i_0) = (2i_1 + i_0) + 2c_1 + c_0) + \zeta) \oplus (2i_1 + i_0) = (i + 2c + \zeta) \oplus i$.

Подстановка этого результата в (7) даёт (3).

Вычисление (3) предоставляет способ распараллеливания сложения, как описано в следующих разделах. Это может дать прирост производительности, если, во-первых, вычисление ν_W^{n+1} ненакладно (например, когда отображение является простым (пере-)представлением тех же данных и не включает, например, копирований и операций ввода-вывода, что может быть накладно, например, как в случае с CUDA), и, во-вторых, если вычисления ε и $(\gamma_W^{n+1} \circ \nu_2^{-(n+1)})(\varepsilon)$ эффективны. Влияние этих вычислений существенно определяет общую эффективность сумматоров, как показано ниже.

Распараллеливание. Используя (3), можно следующим образом сложить два длинных целых параллельно.

Сложение двух целых $X, Y \in \mathbb{Z}_{W^n}$ при $W > 2$ и $n > 0$, включает в себя параллельное сложение без переносов $\nu_W^n(X) \boxplus \nu_W^n(Y)$ с использованием T потоков со временем выполнения $O(n/T)$. Далее перенос разрядов должен быть выполнен с применением (4). Вычисление $\varepsilon \in \mathbb{Z}_B$ (где $B = 2^b$) также требует возможно длинного сложения битовых масок i и $2c + \zeta$ с последующим битовым суммированием по модулю два с i. Последнее является сложением двоичных цифр без переносов, которое не требует отдельных усилий для распараллеливания. Сумма $2c + \zeta$ также не требует переноса, потому что ζ является однобитовой, а вычисление $2c$ достигается простым битовым сдвигом влево (по направлению к самому старшему разряду) на одну позицию, следовательно, $2c + \zeta = (c \ll 1) \oplus \zeta$. Но вычисление суммы $i + (2c + \zeta)$ опять-таки требует переноса, что, в свою очередь, тоже может быть выполнено с помощью (3). Получается, что исходное сложение чисел размера n

уменьшено до сложения чисел i и $2c + \zeta$ размера $\lceil n \log_W 2 \rceil$. Аналогично этому сложение i и $2c + \zeta$ уменьшено до сложения $\lceil n(\log_W 2)^2 \rceil = 1$. Это уменьшение продолжается до тех пор, пока размер сложения не достигнет 1, что требует одного скалярного сложения в $\mathbb{Z}_W$, то есть $\lceil n(\log_W 2)^{\max k} \rceil = 1$ для $\max k \in \mathbb{N}_0$. Следовательно, общее количество слов, представленных в системе счисления по основанию W, которые нужно сложить, равно

$$2\sum_{k=0}^{\max k} \left\lceil \frac{n}{(\log_2 W)^k} \right\rceil = O\left(\frac{n \log_2 W - 1}{\log_2 W - 1}\right). \quad (8)$$

Для всех k таких, что $k < \max k$, то есть $\left\lceil \frac{n}{(\log_2 W)^k} \right\rceil > 1$, поэтому

$$\max k = \lceil \log_{\log_2 W} n \rceil = \left\lceil \frac{\log_2 n}{\log_2 \log_2 W} \right\rceil.$$

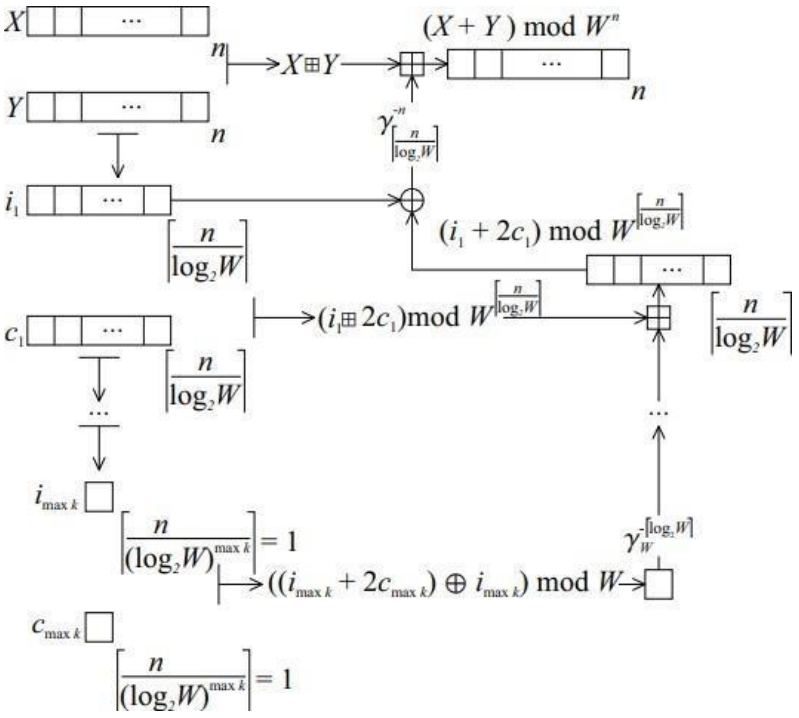


Рисунок 2 – Сложение X и Y из $\mathbb{Z}_{W^n}$ по модулю W^n с использованием (3) и параллельной редукции

Так как параллельное сложение (без учета ε) может быть выполнено параллельно T потоками, и один и тот же алгоритм параллельного сложения выполняется для слагаемых для каждого k, то общее время, требуемое для выполнения сложения T потоками, может быть оценено как

$$\sum_{k=0}^{\max k} \left\lceil \frac{n}{T(\log_2 W)^k} \right\rceil = O\left(\frac{n \log_2 W - 1}{T(\log_2 W - 1)}\right), \quad (9)$$

потому что

$$\sum_{k=0}^{\max k} \left\lceil \frac{n}{T(\log_2 W)^k} \right\rceil = O\left(\sum_{k=0}^{\max k} \frac{n}{T(\log_2 W)^k}\right) = O\left(\frac{n}{T} \frac{(\log_W 2)^{\max k+1} - 1}{\log_W 2 - 1} \frac{(\log_2 W)^{\max k+1}}{(\log_2 W)^{\max k+1}}\right) =$$

$$O\left(\frac{n}{T} \frac{1 - (\log_2 W)^{\max k+1}}{(\log_2 W)^{\max k} (1 - \log_2 W)}\right) = O\left(\frac{n}{T} \frac{1 - (\log_2 W)^{\lceil \log_{\log_2 W} n \rceil + 1}}{(\log_2 W)^{\lceil \log_{\log_2 W} n \rceil} (1 - \log_2 W)}\right) = O\left(\frac{n}{T} \frac{1 - (\log_2 W)^{\log_{\log_2 W} n + 1}}{(\log_2 W)^{\log_{\log_2 W} n} (1 - \log_2 W)}\right) =$$

$$O\left(\frac{n}{T} \frac{1 - n \log_2 W}{n(1 - \log_2 W)}\right) = O\left(\frac{n \log_2 W - 1}{T(\log_2 W - 1)}\right).$$

Следует заметить, что для достижения (9) следует исключить состояние гонки и ограничить использование блокирующей синхронизации потоков, получающих доступ к различным частям сгенерированных i и c. Это может быть достигнуто выбором (возможно увеличением) значений $\left\lfloor \frac{n}{T(\log_2 W)^k} \right\rfloor$, кратных размеру слов, из которых составлены i и c. В частности, если i и c реализованы в виде векторов из $\mathbb{Z}_W^n$, то $\left\lfloor \frac{n}{T(\log_2 W)^k} \right\rfloor$ должно быть кратно $\lceil \log_2 W \rceil$ для каждого потока, устанавливающего биты в наборе его собственных слов.

Изложенный выше вывод также может быть применён к (8) с $T = 1$ для оценки требований к памяти. Конкретнее, пространство, требуемое этим алгоритмом, исключая $3n$ слов слагаемых и суммы (то есть пространство, требуемое для хранения значений i, c и $\varepsilon \bmod 2^n$), может быть оценено верхней границей

$$3\sum_{k=1}^{\max k}\left\lceil\frac{n}{(\log_2 W)^k}\right\rceil = 3\sum_{k=1}^{\max k}\left\lfloor\frac{n+(\log_2 W)^k-1}{(\log_2 W)^k}\right\rfloor \quad 3\left(\max k+\sum_{k=1}^{\max k}\left\lfloor\frac{n-1}{(\log_2 W)^k}\right\rfloor\right)$$

$$\leq 3\left(\max k+\sum_{k=1}^{\max k}\frac{n-1}{(\log_2 W)^k}\right) = 3\left(\max k+\frac{n-1}{\log_2 W}\frac{(\log_W 2)^{\max k}-1}{\log_W 2-1}\right)$$

$$\leq 3\left(\max k+\left\lceil\frac{n-1}{\log_2 W}\frac{(\log_W 2)^{\max k}-1}{\log_W 2-1}\right\rceil\right)$$

$$= 3\left(\max k+\left\lfloor 1+\frac{((\log_W 2)^{\max k}-1)(n-1)-1}{1-\log_2 W}\right\rfloor\right)$$

$$= 3\left(\max k+\left\lfloor 1+\frac{((\log_2 W)^{\max k}-1)(n-1)-(\log_2 W)^{\max k}}{(\log_2 W)^{\max k+1}-(\log_2 W)^{\max k}}\right\rfloor\right)$$

$$= 3\left(\max k+\left\lfloor 1+\frac{n-2}{\log_2 W-1}-\frac{n-1}{(\log_2 W)^{\lceil\log_{\log_2 W} n\rceil}(\log_2 W-1)}\right\rfloor\right)$$

$$\leq 3\left(\max k+\left\lfloor 1+\frac{n-2}{\log_2 W-1}-\frac{n-1}{n(\log_2 W-1)}\right\rfloor\right) = 3\left(\max k+\left\lfloor 1+\frac{n^2-3n+1}{n(\log_2 W-1)}\right\rfloor\right).$$

Векторизация. Как показано в данной статье, скалярные операции над битовыми масками i и c, как если бы эти маски были обычными целыми размером в машинное слово, дают возможность увеличить производительность векторизованного сложения и обогнать в производительности существующие скалярные реализации с последовательным переносом.

Это зависит от способности параллельной (векторной) платформы эффективно реализовывать оба отображения, использованных в утверждении теоремы, т. е. γ_W^n (и инверсию γ_W^{-n}) и ν_2^n (или композицию $\gamma_W^n \circ \nu_2^{-n}$). Так обстоит дело с новыми масочными регистрами и инструкциями расширения AVX-512, которые обеспечивают прирост в производительности сумматоров с опережением переноса, благодаря использованию (3).

Уравнение (3) также может быть использовано для улучшения производительности векторного сложения, если, помимо сложения, отображения ν_m^n и γ_m^n также могут быть реализованы эффективно с помощью векторного процессора. В то время как поддержка ν_m^n, применяемая к результатам сравнения (1) и (2), широко распространена (например, PCMPEQ/PCMPGT в SSE2 и CMEQ/CMHI в ARM), поддержка последнего заметно ограничена, и в то время как его реализация возможна с применением таблиц поиска, она требует обращения к внешней памяти и таким образом может быть неэффективна. Экспериментальным путём значительного увеличения производительности получилось достичь только применением масочных операций Intel AVX-512 над регистрами K0-K7. Реализация критического цикла с использованием AVX-512 в синтаксисе Microsoft Assembly (MASM) представлена на рисунке 3. В этой реализации 512-битные векторные величины находятся в $\mathbb{Z}_{2^{64}}^8$, и значения масок – в $\mathbb{Z}_{2^{16}}$ (чтобы учитывать дополнительный бит переноса из (4)).

В других случаях реализация отображений $\nu_2^n(I(V,U))$ и $\nu_2^n(C(V,U))$ довольно проста с применением широко распространённых инструкций для сравнения векторов (см. раздел 2). Такими являются, например, (V)PCMPEQ и (V)PCMPU у Intel [14, раздел 5.2] (том 2C) и CMEQ и CMHI у ARM [15], которые устанавливают биты частей регистра-приёмника в зависимости от того, как соответствующие части операндов соотносятся с предикатом сравнения.

С другой стороны, обратное преобразование, $(\gamma_W^n \circ \nu_2^{-n})$, использованное в (3), не является широко распространённым, что делает его реализацию менее эффективной. Так как длины векторов регистров обычно малы, преобразование во многих случаях может быть реализовано с помощью таблицы поиска, которая отображает короткие скалярные целые в соответствующие векторные величины. Очевидным недостатком этого способа является потребность в структуре данных во внешней памяти, доступ к которой может быть дорогостоящим, хотя такая таблица может быть достаточно небольшой, чтобы находиться в кэш-памяти. Такая реализация для 256-битных векторов AVX-2 (с $n = 4$) показала уменьшение производительности (рис. 8) по сравнению с последовательным сумматором.

Наиболее выгодным путём совмещения параллельного алгоритма, показанного на рисунке 2, с векторизацией показала себя редукция подвектора до множества одиночных битов c (полученного из ε суммой наиболее значащих частей подвекторов) и i (которое может быть получено из накопленного поразрядного И значений $\nu_2^n(I(v_i, u_i))$ элементов v_i и u_i подвекторов, в результате дающее $2^n - 1$, если результирующий бит i установлен), записать c и i в соответствующие векторы слов так, что каждое слово занято одним битом, а затем, используя параллельную редукцию, упаковать эти биты в слова: $\mathbb{Z}_w^n \to \mathbb{Z}_2^n \to \mathbb{Z}_w^{\lceil n/\log_2 W\rceil}$. Элементы результата затем могут быть объединены для получения ε с использованием параллельного алгоритма (рис. 2) и/или векторного алгоритма (рис. 3). Если

использован последний, потребуется найти способ удвоения значения целых чисел, представляющих биты c, которое может быть выполнено с помощью инструкций битовых сдвигов (например, (V)PSLL из x86-64 или SHL из ARM) и горизонтальной перестановкой элементов (соответственно, (V)PSHUF и VEXT).

```
start:
xor rax, rax; memory index
;zmm2 := (-1  -1  -1  -1  -1  -1  -1  -1), т. е.
;установить все биты zmm2
vpternlogq zmm2, zmm2, zmm2, 0FFh
kxorw k1, k1, k1 ;k1:= ζ = 0
loop_start:
;zmm0 := (v0  v1  v2  v3  v4  v5  v6  v7)
vmovdqu64 zmm0, [V + rax]
;zmm1 := (u0  u1  u2  u3  u4  u5  u6  u7)
vmovdqu64 zmm1, [U + rax]
;векторное сложение:
;zmm0 := zmm0 ⊞ zmm1
vpaddq zmm0, zmm0, zmm1
;k0 := vW^k(CMPGT(zmm1, zmm0)) = c
vpcmpuq k0, zmm0, zmm1, 1
kaddw k0, k0, k0 ; k0 := k0 + k0
kxorw k0, k0, k1 ; k0 := k0 + ζ
;k1 := vW^k(CMPEQ(zmm0, zmm2)) = t
vpcmpeqq k1, zmm0, zmm2
kaddw k0, k0, k1 ; k0 := k0 + k1
kxorw k1, k0, k1 ; k1 := k0 ⊕ k1 = ε
;zmm0 := zmm0 ⊞ (γ2^β ∘ v2^-β)(ε mod 2^β)
vpsubq zmm0 {k1}, zmm0, zmm2
;k1:= ζ = [k1 / 2^β] = [ε / 2^β]
kshiftrw k1, k1, 8
;(s0  s1  s2  s3  s4  s5  s6  s7) := zmm0
vmovdqu64 [S + rax], zmm0
add rax, 64
cmp rax, r9
jc loop_start
```

Рисунок 3 – Векторное сложение X и Y, принадлежащих $\mathbb{Z}_{W^n}$, по модулю W^n, основанное на (3) с использованием инструкций AVX-512 для векторов и масок

Эксперименты. Измерения производительности алгоритмов были выполнены на компьютере с процессором Intel Core i9-10980XE с 18 физическими ядрами и включённой многопотоковостью ядер, с видеокартой NVIDIA Tesla K40m CUDA под управлением Ubuntu Workstation 20.04.3 LTS.

Измерения были выполнены в виде разницы между двумя значениями счётчика тактов процессора, получаемыми с помощью инструкции RDTSC.

Разным реализациям параллельных и векторных алгоритмов сложения были даны наборы случайных данных, представлявших слагаемые размерами от 64 байт до 8 гигабайт. Измерения были выполнены 10 раз для каждого эксперимента, а затем усреднены. Результаты, представленные в статье, являются средними арифметическими.

Измерения производительности параллельного алгоритма (рис. 2) демонстрируют увеличение производительности длинного сложения (рис. 4).

Однако измерения показывают низкую масштабируемость параллельных алгоритмов как с векторизацией, так и без векторизации (рис. 5), достигающих соответственно ускорений около 2,1 и 2,2, когда алгоритмы выполнялись для сложения двух 8-гигабайтных величин 11 потоками выполнения на компьютере с 18 физическими ядрами. Тем не менее показан устойчивый прирост производительности, когда используется параллельный сумматор по сравнению с производительностью последовательного сумматора и аналогично, когда используется параллельное сложение с векторизацией AVX-512 по сравнению со всеми другими сумматорами.

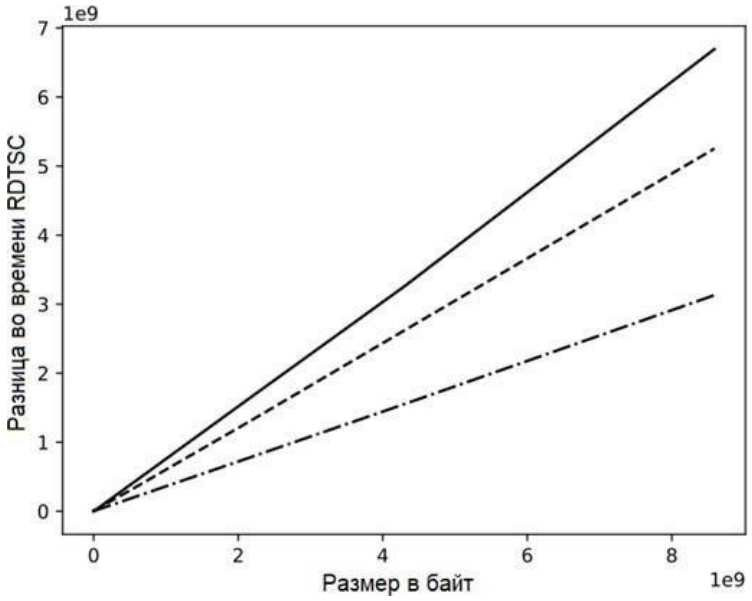


Рисунок 4 – Время, затраченное на выполнение сложения двух длинных величин с использованием параллельного алгоритма, показанного на рисунке 2, выполненного 36 логическими ядрами (пунктирная линия), сравнённое со временем, затраченным тем же алгоритмом, но таким, что каждый поток выполнял векторизованное сложение (рис. 3), создавая пару битов i и c для рекурсивного сложения с применением (4) (точка-пунктир), и со временем выполнения последовательного сложения с использованием инструкции ADC (сплошная линия)

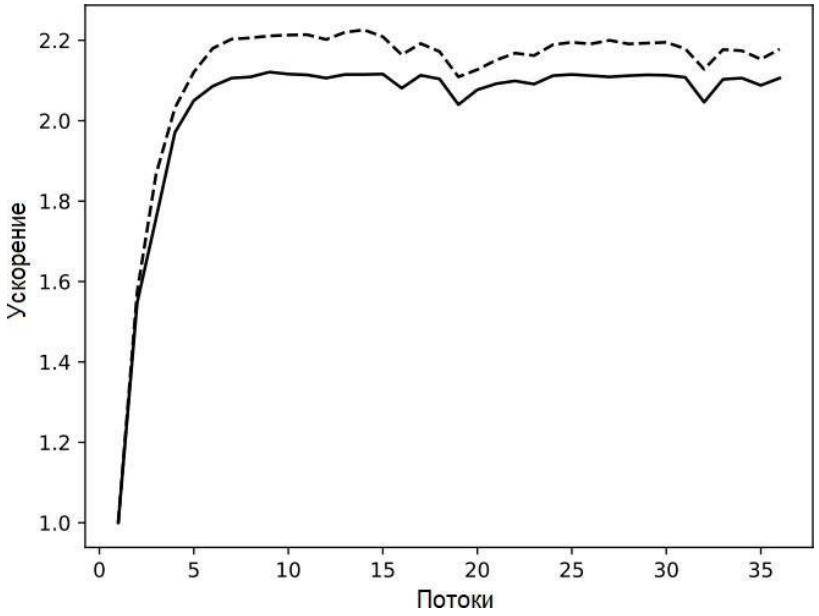


Рисунок 5 – Ускорения, достигнутые с использованием параллельного сумматора без векторизации (сплошная линия) и с (пунктирная линия) векторизацией AVX-512 на компьютере с 18 физическими (36 логическими) ядрами процессора

Что касается векторизации на одном процессоре, прирост производительности заметен до тех пор, пока потери времени на взаимодействие с памятью не начинают превосходить прирост производительности, что происходит на отметке около 8 Мб на каждое слагаемое (рис. 6).

Кроме того, реализация параллельного сложения для CUDA даёт прирост производительности, показанный на рисунке 7, который не учитывает время, требуемое на передачу данных через шину PCI-E. Однако как только начинается передача данных через шину, например, когда у CUDA устройства недостаточно памяти для хранения всех данных сразу (т. е. обоих слагаемых, суммы, а также наборов бит i, c и ε из (4) на каждой итерации параллельного алгоритма (рис. 2)), производительность сложения быстро падает.

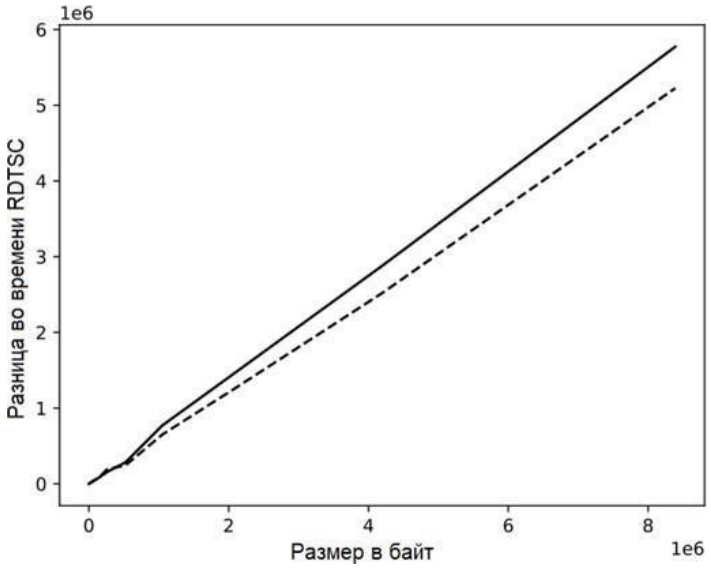


Рисунок 6 – Время, затраченное на выполнение сложения двух длинных величин, до 8 МБ случайных данных на слагаемое с использованием AVX-512 реализации векторного алгоритма из рисунка 3 (пунктирная линия), сравнённое со временем выполнения последовательного сложения с использованием инструкции ADC (сплошная линия)

Следует отметить, что все исследованные реализации длинного сложения значительно превзошли в производительности сложение библиотеки GNU Multiprecision Library (GMP) версии 2.6.0 [16], собранной с соответствующими флагами поддержки AVX-512, даже если измерения не учитывают обмен данными, выполняемый вызовами mpz_import и mpz_export. Это показано на рисунке 8.

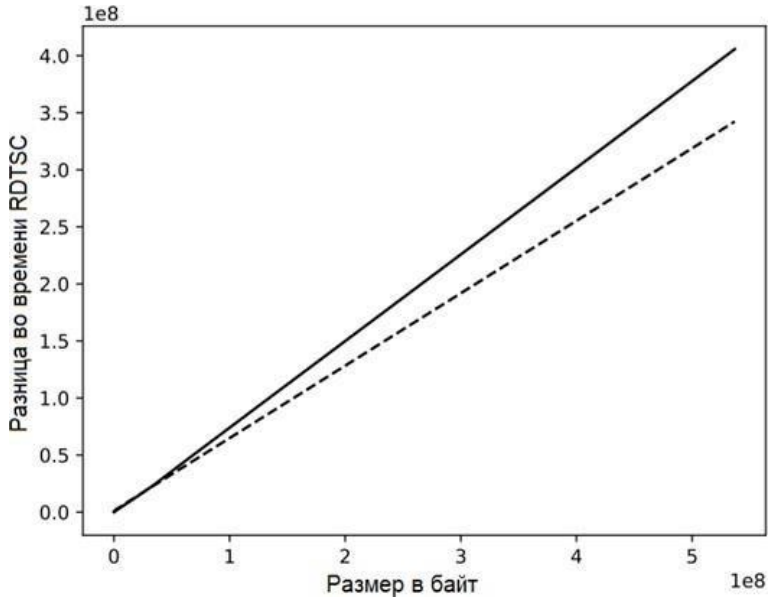


Рисунок 7 – Измеренная производительность CUDA реализации (пунктирная линия) сложения с использованием NVIDIA Tesla K40m, сравнённая с последовательным сложением на процессоре с использованием инструкции ADC (сплошная линия). Времена для CUDA не учитывают обмен данными между хостом и устройством

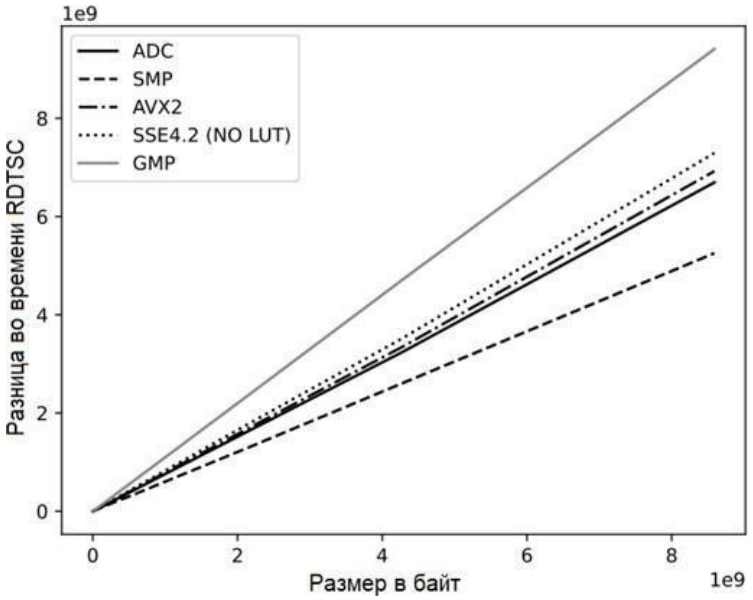


Рисунок 8 – Производительность длинного сложения с помощью библиотеки GNU Multiple Precision (GMP) [16] в сравнении с производительностью других реализаций. Показательна производительность ADC и SMP в сравнении с другими результатами

Заключение. Широко распространено мнение, что сложение полнослововых длинных целых параллельно, и в особенности с использованием векторизации, непрактично из-за необходимости переноса, который создаёт взаимосвязи между разрядами слагаемых и суммы. С одной стороны, это может быть справедливо, потому что распараллеливание и векторизация может быть применена только частично и ценой увеличения сложности алгоритма. Тем не менее существуют различные применения, например, в высокоточных научных вычислениях, включая те, которые основаны на вещественной арифметике, обработке цифровых сигналов и криптографии, где сложение может стать критичным для производительности и энергоэффективности. В этом случае сложность реализации может стать приемлемой или может быть снижена, как показано в [3, 6, 7].

Однако существующие источники концентрируются на аппаратной реализации сумматоров и используют распараллеливание на уровне бит, требуя специализированного аппаратного обеспечения для выполнения сложения с малой задержкой. Представленная статья, с другой стороны, фокусируется на использовании неспециализированных скалярных и векторных процессоров, которые обладают минимальным набором обычных арифметических инструкций для достижения похожих приростов производительности. Поэтому предложены алгоритмы и их формальный анализ. В частности, если длина слова равна 1 бит, т. е. $W = 2$, тогда из утверждения теоремы 1 можно легко вывести полнослововые сумматоры, выполняющие векторизацию на уровне бит, с опережением переноса (описанные, например, в [5]). Представленный параллельный алгоритм, показанный на рисунке 2, соответствует одному из них [2] и [7].

Эксперименты, проведённые для измерения производительности результатов подтверждают прогноз (9) из статьи. В особенности AVX-512 с его аппаратной реализацией χ_W^n через операции над битовыми масками помогает значительно увеличить производительность сложения, особенно когда сложение реализовано на многоядерном процессоре. Параллельная реализация без использования векторизации, хоть и не очень масштабируема, предоставляет значительный прирост производительности по сравнению с последовательным скалярным сложением, реализующим алгоритм с последовательным переносом, даже если к последнему применены методы оптимизации, такие как развёртка циклов.

Приросты производительности также имеют место, когда сложение выполняется на устройстве CUDA, пока отсутствуют передачи параметров между хостом и устройством. Все реализации значительно превзошли в производительности сложение, реализованное в библиотеке GNU Multiple Precision (версия 6.2.0), даже если импорт и экспорт операндов и результата не учитывались при измерении времени. Поверхностный анализ исходного кода GMP, а также его дизассемблированного представления показал, что много времени занимает реструктуризация и перераспределение данных с выполнением сложения в нескольких разных циклах с последовательным переносом.

Библиографический список

1. Awasthi, V. Hybrid Signed Digit Arithmetic in Efficient Computing: A Comparative Approach to Performance Essay / V. Awasthi, K. Raj // Novel Perspectives of Engineering Research. – 2021. – Vol. 2, № 10. – P. 47–58.
2. Kogge P. M. A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations / P. M. Kogge, H. S. Stone // IEEE Transactions on Computers. – 1973. – Vol. C-22, no. 8. – P. 786–793.
3. Brent. A Regular Layout for Parallel Adders / Brent, Kung // IEEE Transactions on Computers. – 1982. – Vol. C-31, № 3. – P. 260–264.
4. Paci, G. Exploration of Low Power Adders for a SIMD Data Path / G. Paci, P. Marchal, L. Benini // 2007 Asia and South Pacific Design Automation Conference. – 2007. – P. 914–919.
5. Srikanth, S. Low Power Array Multiplier using Modified Full Adder / S. Srikanth, I. T. Banu, G. V. Priya, G. Usha // 2016 IEEE International Conference on Engineering and Technology (ICETECH). – 2016. – P. 1041–1044.
6. Kumar, S. High-Speed, Low Area and Energy Efficient 32bit Carry Skip Adder using Verilog HDL / S. Kumar, B. P. Konduru // International Conference on Emerging Trends in Engineering, Science and Technologies (ICETEST 2017). – 2017. – № 03.
7. Jafarzadehpour, F. A New Energy-Efficient Hybrid Wide-Operand Adder Architecture / F. Jafarzadehpour, A. Sabbagh Molahosseini, A. Emrany, L. Sousa // IET Circuits, Devices & Systems. – 2019. – Vol. 13, № 11.
8. Ahammed, M. J. Fast Performance of Parallel Adders using VLSI / M. J. Ahammed, M. M. Parvez // International Journal of Engineering Research & Technology (IJERT). – 2014. – Vol. 3, № 10. – P. 356–360.
9. Sarabdeep, S. Design of Area and Power Efficient Modified Carry Select Adder / S. Sarabdeep, K. M. Dilip // International Journal of Computer Applications. – 2011. – Vol. 33. – P. 14–18.
10. Mohanty, B. Area-Delay-Power Efficient Carry-Select Adder / B. Mohanty, S. Patel // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2014. – Vol. 61, № 06. – P. 418–422.
11. Langhammer, M. High Precision, High Performance FPGAAdders / M. Langhammer, B. Pasca, G. Baeckler // 2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM). – 2019. – P. 298–306. – DOI: 10.1109/FCCM.2019.00047.
12. Selsi Aulvina, C. Low Power and Area Efficient Borrow Save Adder Design / C. Selsi Aulvina, R. Kabilan // 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT). – 2018. – pp. 339–342.
13. Knuth, D. E. The Art of Computer Programming, Seminumerical Algorithms / D. E. Knuth. – 3rd ed. – Boston, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 1997. – Vol. 2.
14. Intel Corporation. Intel® 64 and IA-32 Architectures Software Developer's Manual. – Intel Corporation, 2022. – Режим доступа: https://www.intel.com/content/www/us/en/develop/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4.html.
15. Arm Limited. Arm® Architecture Reference Manual Armv8, for A-profile architecture. – ARM Limited, 2021. – Режим доступа: https://developer.arm.com/documentation/ddi0487/gb/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 10.09.2022).
16. Free Software Foundation. (2020) Integer Arithmetic (GNU MP 6.2.1). – Режим доступа: https://gmplib.org/manual/Integer-Arithmetic, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 10.09.2022).

References

1. Awasthi, V., Raj, K. Hybrid Signed Digit Arithmetic in Efficient Computing: A Comparative Approach to Performance Essay. *Novel Perspectives of Engineering Research*, 2021, vol. 2, no. 10, pp. 47–58.
2. Kogge, P. M., Stone, H. S. A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations. *IEEE Transactions on Computers*, 1973, vol. C-22, no. 8, pp. 786–793.
3. Brent and Kung. A Regular Layout for Parallel Adders. IEEE Transactions on Computers, 1982, vol. C-31, no. 3, pp. 260–264.
4. Paci, G., Marchal, P., Benini, L. Exploration of Low Power Adders for a SIMD Data Path. *2007 Asia and South Pacific Design Automation Conference*, 2007, pp. 914–919.
5. Srikanth, S., Banu, I. T., Priya, G. V. and Usha, G. Low Power Array Multiplier using Modified Full Adder. *2016 IEEE International Conference on Engineering and Technology (ICETECH)*, 2016, pp. 1041–1044.
6. Kumar S. and B. Konduru, P. High-Speed, Low Area and Energy Efficient 32bit Carry Skip Adder using Verilog HDL. *International Conference on Emerging Trends in Engineering, Science and Technologies (ICETEST 2017)*, 2017, no. 03.
7. Jafarzadehpour, F. Molahosseini, Sabbagh A., Emrany, A. and Sousa, L. A New Energy-Efficient Hybrid Wide-Operand Adder Architecture. *IET Circuits, Devices & Systems*, 2019, vol. 13, no. 11.
8. Ahammed, M. J. and Parvez, M. M. Fast Performance of Parallel Adders using VLSI. *International Journal of Engineering Research & Technology (IJERT)*, 2014, vol. 3, no. 10, pp. 356–360.
9. Sarabdeep, S. and Dilip, K. M. Design of Area and Power Efficient Modified Carry Select Adder. *International Journal of Computer Applications*, 2011, vol. 33, pp. 14–18,
10. Mohanty, B. and Patel, S. Area-Delay-Power Efficient Carry-Select Adder. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2014, vol. 61, no. 06, pp. 418–422.
11. Langhammer, M., Pasca, B. and Baeckler, G. High Precision, High Performance FPGA Adders. *2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2019, pp. 298–306. DOI: 10.1109/FCCM.2019.00047.
12. Aulvina Selsi C. and Kabilan, R. Low Power and Area Efficient Borrow Save Adder Design. 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2018, pp. 339–342.

13. Knuth, D. E. The Art of Computer Programming, Seminumerical Algorithms. 3rd ed. Boston, MA, USA, Addison-Wesley Longman Publishing Co., Inc., 1997. Vol. 2.

14. *Intel Corporation, Intel® 64 and IA-32 Architectures Software Developer's Manual*. Intel Corporation, 2021. Available: https://www.intel.com/content/www/us/en/develop/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4.html.

15. *Arm Limited, Arm® Architecture Reference Manual Armv8, for A-profile architecture*. ARM Limited, 2021. Available: https://developer.arm.com/documentation/ddi0487/gb/ (acessed 10.09.2022).

16. *Free Software Foundation. (2020) Integer arithmetic (GNU MP 6.2.1)*. Available: https://gmplib.org /manual/Integer-Arithmetic (acessed 10.09.2022).

УДК 004.052

СНИЖЕНИЕ РЕСУРСНЫХ ЗАТРАТ НА ОБРАБОТКУ КОДОВ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ ЗА СЧЕТ ОГРАНИЧЕНИЯ ЧИСЛА ОБРАБАТЫВАЕМЫХ СООБЩЕНИЙ

Статья поступила в редакцию 30.09.2022, в окончательном варианте – 14.10.2022.

Таныгин Максим Олегович, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19,

кандидат технических наук, доцент, ORCID: 0000_0002_4099_1414, e-mail: tanygin@yandex.ru

Чеснокова Алина Андреевна, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19,

аспирант, ORCID: 0000_0003_1183_4572, e-mail: chesnokova.50@yandex.ru

Ахмад Али Айед Ахмад, Юго-Западный государственный университет, 305004, Российская Федерация, г. Курск, ул. Челюскинцев, 19,

аспирант, ORCID: 0000_0002_6031_9414, e-mail: aliayid2013@gmail.ru

Исследованы особенности практической реализации методов аутентификации и опознавания источника сообщений, основанные на использовании кодирования в режиме сцепления блоков. Приёмник выполняет обработку кодов поступающих сообщений и формирование структурированной их последовательности на основе известных статистических характеристик потока сообщений от отправителя и посторонних источников. При этом из обработки исключается часть сообщений, исходя из характеристик сформированной к текущему моменту времени структурированной последовательности и значения специального индексного поля, являющегося неотъемлемой частью кода аутентификации сообщения. Реализация метода требует формирования и хранения во внутренней памяти получателя динамических списочных структур, описывающих формируемые множества сообщения. Создана оригинальная математическая модель заполнения внутренней памяти получателя, позволившая оценить сложность формируемой динамической структуры. Полученные на основе математического моделирования результаты показали, что исключение из обработки части поступающих сообщений позволяет снизить затраты памяти приёмника в 3–4 раза, сохраняя достоверность аутентификации на уровне, приемлемом для протоколов связи, используемых в энергоэффективных сетях передачи данных с большим радиусом действия.

Ключевые слова: аутентификация, сообщение, кодирование в режиме сцепления блоков, ресурсная сложность

REDUCING RESOURCE COSTS FOR PROCESSING MESSAGE AUTHENTICATION CODES BY LIMITING THE NUMBER OF MESSAGES PROCESSED

The article was received by the editorial board on 30.09.2022, in the final version – 14.10.2022.

Tanygin Maxim O., Southwest State University, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, ORCID: 0000_0002_4099_1414, e-mail: tanygin@yandex.ru

Chesnokova Alina A., Southwest State University, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,

postgraduate student, ORCID: 0000_0003_1183_4572, e-mail: chesnokova.50@yandex.ru,

Ahmad Ali Ayed Ahmad, Southwest State University, 19 Chelyuskintsev St., Kursk, 305004, Russian Federation,

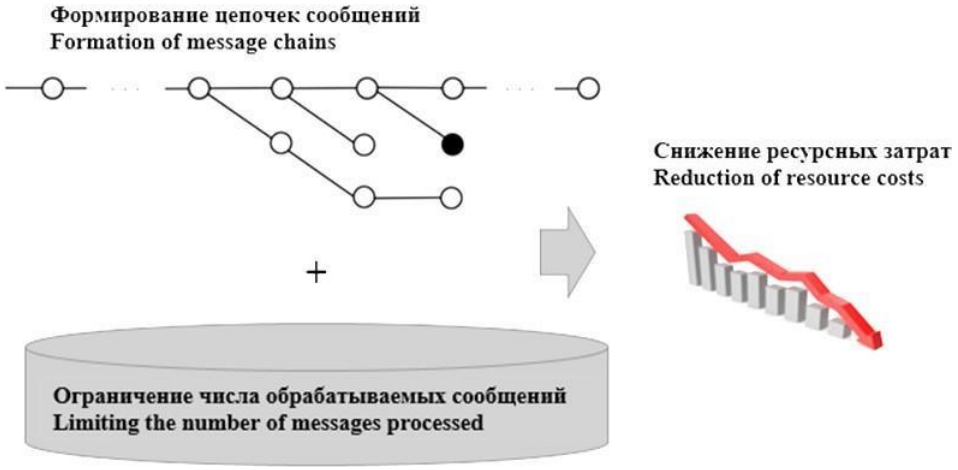
postgraduate student, ORCID: 0000_0002_6031_9414, e-mail: aliayid2013@gmail.ru

The features of the practical implementation of authentication methods and identification of the source of messages based on the use of coding in the mode of block coupling are investigated. The receiver processes the codes of incoming messages and forms a structured sequence based on the known statistical characteristics of the message flow

from the sender and from outside sources. At the same time, a part of the messages is excluded from processing, based on the characteristics of the structured sequence formed by the current time and the value of a special index field, which is an integral part of the message authentication code. The implementation of the method requires the formation and storage in the recipient's internal memory of dynamic list structures describing the message sets being formed. An original mathematical model of filling the recipient's internal memory has been created, which made it possible to assess the complexity of the dynamic structure being formed. The results obtained on the basis of mathematical modeling showed that excluding part of incoming messages from processing reduces receiver memory costs by 30–40 %, while maintaining authentication reliability at a level acceptable for communication protocols used in energy-efficient data transmission networks with a long range.

Keywords: authentication, message, coding in block coupling mode, resource complexity

Graphical annotation (Графическая аннотация)



Введение. Необходимость доверенного взаимодействия меду компонентами систем дистанционного мониторинга и управления системы является основой корректного выполнения такой системой её функций. Для этого в составе каждого компонента системы реализуется модуль опознавания, обеспечивающий определение источника поступающей информации за счёт использования протоколов аутентификации [1]. В то же время особенности реализации указанных систем управления, такие как использование беспилотных летающих аппаратов [2], искусственных спутников земли [3], высокоавтономных средств контроля состояния физической среды и технологических процессов[4], могут накладывать серьезные ограничения на реализацию протоколов и выбор их математического базиса.

Требования по низкой вычислительной сложности и небольшому объёму передаваемых кадров данных (до нескольких байтов) вынуждают использовать алгоритмы, обеспечивающие высокую достоверность при размере поля, содержащего аутентифицирующую информацию, до нескольких битов сообщения [5, 6]. В их основе лежит определение источника не единичного сообщения, а последовательности сообщений, сформированных одним отправителем. Сами сообщения кодируются в режиме сцепления блоков, т. е. код аутентификации сообщения содержит некоторый цифровой отпечаток не только идентификатора отправителя, но и предыдущего отправленного сообщения. Различные вариации такого подхода, заключающиеся в преобразовании содержимого информационных полей в соответствии с некоторым ключом и формировании хеш-последовательностей, описываются и в работах [8–10].

Практическая реализация кодирования в режиме сцепления блоков для опознавания источника последовательности сообщений требует последовательной обработки поступающих сообщений, формирования из них динамических списочных структур, которые при последующей проверке будут интерпретированы как последовательность сообщений от целевого источника [11]. Это требует внедрения в состав устройства-получателя дополнительной буферной памяти для временного хранения как самих блоков данных, так и сформированных из них промежуточных результатов вычислений. Кроме того, принятие решения об источнике полученных данных происходит с некоторой задержкой, связанной с необходимостью полностью сформировать из сообщений динамическую структуру и произвести её проверку. Принадлежность сообщения единственной последовательности требуемой длины n является критерием успешной аутентификации его источника. В то же время при формировании последовательности коды аутентификации сообщений целевого источника могут случайным образом совпадать с кодами аутентификации сообщений посторонних источников, в качестве которых могут выступать как злоумышленники, так и отличные от источника и приёмника компоненты распределенных систем, обменивающихся информацией по общему каналу связи.

Для рассмотренного нами целевого класса получателей, представляющих собой высокоавтономные вычислительные устройства с невысокой производительностью и аппаратной сложностью довольно остро стоит проблема снижения объёма задействованной регистровой памяти. В этой связи был предложен метод, в основе которого внедрение в код аутентификации сообщения некоторого индекса, определяющего расположение конкретного сообщения в последовательности формированной отправителем. На основании значения этого индекса сообщение может быть исключено из обработки, так как между индексом поступающего сообщения легального отправителя и индексами сообщений, помещённых приемником в вышеописанную динамическую структуру имеется зависимость, позволяющая с высокой вероятностью определять диапазон значений индексов, которыми в каждый момент времени могут обладать сообщения отправителя [12].

Формулировка задачи. Пусть имеется последовательность сообщений, передаваемых от отправителя получателю $S = \{S_i\}$, $i = \overline{1,n}$. Каждое сообщение состоит из информационной части, кода аутентификации, представляющего собой кодограмму из данных предыдущего сообщения, и кода порядкового номера i сообщения в последовательности. Сообщения последовательно передаются отправителем в канал связи. Так как модель Аллоха [13], используемая для организации обмена данными в современных беспроводных сетях, предусматривает сохранение последовательности передачи сообщений, то считаем, что в такой же последовательности они доходят до получателя, помимо сообщений целевого источника из-за асинхронного доступа к каналу связи [14]. Число таких сообщений является случайной величиной, определяемой параметром K – отношением общей интенсивности формирования сообщений в системе к интенсивности формирования сообщений отправителем, и для беспроводных сетей передачи может быть описано распределением Пуассона [15, 16]. Получатель последовательно проверяет каждое поступающее сообщение. При этом выделяется его порядковый номер J^s [12], проверяется условие:

$$M_{max} - W_{back} \leq J^s \leq M_{max} + 1, \quad (1)$$

где W_{back} – число, на которое порядковый номер сообщения может быть меньше M_{max}, $1 \leq W_{back} \leq M$;

M_{max} – максимальный индекс всех поступивших сообщений.

В случае если для кода аутентификации сообщения C^s выполняется условие:

$$C^s = F(S_i), \max(1, M_{max} - W_{back}) \leq i \leq M_{max}, \quad (2)$$

где F – операция кодирования сообщения s_i с порядковым номером i, поступившее сообщение добавляется в цепочку после сообщения s_i

Добавление сообщения в цепочку проиллюстрировано на рисунке 1, где штриховкой обозначены сообщения отправителя, чёрным – текущее обрабатываемое получателем сообщение, белым – посторонние сообщения, добавленные в цепочку.

Таким образом формируется дерево сообщений, и критерием аутентичности последовательности сообщения является единственность пути длиной n от корня дерева до самого удалённого его элемента [17].

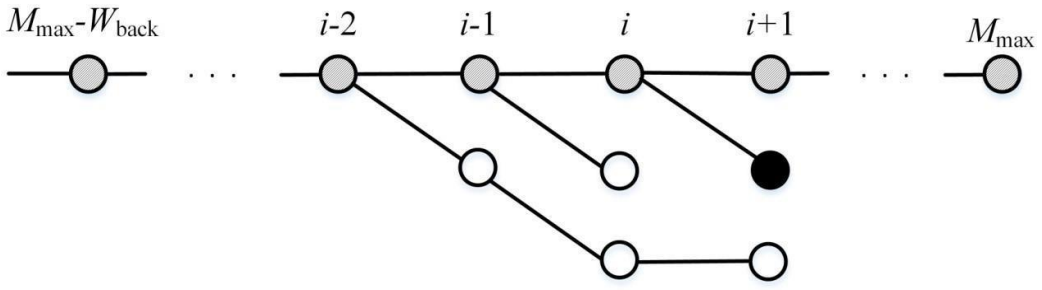


Рисунок 1 – Формирование цепочек сообщений

В [19] показано, что наиболее приемлемой с точки зрения скорости выполнения операций формирования и обработки последовательностей сообщений является комбинированная косвенная организация памяти, при которой сами сообщения хранятся в буферной оперативной памяти, а последовательности представляют собой матрицу регистров, содержащих указатели на сообщения в буфере и дополнительную информацию, необходимую для проверки кодов аутентификации поступающих сообщений. Параметром, влияющим на затраты регистровой памяти для хранения дерева, является его максимальная ширина или, максимальное число сообщений с одинаковым порядковым номером, добавленных в структуру.

Оценки затрат памяти для хранения цепочек (ветвей древовидной структуры) для методов, не учитывающих порядок поступления сообщений, приведены в [20]. Тогда как ограничение числа обрабатываемых получателем сообщений, помимо повышения достоверности аутентификации приёмника, снижает ширину графа и, соответственно, ресурсные затраты на его хранение и обработку. При этом для практической реализации представляет интерес оценка вероятности достижения ширины дерева определённого числа, так как именно она определяет вероятность возникновения ошибки переполнения буфера [21, 22].

Модель формирования посторонних ветвей. Оценку максимальной ширины древовидной структуры будем вести из следующих соображений. Пусть мы имеем некоторое распределение вероятностей числа посторонних ветвей древовидной структуры в позиции $i-1$:

$$P_{i-1}(k_{i-1}) = f(k_{i-1}), k_{i-1} \in_N, \quad (3)$$

где k_i-1 – число посторонних сообщений в древовидной структуре с индексом $i-1$. Тогда посторонние сообщения в позиции i будут ветвями длиной 1, присоединёнными к сообщению источника с индексом $i-1$ и блоками, присоединёнными к этим k_i-1 блокам. Число первых будет распределено по закону Пуассона с интенсивностью $2^{-H} \cdot K$, где H – длина кода аутентификации в сообщении, переданному от отправителя, K – отношение общего числа переданных по каналу связи сообщений к числу сообщений n, переданному от отправителя:

$$P_i^{\langle 0\rangle} = \frac{(K\cdot 2^{-H})^i}{i!} e^{-K\cdot 2^{-H}}. \quad (4)$$

В общем случае с некоторой погрешностью параметр K может рассматриваться как число взаимодействующих в распределённой системе компонентов.

Распределения числа вторых получим на основании следующих рассуждений. Распределение числа сообщений, присоединённых к первому из k_i-1 сообщений:

$$P_{j,i-1}^{\{1\}} = P_{i-1}(1) \frac{(K\cdot 2^{-H})}{j} e^{-K\cdot 2^{-H}}. \quad (5)$$

Аналогично для второго:

Распределение числа сообщений, присоединённых к первому из k_i-1 сообщений:

$$P_{j,j-1}^{\{2\}} = P_{i-1}(2) \frac{(K\cdot 2^{-H})}{j} e^{-K\cdot 2^{-H}} \quad (6)$$

Распределение числа сообщений, присоединённых к двум данным:

$$P_{j,i-1}^{\{1,2\}} = \sum_{k=0}^{j} P_k^{\{1\}} P_{j-k}^{\{2\}}. \quad (7)$$

Соответственно, получаем рекуррентную формулу для распределения числа сообщений, присоединённых к v сообщениям с индексом $i-1$:

$$P_{j,i-1}^{\{1,\dots v\}} \quad \sum_{l=0}^{j} P_l^{\{v\}} P_{j-l}^{\{v-1\}} \quad P$$

Из этого получаем рекуррентную формулу для числа посторонних сообщений с определённым индексом

$$P_i(k_i) = \sum_{l=0}^{ki} P_l^{\{1,\dots\infty\}} P_{k_i-l}^{\langle 0\rangle},$$
$$P_0(k_0) \frac{(K\cdot 2^{-H})^{k_0}}{k_0!} e^{-K\cdot 2^{-H}}. \quad (9)$$

Данные формулы получены без учёта возможности ограничения множества обрабатываемых сообщений. Если же таковое вводится, тогда, с учётом того, что у посторонних сообщений индексы случайны, снижается интенсивность поступления сообщений в формуле (4) и становится равной $K \cdot W_{back}/n$ [12]. Формула (9) в результате приобретёт следующий вид:

$$P_i(k_i) = \sum_{l=0}^{ki} P_l^{\{1,\dots\infty\}} P_{k_i-l}^{\langle 0\rangle},$$
$$P_0(k_0) \frac{(\frac{K\cdot 2^{-H}\cdot W_{back}}{n})^{k_0}}{k_0!} e^{\frac{K\cdot 2^{-H}\cdot W_{back}}{n}}. \quad (10)$$

Результаты и их обсуждения. Численные значения вероятностей формирования определённого числа ветвей, содержащих посторонние сообщения, в древовидной структуре (рис. 1) для одного набора значений длины кода поля аутентификации H, длины цепочки n и параметра K сообщений приведены в таблице 1.

Отмечено, что при теоретически определённой в [20] длине кода аутентификации $H > \log_2 K$ начиная с порядкового номера сообщения i = 4…6 изменения вероятностей формирования посторонних ветвей $P_i(k_i)$ меняются незначительно. Тогда считаем, что $P_i(a) \approx P_{i+1}(a)$, a – натуральное число, $i > 7$.

Таблица 1 – Численные значения вероятностей формирования определённого числа ветвей ($H = 7$, $n = 15$, $K = 30$)

		Порядковый номер сообщения в цепочке								
		1	2	3	4	5	6	7	8	9
Число посторонних ветвей	0	0,79	0,75	0,74	0,74	0,74	0,74	0,74	0,74	0,74
	1	0,18	0,21	0,21	0,21	0,22	0,22	0,22	0,22	0,22
	2	0,02	0,03	0,03	0,03	0,03	0,04	0,04	0,04	0,04
	3	$1{,}69\cdot10^{-3}$	$3{,}87\cdot10^{-3}$	$4{,}42\cdot10^{-3}$	$4{,}55\cdot10^{-3}$	$4{,}58\cdot10^{-3}$	$4{,}59\cdot10^{-3}$	$4{,}59\cdot10^{-3}$	$4{,}59\cdot10^{-3}$	$4{,}59\cdot10^{-3}$
	4	$9{,}94\cdot10^{-5}$	$3{,}87\cdot10^{-4}$	$4{,}67\cdot10^{-4}$	$4{,}87\cdot10^{-4}$	$4{,}91\cdot10^{-4}$	$4{,}93\cdot10^{-4}$	$4{,}93\cdot10^{-4}$	$4{,}93\cdot10^{-4}$	$4{,}93\cdot10^{-4}$

Из данных вероятностей можно определить высоту матрицы регистров (её ширина равна длине цепочки сообщений n), которая обеспечивала бы размещение ветвей древовидной структуры с требуемой вероятностью возникновения ошибки переполнения, то есть ситуации, при которой число сформировавшихся посторонних ветвей превышает число регистров получателя, предназначенных для их хранения. Необходимо определить такое число b, при котором вероятность ошибки не превышает значение P^{ERR}:

$$1 - \sum_{j=0}^{b} P_i(j) < P^{ERR}, i > 7(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}. \quad (11)$$

Результаты, полученные для одного набора значений длины цепочки сообщений, приведены в таблице 2.

Таблица 2 – Необходимое число регистров для хранения элементов посторонних ветвей ($n = 15$, $P^{ERR} = 10^{-2}$)

$H\backslash K$	2	5	13	25	40	60	80	110	140	170	200	240
5	1	3	5	14	15	15	25	37	42	71	86	117
6	1	2	3	3	4	4	4	9	13	14	19	24
7	1	1	2	2	2	2	2	3	3	3	2	4
8	1	1	1	1	1	1	2	2	2	2	2	2
9	1	1	1	1	1	1	1	1	1	1	1	1

Снижение параметра W_{back} уменьшает интенсивность добавления сообщений в древовидную структуру, что выражается в снижении требуемого числа регистров хранения. За счёт ограничения множества обрабатываемых сообщений уменьшается количество посторонних ветвей, благодаря этому снижаются затраты памяти приемника.

Зависимость требуемого числа регистров для хранения описателей древовидной структуры, формируемой в приёмнике, от длины поля кода аутентификации H и отношения K общего числа переданных сообщений к числу сообщений, переданному от отправителя, приведена на рисунке 2. Видно, что в области $H \approx \boldsymbol{log_2}\ K$ наблюдается кратное снижение (в 3–4 раза) требуемого числа регистров (до 5 … 10), что делает возможной реализацию рассматриваемой схемы хранения древовидной структуры в целевом классе устройств – высокоавтономных вычислителях.

Другим следствием снижения числа обрабатываемых сообщений является возможность уменьшения размера поля кода аутентификации сообщения. Для сообщений длиной в несколько десятков битов уменьшение его на 1–2 бита приводит к повышению пропускной способности канала связи, повышению автономности радиопередающей аппаратуры и снижению вероятности коллизий в канале связи.

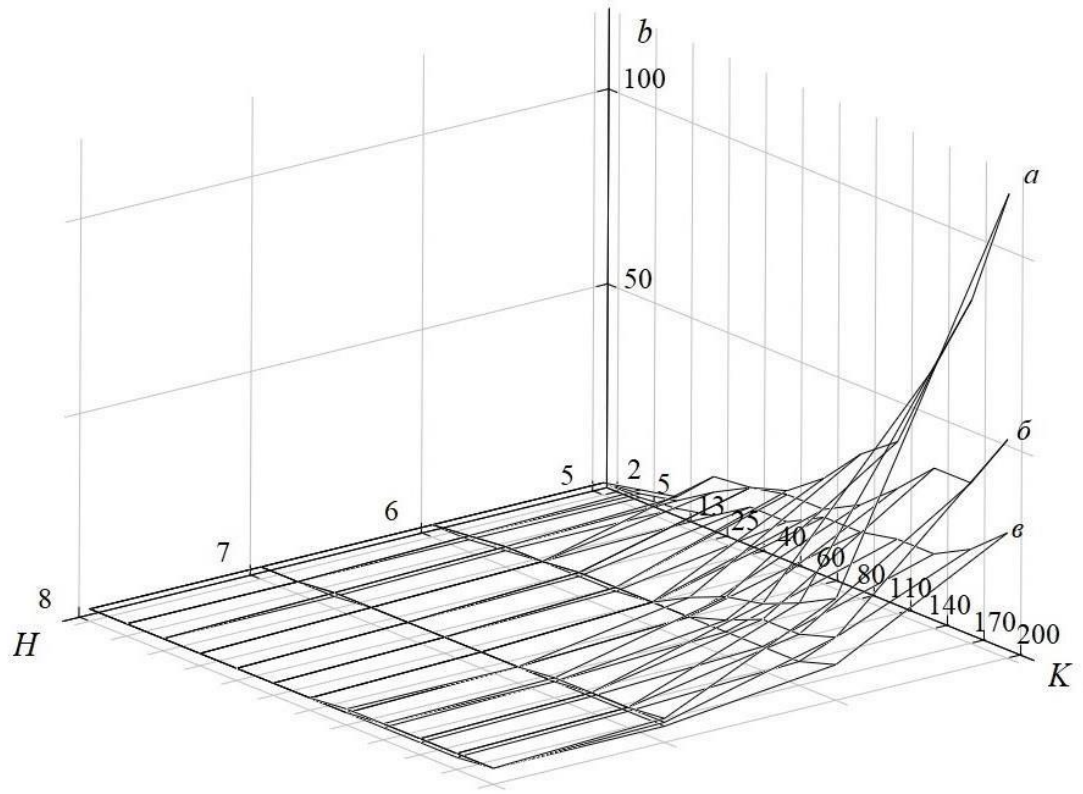


Рисунок 2 – Зависимость затрат памяти на обработку зависимости от размера структурированного множества информационных блоков и параметра обработки сообщений W_{back}: *а*) $W_{back} = n$; *б*) $W_{back} = 0{,}6 \cdot n$; *в*) $W_{back} = 0{,}3 \cdot n$

Заключение. Проведённые исследования позволили установить зависимости между параметрами обработки кодов аутентификации и требуемым объёмом внутренней памяти приёмника, что позволяет синтезировать приёмники, отличающиеся, с одной стороны, отсутствием избыточных ресурсов при известных параметрах работы системы дистанционного мониторинга и управления, а с другой стороны, обеспечением низкой вероятности нехватки ресурсов для обработки сообщений. Использование метода ограничения числа обрабатываемых сообщений, в основе которого лежит использование свойств потока сообщений от отправителя к приёмнику, позволяет снизить в 3–4 раза требуемый объём памяти приёмника и уменьшить на 1–2 бита размер кода аутентификации на теоретически определённой границе применимости методов кодирования в режиме сцепления блоков для аутентификации удалённых источников. Кроме того, результаты, полученные на рассмотренной модели, подтвердили полученную в более ранних исследованиях экспоненциальную зависимость количества посторонних ветвей от изменения множества обрабатываемых сообщений.

Библиографический список

1. Rezenkov, R. N. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication / R. N. Rezenkov, V. P. Pashintsev, P. A. Zhuk, M. I. Kalmykov // International Journal of Mechanical Engineering and Technology (IJMET). – 2018. – Vol. 9, № 5. – P. 958–965.

2. Domin, K. Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol / K. Domin // Engineering Secure Software and Systems. – 2016. – P. 198–204. – DOI: 10.1007/978-3-319-94496-8_7.

3. Чистоусов, Н. К. Модификация метода аутентификации низкоорбитальных спутников на основе кодов полиномиальной системы классов вычетов / Н. К. Чистоусов, И. А. Калмыков, Д. В. Духовный [и др.] // Современные наукоемкие технологии. – 2022. – № 2. – С. 164–169. – DOI: 10.17513/snt.39052.

4. Wei, Liang. A distributed data secure transmission scheme in wireless sensor network / Wei Liang, Yin Huang, Jianbo Xu and Songyou Xie // International Journal of Distributed Sensor Networks. – 2017. – Vol. 13, issue 4, 155014771770555. – DOI: 10.1177/1550147717705552.

5. Black, J. CBC MACs for arbitrary-length messages: The three-key constructions / J. Black, P. Rogaway // J. Cryptol. – 2015. – Vol. 18, № 2. – P. 111–131.

6. Stallings, W. NIST Block Cipher Modes of Operation for Confidentiality / W. Stallings // Cryptologia. – 2010. – № 34 (2) – P. 163–175.

7. Fangfang, Dai. From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues / Fangfang Dai, Yue Shi, Nan Meng, Liang Wei and Zhiguo Ye // The 2017 4th International Conference on Systems and Informatics (ICSAI 2017). – Hangzhou, China, 2017.

8. Dworkin, M. Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality / M. Dworkin // Nist Spec. Publ. – 2004. – Vol. 800. – P. 38.

9. Iwata, T. OMAC: one-key CBC MAC / T. Iwata, K. Kurosawa // Fast Software Encryption. – 2003. – P. 129–153.

10. Liu, C. Implementation of DES Encryption Arithmetic based on FPGA / C. Liu, J. Ji, Z. Liu // AASRI Procedia. – 2013. – Vol. 5. – P. 209–213.

11. Ben Othman, S. An efficient secure data aggregation scheme for wireless sensor networks / S. Ben Othman, H. Alzaid, A. Trad & H. Youssef // IISA. – 2013. – DOI: 10.1109/iisa.2013.6623701.

12. Таныгин, М. О. Метод ограничения множества обрабатываемых приёмником блоков данных для повышения достоверности операций определения их источника / М. О. Таныгин, О. Г. Добросердов, А. О. Власова, А. А. А. Ахмад // Труды МАИ. – 2021. – № 118. – DOI: 10.34759/trd-2021-118-14.12.

13. Goursaud, Claire. Dedicated networks for IoT: PHY/MAC state of the art and challenges / Goursaud Claire, Gorce Jean-Marie. // EAI endorsed transactions on Internet of Things. – 2015.

14. Sant, Deepak. Throughput of Unslotted ALOHAChannels with Arbitrary Packet Interarrival Time Distributions / Sant Deepak // IEEE Transactions on Communications. – 1980. – Vol. 28, № 8. – P. 1422–1425.

15. Khorov, Evgeny. Testbed to Study the Capture Effect: Can we Rely on this Effect in Modern Wi-Fi Networks / Evgeny Khorov, Aleksey Kureev, Ilya Levitsky, Andrey Lyakhov // 2018 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). – 2018.

16. Bankov, Dmitry. LoRaWAN Modeling and MCS Allocation to Satisfy Heterogeneous QoS Requirements / Dmitry Bankov, Evgeny Khorov, Andrey Lyakhov // Sensors. – 2019. – Vol. 19, № 19. – P. 1–23.

17. Алшаиа, Х. Я. Принципы организации буферной памяти специализированного приёмника, определяющего источник поступающих данных / Х. Я. Алшаиа // Распознавание – 2021 : XVI Международная научно-техническая конференция. – Курск, 2021. – С. 44–46.

18. Таныгин, М. О. Сложность алгоритма определения источника данных / М. О. Таныгин, Х. Я. Алшаиа, А. В. Митрофанов // Труды МАИ. – 2021. – № 117. – DOI: 10.34759/trd-2021-117-12.

19. Алшаиа, Х. Я. Метод и алгоритм обработки данных на основе идентификаторов в специализированном вычислительном устройстве : дис. … канд. техн. наук : 05.13.05 / Хайдер Яхья Атоун Алшаиа. – Курск, 2021. – 138 с.

20. Таныгин, М. О. Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера / М. О. Таныгин. – Курск : Закрытое акционерное общество «Университетская книга», 2020. – 198 с.

21. Губарев, А. В. Моделирование работы системы контроля подлинности командных слов / А. В. Губарев // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 4. – С. 169–175.

22. Губарев, А. В. Описание функциональной схемы устройства определения подлинности передаваемых командных слов / А. В. Губарев // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение – 2014. – № 4 – С. 22–30.

23. Мальчуков, А. Н., Система автоматизированного проектирования кодеков помехоустойчивых кодов короткой длины / А. Н. Мальчуков, А. Н. Осокин // Известия Томского политехнического университета. – 2008. – Т. 312, № 5. – С. 70–75.

24. Мыцко, Е. А. Исследование алгоритмов вычисления контрольной суммы CRC8 в микропроцессорных системах при дефиците ресурсов / Е. А. Мыцко, А. Н. Мальчуков, С. Д. Иванов // Приборы и системы. Управление, контроль, диагностика. – 2018. – № 6. – С. 22–29.

25. Panagiotis, Papadimitratos. Secure message transmission in mobile ad hoc networks / Panagiotis Papadimitratos, Zygmunt J. Haas // Ad Hoc Networks. – 2003 – № 1. – P. 193–209.

References

1. Rezenkov R. N., Pashintsev, V. P., Zhuk, P. A., Kalmykov, M. I. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. *International Journal of Mechanical Engineering and Technology (IJMET)*, 2018, vol. 9, no. 5, pp. 958–965.

2. Domin, K. Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol. *Engineering Secure Software and Systems*, 2016, pp. 198–204. DOI: 10.1007/978-3-319-94496-8_7.

3. Chistousov, N. K., Kalmykov, I. A., Dukhovny, D. V. [et al.] Modifikatsiya metoda autentifikatsii nizkoorbitalnykh sputnikov na osnove kodov polinomialnoy sistemy klassov vychetov [Modification of the authentication method of low-orbit satellites based on the codes of the polynomial system of deduction classes] *Sovremennye naukoemkie tekhnologii* [Modern Science-Intensive Technologies], 2022, no. 2, pp. 164–169. DOI 10.17513/snt.39052.

4. Wei Liang, Yin Huang, Jianbo Xu and Songyou Xie A distributed data secure transmission scheme in wireless sensor network. *International Journal of Distributed Sensor Networks*, 2017, vol. 13, issue 4, 155014771770555. DOI: 10.1177/1550147717705552.

5. Black, J. CBC MACs for arbitrary-length messages: The three-key constructions. *Cryptol*, 2015, vol. 18, no. 2, pp. 111–131.

6. Stallings, W. NIST Block Cipher Modes of Operation for Confidentiality. *Cryptologia*, 2010, no. 34 (2), pp. 163–175.

7. Fangfang, Dai, Yue, Shi, Nan, Meng, Liang, Wei and Zhiguo, Ye. From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues. *The 2017 4th International Conference on Systems and Informatics (ICSAI 2017)*. Hangzhou, China, 2017.

8. Dworkin, M. Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. *Nist Spec. Publ*., 2004, vol. 800, p. 38.

9. Iwata, T., Kurosawa, K. OMAC: one-key CBC MAC. *Fast Software Encryption*, 2003, pp. 129–153.

10. Liu, C., Ji, J., Liu, Z. Implementation of DES Encryption Arithmetic based on FPGA. *AASRI Procedia*, 2013, vol. 5, pp. 209–213.

11. Ben, Othman, S., Alzaid, H., Trad, A., & Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks. *IISA*, 2013. DOI:10.1109/iisa.2013.6623701.

12. Tanygin, M. O., Dobroserdov, O. G., Vlasova, A. O., Akhmad, A. A. Metod ogranicheniya mnozhestva obrabatyvaemykh priyomnikom blokov dannykh dlya povysheniya dostovernosti operatsiy opredeleniya ikh istochnika [The method of limiting the set of data blocks processed by the receiver to increase the reliability of operations for determining their source]. *Trudy MAI* [Proceedings of MAI], 2021, no. 118. DOI 10.34759/trd-2021-118-14.12.

13. Goursaud, Claire, Gorce, Jean-Marie. Dedicated networks for IoT: PHY/MAC state of the art and challenges. *EAI endorsed transactions on Internet of Things*, 2015.

14. Sant, Deepak. Throughput of Unslotted ALOHA Channels with Arbitrary Packet Interarrival Time Distributions. *IEEE Transactions on Communications*, 1980, vol. 28, no. 8, pp. 1422–1425.

15. Khorov, Evgeny, Kureev, Aleksey, Levitsky, Ilya, Lyakhov, Andrey. Testbed to Study the Capture Effect: Can we Rely on this Effect in Modern Wi-Fi Networks. *2018 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) IEEE*, 2018.

16. Bankov, Dmitry, Khorov, Evgeny, Lyakhov, Andrey. LoRaWAN Modeling and MCS Allocation to Satisfy Heterogeneous QoS Requirements. *Sensors*, 2019, vol. 19, no. 19, pp. 1–23.

17. Alshaia, H. Ya. Printsipy organizatsii bufernoy pamyati spetsializirovannogo priyomnika, opredelyayushchego istochnik postupayushchikh dannykh [Principles of organization of buffer memory of a specialized receiver that determines the source of incoming data]. *Raspoznavanie – 2021* : *XVI Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya* [Recognition – 2021 : XVI International Scientific and Technical Conference]. Kursk, 2021, pp. 44–46.

18. Tanygin, M. O. *Slozhnost algoritma opredeleniya istochnika dannykh* [The complexity of the algorithm for determining the data source]. *Trudy MAI* [Proceedings of MAI], 2021, no. 117. DOI 10.34759/trd-2021-117-12.

19. Alshaia, H. Ya. *Metod i algoritm obrabotki dannykh na osnove identifikatorov v specializirovannom vychislitelnom ustroystve* [Method and algorithm of data processing based on identifiers in a specialized computing device]. Kursk, 2021. 138 p.

20. Tanygin, M. O. *Teoreticheskie osnovy identifikatsii istochnikov informatsii, peredavaemoy blokami ogranichennogo razmera* [Theoretical foundations of identification of information sources transmitted by blocks of limited size]. Kursk, Closed Joint Stock Company "University Book", 2020. 198 p.

21. Gubarev, A. V. Modelirovanie raboty sistemy kontrolya podlinnosti komandnykh slov [Modeling of the authenticity control system of command words]. *Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy* [Problems of Information Security. Computer Systems], 2014, no. 4, pp. 169–175.

22. Gubarev, A. V. Opisanie funktsionalnoy skhemy ustroystva opredeleniya podlinnosti peredavaemykh komandnykh slov [Description of the functional scheme of the device for determining the authenticity of transmitted command words]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitelnaya tekhnika, informatika. Meditsinskoe priborostroenie* [News of South-West University. Series: Management, Computer Engineering, Computer Science. Medical Instrumentation], 2014, no. 4, pp. 22–30.

23. Malchukov, A. N., Osokin, A. N. Sistema avtomatizirovannogo proektirovaniya kodekov pomekhoustoychivykh kodov korotkoy dliny [System of computer-aided design of codecs of noise-resistant codes of short length]. *Izvestiya Tomskogo politekhnicheskogo universiteta* [Izvestiya of Tomsk Polytechnic University], 2008, vol. 312, no. 5, pp. 70–75.

24. Mytsko, E. A. Issledovanie algoritmov vychisleniya kontrolnoy summy CRC8 v mikroprotsessornykh sistemakh pri defitsite resursov [Investigation of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources] *Pribory i sistemy. Upravlenie, kontrol, diagnostika* [Devices and systems. Management, control, diagnostics], 2018, no. 6, pp. 22–29.

25. Panagiotis, Papadimitratos, Zygmunt J., Haas Secure message transmission in mobile ad hoc networks. *Ad Hoc Networks*, 2003, no. 1, pp. 193–209.

DOI 10.54398/20741707_2022_4_30
УДК 004.056.53

МОДЕЛЬ ОПРЕДЕЛЕНИЯ ИСТОЧНИКА СООБЩЕНИЙ НА ОСНОВЕ СТАТИСТИЧЕСКОГО АНАЛИЗА МЕТАДАННЫХ В ОТКРЫТОМ КАНАЛЕ СВЯЗИ

Статья поступила в редакцию 26.09.2022, в окончательном варианте – 29.09.2022.

Плугатарев Алексей Владимирович, Юго-Западный государственный университет, 305040, Российская Федерация, г. Курск, ул. 50 лет Октября, 94,
аспирант, ORCID: 0000-0002-8549-4382, e-mail: aplugatarev@bk.ru

Работа посвящена проблеме контроля аутентификации источников данных в распределенных информационных системах, использующих каналы связи с низкой пропускной способностью. Целью исследования является создание модели определения источника сообщений в устройстве-приёмнике, позволяющей на основе анализа характеристик распределения времени поступления сообщений повысить достоверность определения источника. Идентификация источника сообщений производится на основе статистического анализа значений метаданных. В данном исследовании метаданными являются интервалы времени между поступившими сообщениями. За основу модели взята известная модель системы поступления сообщений от множества источников в сетях LoRaWAN. Определение источника производилось с помощью методов кодирования в режиме сцепления блоков, которые обеспечивают более высокую достоверность идентификации для сообщений небольшой длины, характерных для указанного типа сетей. С помощью численного моделирования были определены закономерности изменения статистических характеристик времени поступления сообщений в случае возникновения ошибки идентификации. В результате сформулированы критерии принятия решения в случае невозможности проведения идентификации на основе обработки содержимого идентификационных полей. Итогом проведенных исследований являются выводы о возможности применения модели как средства повышения достоверности процедуры аутентификации, выполняемой для удалённого субъекта информационного обмена в условиях, когда использование обычных криптографических алгоритмов не даёт требуемую достоверность, а использование в сочетании с методами кодирования в режиме сцепления сообщений обеспечивает снижение вероятности возникновения ошибки по сравнению с методами, выполняющими идентификацию только по результатам обработки идентификаторов самих сообщений. Результат экспериментальных исследований показал возможность при помощи разработанной модели повысить достоверность определения аутентичности источника сообщений, снижения числа переспросов, возникающих при обнаружении ошибок, уменьшении размеров дополнительных полей идентификаторов в каждом сообщении.

Ключевые слова: удалённое взаимодействие, обработка информации, метаинформация, аутентификация

MODEL FOR DETERMINING THE MESSAGE SOURCE BY STATISTICAL ANALYSIS OF METADATA IN AN OPEN COMMUNICATION CHANNEL

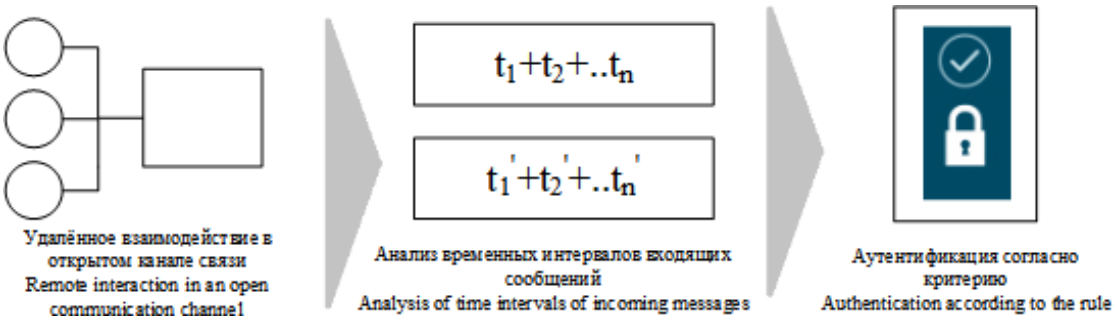
The article was received by the editorial board on 26.09.2022, in the final version – 29.09.2022.

Plugatarev Aleksey V., Southwestern State University, 305040, Russian Federation, Kursk, st. 50 years of October, 94.
post-graduate student, ORCID: 0000-0002-8549-4382, e-mail: aplugatarev@bk.ru

The paper is devoted to the issue of authenticity control of data transmitted via open communication channels. The study is aimed at building a model for determining the message source by the receiver, which allows for improving the source determination reliability by analyzing the message arrival time distribution characteristics. The message source is identified by statistically analyzing metadata, which herein are the time intervals between messages received. The metadata processing model is based on the well-known model for receiving messages from a target source in LoRaWAN networks. In this case, the source is determined by coding in the block chaining mode, which ensures higher identification reliability for small packets typical for the specified network type. The criteria have also been formulated for deciding when identification by processing the identification field contents is impossible. Studies have shown the efficiency of the source identification model within various ranges of message chain formation parameters. As a result of the study, an authentication model has been developed, based on the analysis of the message arrival time at the receiver. Using it in combination with coding in the message chaining mode reduces the error probability compared to the techniques performing identification by only processing identifiers of the messages themselves. The experimental study results have shown that the model developed allows improving the message source authenticity determination reliability and reducing negative acknowledgment occurring in the case of error and the size of additional identifier fields in each message.

Keywords: remote interaction, information processing, meta-information, authentication

Graphical annotation (Графическая аннотация)



Введение. Высокий темп развития информационных технологий, повсеместный переход на электронные формы хранения и передачи информации, а также тенденции к автоматизации всевозможных технологических процессов способствуют тому, что безопасность информационных сетей, сетевых сервисов и распределённых систем становится проблемой всё большего числа различных пользователей и организаций.

В вышеупомянутых системах в процессе взаимодействия устройств [1], как правило, требуется процедура проверки подлинности. Для этого проектируются механизмы аутентификации. Традиционным методом определения источника поступающих в приёмник информационных сообщений является введение в состав таких сообщений специальных полей, содержащих в явном или закодированном виде идентификатор источника. В сетевых протоколах, где размер единицы взаимодействия составляет несколько килобайт, а один – два байта дополнительной информации незначительно скажутся на общем объёме информации, то для протоколов, в которых размер блока ограничен несколькими десятками байтов, дополнительные поля будут оказывать существенное влияние на пропускную способность канала [2, 3]. Как следствие, вопрос исследования, механизмов аутентификации в распределённых системах с низкой пропускной способностью актуален, так как возникает проблема экономии ресурсов системы без понижения точности процедуры аутентификации [4].

Цель данной работы – создание модели контроля аутентичности сообщений, передаваемых по открытым каналам связи в распределённых системах, которая позволяет на основе анализа характеристик распределения времени поступления сообщений повысить достоверность определения источника. Основой исследования служит гипотеза о возможности использования таких характеристик распределения, как коэффициенты асимметрии и эксцесса для корректной идентификации несанкционированных сообщений на основе анализа временных задержек между ними.

Методы и материалы. Рассмотрим систему с открытым каналом связи, в которой взаимодействует множество устройств, среди которых целевой источник сообщений и приёмник информации. Задача приёмника в данной модели – контролировать аутентичность, целостность и порядок следования всех поступающих сообщений от целевого источника. Схема взаимодействия представлена на рисунке 1.

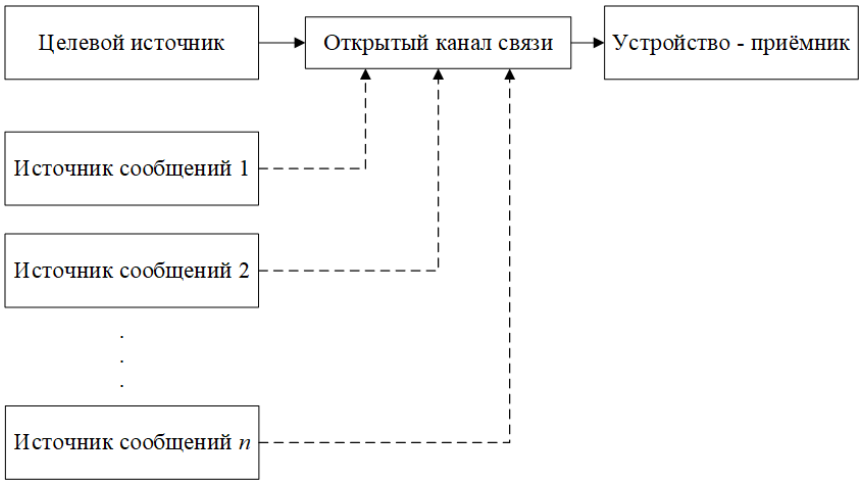


Рисунок 1 – Схема взаимодействия устройств в информационной системе

Целевой источник сообщений, генерируя единицы сетевого взаимодействия с устройствами, добавляет к ним значение хеш-функции от этого сообщения, на приёмной стороне также вычисляется значение хеш-функции от полученного сообщения [5, 6]. Имитовставка каждого поступившего сообщения сравнивается с имитовставкой (хешем) всех уже принятых сообщений. Условием для включения сообщения в последовательность является полное равенство хеша (имитовставки), сформированного из данных предыдущего блока цепочки содержимого [7, 8].

Рассмотрим модель, в которой на некоторый промежуток времени на устройство-приёмник, поступает множество сообщений. На первом этапе в буфере данных формируется цифровое представление сформированных последовательностей сообщений в виде графа временного сеанса $G = \{V,R\}$, в котором V – множество сообщений, поступивших на приёмник, а R – множество значений временных задержек между сообщениями из множества V. При этом сообщения, в которых не выполняются условия равенства значений имитовставки, не включаются во множество вершин графа. Новое сообщение, полученное приёмником n_i, добавляет вершину v_i в множество V, соединённую с ребром $(v,\ v')$ из множества R, если имитовставки n_i и любого другого сообщения n полностью совпадают. Вес получившегося ребра графа, равный временному интервалу между соответствующими сообщениями, определяется по следующей формуле:

$$r_{v_i - v_{i-1}} = t(v_i) - t(v_{i-1}) . \quad (1)$$

На начальном этапе функционирования системы необходимо определить параметр N, длину графа сеанса – значение длины последовательности тех цепочек сообщений, которые будут проходить проверку аутентичности.

В буферном хранилище приёмника содержится представленная в виде матрицы расстояний информация об ориентированном графе. Матрица расстояний в получившемся графе сеанса с длиной цепочки n в общем виде будет выглядеть следующим образом:

$$M = \{ \begin{matrix} r_{00}\, r_{01} \dots r_{0n} \\ r_{10}\, r_{11} \dots r_{1n} \\ \dots \\ r_{m0}\, r_{m1} \dots r_{mn} \end{matrix} \}. \quad (2)$$

Значение каждого элемента (2) r_{kl} – временной интервал между поступлениями на приёмник сообщения с индексом l и k. Если в графе присутствует только одна последовательность сообщений длиной N, все сообщения цепочки считаются аутентифицированными, и их можно отправить на дальнейшую обработку в системе.

В ситуации, когда с каждым новым поступившем сообщением однозначно определяется его принадлежность к целевому источнику, информация из первого столбца и первой строки удаляется и дополняется строкой с индексом n и столбцом с индексом n (в таком случае содержимое матрицы не меняется). Как только появляется сообщение, которое невозможно однозначно идентифицировать, матрица изменяется лишь добавлением строк и столбцов, до тех пор, пока в графе не образуется два идущих подряд однозначно определённых отдельных сообщения. Таким образом, размер матрицы (2) динамичный. В ситуации, когда в буфер приёмника попадают только однозначно аутентифицированные сообщения, размер матрицы составляет N x N, где N – параметр длины графа сеанса.

После того как приёмник получил несколько идущих целевых сообщений, необходимо выделить все последовательности сообщений длиной N. Графически это представлено на рисунке 2, для наглядности с N = 5.

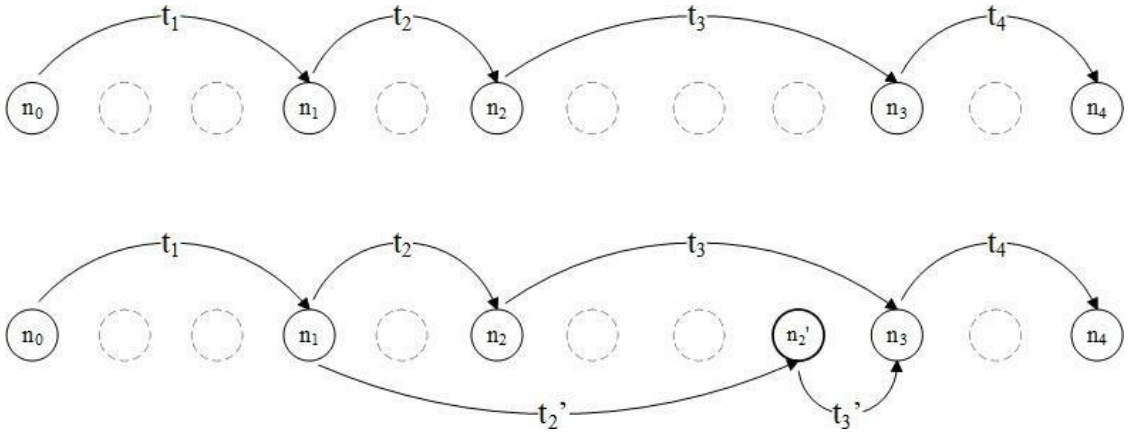


Рисунок 2 – Графическое отображение примеров рядов сообщений на приёмнике

На рисунке 2 представлены две ситуации. Пунктирными вершинами обозначены сообщения, пришедшие не от целевого источника и не нуждающиеся в обработке. На верхнем рисунке существует однозначная последовательность сообщений длиной $N = 5$. Это означает, что все сообщения n_0-n_1-n_2-n_3-n_4 отправлены от целевого источника и их необходимо отправить на дальнейшую обработку. Иная ситуация на нижнем рисунке. Между сообщениями n_1 и n_3 на приёмник пришли два сообщения с совпадающими имитовставками n_2 и n_2'. Таким образом, получается, что необходимо сравнить две выборки чисел $t_1t_2t_3t_4$ и $t_1t_2't_3't_4$ и определить аутентичную.

Следовательно, в вышеописанной модели возникает задача сравнения нескольких одинаковой длины небольших числовых последовательностей, различающихся несколькими (1…3) элементами. Из того факта, что устройства-источники в системе генерируют сообщения по модели типа ALOHA, можно сделать вывод, что значения временных интервалов будут иметь свои характеристики распределения [9].

В работах [10] исследуются характеристики моментов высоких порядков для классификации различных законов распределения, в том числе по коэффициентам асимметрии и эксцесса [11]. В данных работах исследуются возможности идентификации типа распределения и его параметров, используя информацию о первых четырех выборочных моментах, с применением линейных преобразований сдвига и масштаба. Выводы, полученные в результате исследований однородности случайных выборок [12] и аномальных значений выборки, полученных из наборов выборок [13], позволили выдвинуть гипотезу о возможности использования таких характеристик распределения, как коэффициенты асимметрии и эксцесса, для корректной идентификации несанкционированных сообщений.

Численное моделирование. Для проверки гипотез об использовании характеристик распределения высокого порядка были использованы математические модели, учитывающие реальные особенности проектирования информационных систем LoRaWAN, которые были изложены в работах [14, 15]. В данных работах применяется распространённый подход к моделированию метода доступа - по модели типа ALOHA [16] обобщается на случай множества виртуальных каналов. В данных работах предполагается, что сообщения в сети генерируются согласно пуассоновскому процессу, разделяемому между несколькими виртуальными коммутационными каналами. В описываемой модели передача данных происходит в режиме с подтверждениями, а также вместе с методом повторных передач с наличием эффекта захвата канала.

В данном исследовании, аналогично другим работам, которые посвящены технологии LoRaWAN [14, 18, 19], рассматривается следующий сценарий работы сети LoRaWAN. В беспроводной сенсорной сети LoRaWAN, в которой группа из S устройств-источников передаёт на приёмник сообщения по коммутационному каналу, количество сенсоров в сети – до 10000. Для передачи сообщений сенсоры-источники используют сигнально-кодовые конструкции, а задачей приёмника является определение аутентичности сообщений от целевого источника [19].

Анализ данных для определения решающего правила успешной аутентификации для цепочки сообщений по выборочным коэффициентам асимметрии и эксцесса удобно начать с помощью графика, на котором в общей системе координат горизонтальная ось – коэффициент асимметрии, вертикальная – коэффициент эксцесса. Для примера представлена общая тенденция поведения значений в общей системе координат с параметрами $S = 100$, $N = 30$.

На рисунке 3 слева в общей системе координат представлено множество значений, рассчитанных для цепочек целевых источников, а на рисунке справа – значения аналогичных последовательностей, в которых была заменена одна единица сетевого взаимодействия. Временной интервал в таком случае вычислялся следующим образом:

$$t_i' = random(0;\ t_i + t_j) \quad (3)$$

$$t_j' = (t_i + t_j) - t_i \quad (4)$$

В данных формулах t_i' – временной интервал между посторонним сообщением и последним однозначно аутентифицированным сообщением (аналог t_2' на рисунке 2), а t_j' – временной интервал между последующим однозначно аутентифицированным сообщением и посторонним сообщением (аналог t_3' на рисунке 2). В свою очередь, t_i – временной интервал между целевым сообщением, параллельно которому приходит постороннее сообщение, и последним однозначно аутентифицированным сообщением (аналог t_2 на рисунке 2), t_j – временной интервал между последующим однозначно аутентифицированным сообщением и целевым сообщением, параллельно которому приходит постороннее сообщение (аналог t_3 на рисунке 2). *Random* – функция выбора случайной величины в указанном диапазоне по закону равномерного распределения.

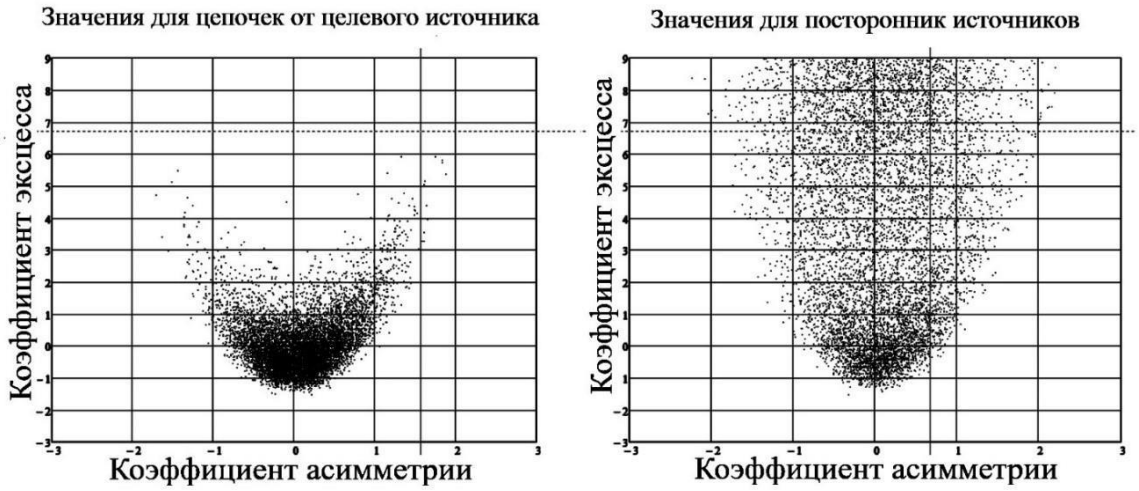


Рисунок 3 – Примеры значений эксцесса и коэффициента асимметрии для целевых и посторонних цепочек сообщений

Из рисунка 3 можно сделать вывод, что коэффициент эксцесса может выступать в качестве критерия для аутентификации данной модели и что существуют участки координатной плоскости, в которых значения коэффициентов ведут себя определённым образом. Проведённые исследования показали возможность использования сравнения коэффициентов асимметрии и эксцесса для аутентификации в распределённых сетях, а именно прослеживается их уменьшение при замене нескольких элементов во множестве задержек.

В ходе численных экспериментов было установлено, что существуют ситуации, в которых коэффициент асимметрии и коэффициент эксцесса для посторонней цепочки сообщений почти гарантировано уменьшаются по сравнению с целевой цепочкой. Доля попадания в данный доверенный интервал зависит от выбранных критериев. В качестве критерия был выбран множитель m для условия:

$$(|\ K_э\ | > |\ m\ \cdot K'_э\ |). \qquad (5)$$

В данном условии $K_э$ – коэффициент эксцесса, рассчитанный для целевой цепочки сообщений, а $K'_э$ – коэффициент эксцесса, рассчитанный для аналогичной цепочки с посторонним сообщением. Таким образом, выполнение условия (5) указывает на принадлежность цепочки сообщений к целевому источнику.

Как видно из рисунка 4, наиболее оптимальными принимаются значения, когда коэффициент эксцесса посторонней цепочки больше в два раза, чем коэффициент целевой цепочки.

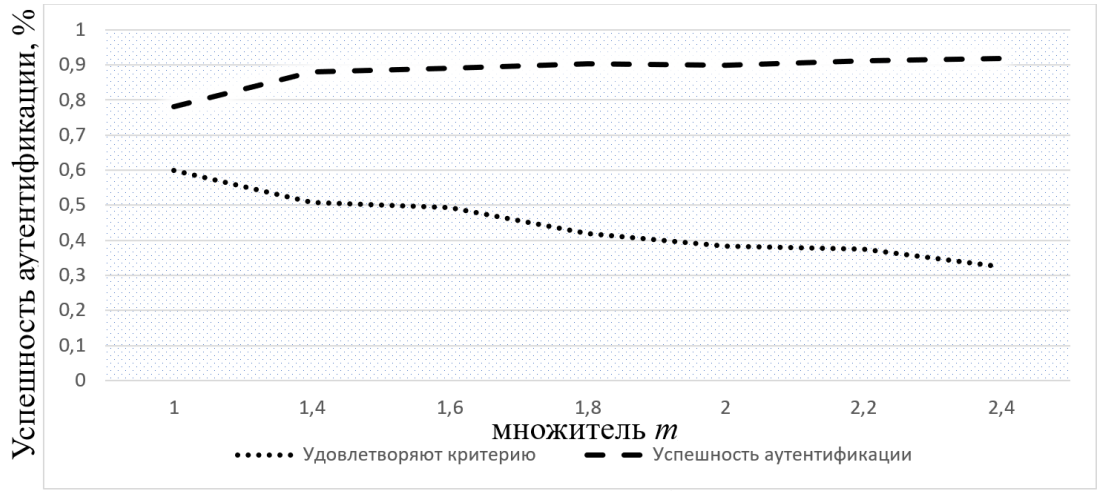


Рисунок 4 – Зависимость успешной аутентификации от выбранных критериев

Доля успешной аутентификации зависит от количества устройств в сети. Результаты данной зависимости представлены в таблице, моделирование проводилось при условии ($|\ K_э\ | > |\ 2\ \cdot K'_э|$) и N = 30.

Таблица – Значения успешной аутентификации для различного количества устройств в сети

S, кол-во устройств, шт	**5**	**10**	**15**	**20**	**25**	**35**	**40**	**50**	**200**	**500**	**1000**	**10^4**
Успешная аутентификация, %	70	73	77	78	81	86	90	91,4	93	94, 8	95,9	97,5

В ходе численных экспериментов, как можно наблюдать в таблице, было установлено, что резкий рост успешной аутентификации в сети идёт до показателя $S = 40$. При этом рост успешной аутентификации продолжается с увеличением количества устройств в сети, но намного медленнее.

Результаты и их обсуждение. Результаты численного моделирования показали, что наилучшее обнаружение целевой цепочки сообщений достигается при использовании следующего правила:

$$auth = (K_A > K_A') \; and \; (|K_Э| > |2 \cdot K_Э'|), \quad (6)$$

где $K_Э$ и $K_Э'$ – коэффициенты асимметрии и эксцесса, рассчитанные для цепочки сообщений, определенной в качестве целевой по рассматриваемой методике; $K_Э$ и $K_Э'$ – коэффициенты асимметрии и эксцесса, рассчитанные для несанкционированной цепочки сообщений.

Другими словами, в ситуациях, где из двух цепочек, у которых коэффициент эксцесса одной цепочки больше более чем в два раза коэффициента другой цепочки (таких ситуаций около 40 % (рис. 4)) целевая цепочка сообщений та, в которой коэффициенты эксцесса и асимметрии больше. Ниже на рисунке 5 представлены зависимости успешной аутентификации и попадания в доверительный интервал относительно длины цепочки N при $S = 40$.

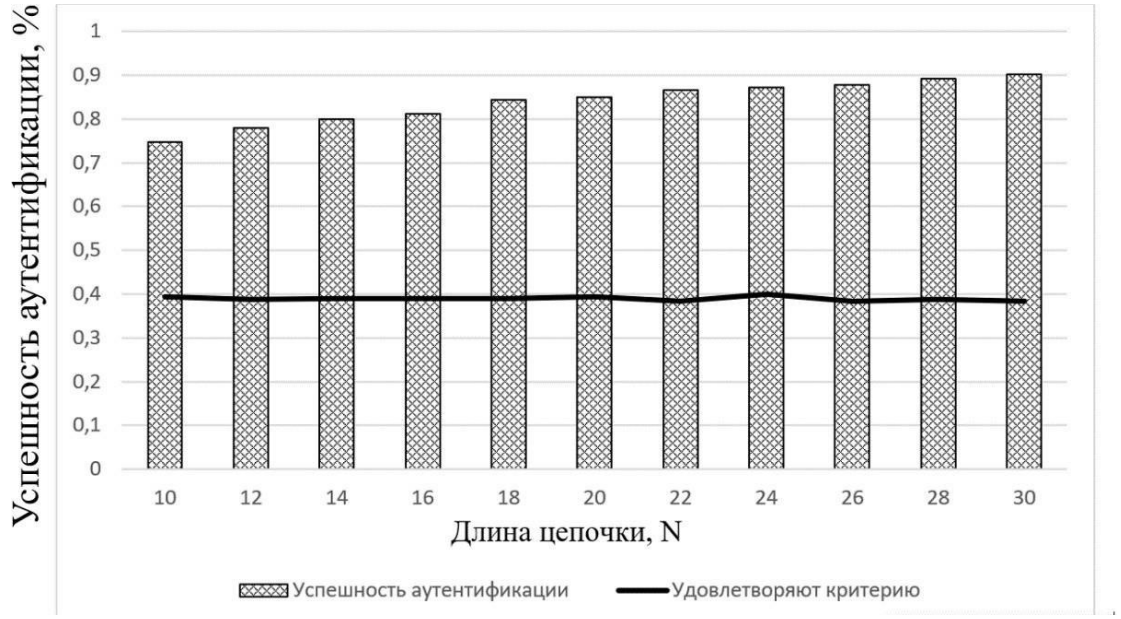


Рисунок 5 – Значения успешной аутентификации

На рисунке 5 показана доля успешных аутентификаций и доля ситуаций, подходящих под критерий (5). Из графика видно, что тенденция к возрастанию успешности аутентификации достигает вероятности 0,9 при $N = 30$, а доля ситуаций, удовлетворяющих критерию при значении $m = 2$, не меняется. Максимальной эффективности алгоритм в распределённой сети устройствами достигает начиная с последовательности длиной $N = 30$, вне зависимости от количества устройств.

Заключение. В данной работе была предложена методика повышения надежности определения источника цепочки сообщений по открытому каналу связи. Описанный метод позволяет увеличить вероятность определения источника на основе временных интервалов между поступлением сообщений к устройству-приёмнику, в случае неопределённости криптографическими протоколами между двумя или более вариантами групп сообщений. Результаты проведённых исследований и численное моделирование позволяет утверждать, что использование времени поступления сообщения в качестве метаданных для повышения вероятности определения источника и модель оценки выборки с использованием моментных характеристик высокого порядка (таких как коэффициенты асимметрии и эксцесса), позволяют уменьшить результирующую ошибку, определенную для используемых протоколов аутентификации, около 40 %.

Предложенный метод предполагается для использования как вспомогательный метод для алгоритмов аутентификации данных в информационных системах, в которых наложенные ограничения не позволяют достичь приемлемой для системы достоверности. Использование анализа метаданных может принести практическую пользу, которая может заключаться в уменьшении размера кода аутентификационных сообщений на несколько бит, что наиболее актуально для протоколов связи с низкой пропускной способностью.

Библиографический список

1. Марухленко, А. Л. Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации / А. Л. Марухленко, А. В. Плугатарев, М. О. Таныгин, Л. О. Марухленко, М. Ю. Шашков // Известия Юго-Западного государственного университета. – 2020. – Т. 24, № 2. – С. 108–121.

2. Capuzzo, Martina. Mathematical Modeling of LoRaWAN Performance with Bi-directional Traffic / Capuzzo Martina, Magrin Davide, Zanella Andrea // 2018 IEEE Global Communications Conference (GLOBECOM). – 2018. – P. 206–212.

3. Croce, Daniele. LoRa Technology Demystified: from Link Behavior to Cell Capacity / Croce Daniele, Gucciardo Michele, Mangione Stefano et al. // IEEE Transactions on Wireless Communications. – 2019.

4. Кулешова, Е. А. Метод обработки данных с учетом взаимного расположения информационных блоков в масштабе вычислительного кластера / Е. А. Кулешова, А. Л. Марухленко, В. П. Добрица, М. О. Таныгин, А. В. Плугатарев // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2021. – № 1. – С. 87–97.

5. Таныгин, М. О. Анализ системы контроля целостности цепочек информационных блоков на основе хэшей / М. О. Таныгин, М. С. Брусов, Е. О. Ефремова, Ю. В. Сухорукова // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : материалы III Всероссийской научно-практической конференции / редкол.: В. Г. Андронов (отв. ред.). – Курск, 2019. – С. 373–378.

6. Гузеев, А. В. Формирование распределения вероятностей появления отдельных сообщений источника при статистическом кодировании / А. В. Гузеев // T-Comm: Телекоммуникации и транспорт. – 2010. – Т. 4, № 6. – С. 12–16.

7. Колегов, Д. Н. Общий метод аутентификации HTTP-сообщений в веб-приложениях на основе хеш-функций / Д. Н. Колегов // Прикладная дискретная математика. Приложение. – 2014. – № 7. – С. 85–89.

8. Mytsko, E. A. Research of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources / E. A. Mytsko, A. N. Malchukov, S. D. Ivanov // Devices and systems. Management, control, diagnostics. – 2018. – № 6. – P. 22–29.

9. Vangelista, Lorenzo. Frequency Shift Chirp Modulation: The LoRa Modulation / Vangelista, Lorenzo // IEEE Signal Processing Letters. – 2017. – Vol. 24, № 12. – P. 1818–1821.

10. Жукова, Г. Н. / Карта коэффициентов асимметрии и эксцесса в преподавании теории вероятностей и математической статистики / Г. Н. Жукова // Концепт. – 2015. – № 8. – С. 56–60.

11. Жукова, Г. Н. / Идентификация распределения по коэффициентам асимметрии и эксцесса / Г. Н. Жукова // Московский государственный университет печати имени Ивана Федорова.

12. Urazbakhtin, A. I. Algorithm for checking the homogeneity of the sample and its representativeness to the random process under study / A. I. Urazbakhtin, I. G. Urazbakhtin // Infocommunication technologies. – 2006. – Vol. 4, № 3. – P. 10–14.

13. Lapina T. I. Time series forecasting based on data normalization methods / T. I. Lapina, I. G. Urazbahtin // Optical Technologies for Telecommunications 2005 : Proceedings. – 2006. – Vol. 6277. – 62770C.

14. Adelantado, Ferran. Understanding the Limits of LoRaWAN / Adelantado, Ferran, Vilajosana Xavier, Tuset Pere et al. // IEEE Communications Magazine. – 2017.

15. Sørensen Rene, Brandborg. Analysis of Latency and MAC-layer Performance for Class A LoRaWAN / Sørensen Rene Brandborg, Kim Dong Min, Nielsen Jimmy Jessen, Popovski Petar // IEEE Wireless Communications Letters. – 2017. – Vol. 6, № 5. – P. 566–569.

16. Bramson, Norman. THE ALOHA SYSTEM: Another Alternative for Computer Communications / Bramson Norman // Proceedings of the November 17–19, 1970, Fall Joint Computer Conference. AFIPS ’70 (Fall). – New York, NY, USA: ACM, 1970. – P. 281–285.

17. Mahmood, Aamir. Scalability Analysis of a LoRa Network under Imperfect Orthogonality / Mahmood Aamir, Sisinni Emiliano, Guntupalli Lakshmikanth et al. // IEEE Transactions on Industrial Informatics. – 2018. – Vol. 15, № 3. – P. 1425–1436.

18. Magrin, Davide. A Thorough Study of LoRaWAN Performance Under Different Parameter Settings / Magrin Davide, Capuzzo Martina, Zanella Andrea // IEEE Internet of Things Journal. – 2019.

19. Лоднева, О. Н. Анализ трафика устройств интернета вещей. / О. Н. Лоднева, Е. П. Ромасевич // Современные информационные технологии и ИТ-образование. – 2018. – Т. 14, № 1. – С. 149–169.

References

1. Marukhlenko, A. L., Plugatarev, A. V., Tanygin, M. O., Marukhlenko, L. O., Shashkov, M. Yu. Variant razgranicheniya dostupa k informatsionnym resursam na osnove neyavnoy autentifikatsii [A variant to restrict access to information resources based on implicit authentication]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta* [Bulletin of the Southwestern State University], 2020, vol. 24, no. 2, pp. 108–121.

2. Capuzzo, Martina, Magrin, Davide, Zanella, Andrea. Mathematical Modeling of LoRaWAN Performance with Bi-directional Traffic. *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 206–212.

3. Croce, Daniele, Gucciardo, Michele, Mangione, Stefano et al. LoRa Technology Demystified: from Link Behavior to Cell Capacity. *IEEE Transactions on Wireless Communications*, 2019.

4. Kuleshova, E. A., Marukhlenko, A. L., Dobritsa, V. P., Tanygin, M. O., Plugatarev, A. V. Metod obrabotki dannykh s uchetom vzaimnogo raspolozheniya informatsionnykh blokov v masshtabe vychislitelnogo klastera [Method of data processing taking into account the relative position of information blocks on the scale of a computing cluster]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyy analiz i informatsionnye tekhnologii* [Bulletin of the Voronezh State University. Series: System Analysis and Information Technology] 2021. № 1. S. 87-97.

5. Tanygin, M. O., Brusov, M. S., Efremova, E. O., Sukhorukova, Yu. V. Analiz sistemy kontrolya tselostnosti tsepochek informatsionnykh blokov na osnove kheshey [Analysis of the integrity control system for chains of information blocks based on hashes]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti resheniya : materialy III Vserossiyskoy nauchno-prakticheskoy konferentsii* [Infocommunications and space technologies: state, problems and solutions : proceedings of the III All-Russian Scientific and Practical Conference]. Kursk, 2019, pp. 373–378.

6. Guzeev, A. V. Formirovanie raspredeleniya veroyatnostey poyavleniya otdelnykh soobshcheniy istochnika pri statisticheskom kodirovanii [Formation of the probability distribution of the occurrence of individual source messages during statistical coding]. *T-Comm: Telekommunikatsii i transport* [T-Comm: Telecommunications and transport], 2010, vol. 4, no. 6, pp. 12–16.

7. Kolegov, D. N. Obshchiy metod autentifikatsii HTTP-soobshcheniy v veb-prilozheniyakh na osnove khesh-funktsiy [General method for authenticating HTTP messages in web applications based on hash functions]. *Prikladnaya diskretnaya matematika. Prilozhenie* [Applied Discrete Mathematics. Application], 2014, no. 7, pp. 85–89.

8. Mytsko, E. A., Malchukov, A. N., Ivanov, S. D. Research of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources. *Devices and systems. Management, control, diagnostics*, 2018, no. 6, pp. 22–29.

9. Vangelista, Lorenzo. Frequency Shift Chirp Modulation: The LoRa Modulation. *IEEE Signal Processing Letters*, 2017, vol. 24, no. 12, pp. 1818–1821.

10. Zhukova, G. N. Karta koeffitsientov asimmetrii i ekstsessa v prepodavanii teorii veroyatnostey i matematicheskoy statistiki [Map of Skewness and Kurtosis Coefficients in Teaching Probability and Mathematical Statistics]. *Kontsept* [Concept], 2015, no. 8, pp. 56–60.

11. Zhukova, G. N. Identifikatsiya raspredeleniya po koeffitsientam asimmetrii i ekstsessa [Identification of the distribution by the coefficients of skewness and kurtosis]. *Moskovskiy gosudarstvennyy universitet pechati imeni Ivana Fedorova* [Moscow State University of Printing Arts named after Ivan Fedorov].

12. Urazbakhtin, A. I., Urazbakhtin, I. G. / Algorithm for checking the homogeneity of the sample and its representativeness to the random process under study. *Infocommunication technologies*, 2006, vol. 4, no. 3, pp. 10–14.

13. Lapina, T. I., Urazbahtin, I. G. Time series forecasting based on data normalization methods. *Optical Technologies for Telecommunications 2005 : Proceedings*, 2006, vol. 6277, 62770C.

14. Adelantado Ferran, Vilajosana Xavier, Tuset Pere et al. Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*, 2017.

15. Sørensen Rene, Brandborg, Kim Dong, Min, Nielsen Jimmy, Jessen, Popovski, Petar. Analysis of Latency and MAC-layer Performance for Class A LoRaWAN. *IEEE Wireless Communications Letters*, 2017, vol. 6, no. 5, pp. 566–569.

16. Bramson Norman. THE ALOHA SYSTEM: Another Alternative for Computer Communications. *Proceedings of the November 17–19, 1970, Fall Joint Computer Conference. AFIPS '70 (Fall)*. New York, NY, USA, ACM, 1970, pp. 281–285.

17. Mahmood, Aamir, Sisinni, Emiliano, Guntupalli, Lakshmikanth et al. Scalability Analysis of a LoRa Network under Imperfect Orthogonality. *IEEE Transactions on Industrial Informatics*, 2018, vol. 15, no. 3, pp. 1425–1436.

18. Magrin, Davide, Capuzzo, Martina, Zanella, Andrea. A Thorough Study of LoRaWAN Performance Under Different Parameter Settings. *IEEE Internet of Things Journal*, 2019.

19. Lodneva, O. N., Romasevich, E. P. Analiz trafika ustroystv interneta veshchey [Internet of Things device traffic analysis]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie* [Modern information technologies and IT education], 2018, vol. 14, no. 1, pp. 149–169.

DOI 10.54398/20741707_2022_4_38
УДК 004.9:517.9

SEIRD-МОДЕЛЬ ДИНАМИКИ РАСПРОСТРАНЕНИЯ ВИРУСНЫХ ИНФЕКЦИЙ С УЧЕТОМ ВОЗНИКНОВЕНИЯ НОВЫХ ШТАММОВ[1]

Статья поступила в редакцию 10.10.2022, в окончательном варианте – 21.10.2022.

Мартьянова Александра Евгеньевна, Астраханский государственный университет имени В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат технических наук, доцент кафедры информационной безопасности, ORCID: 0000-0001-5917-8477, e-mail: mrtnva@rambler.ru
Ажмухамедов Искандар Маратович, Астраханский государственный университет имени В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
доктор технических наук, декан факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности, ORCID: 0000-0001-9058-123X, e-mail: aim_agtu@mail.ru

Детерминистские математические модели эпидемий заболеваний позволяют изучать макроскопические явления распространения этих эпидемий в человеческом обществе. Однозначность, наглядность и простота этих моделей делают их привлекательными для анализа и позволяют получить информацию для управления протеканием эпидемии. Детерминистские математические модели представляют собой инструмент исследования динамики численности индивидуумов в условиях эпидемической обстановки. Предложена математическая SEIRD-модель динамики распространения вирусных инфекций, учитывающая возникновение новых штаммов. Данная SEIRD-модель позволяет учитывать способность инфицированных индивидуумов к заражению окружающих в латентном периоде развития заболевания, что очень важно, поскольку заболевание распространяется скрытно. Число инфицированных индивидуумов значительно больше зарегистрированных случаев. Решение осуществляется в системе компьютерной алгебры (CAS) Maxima. Показана возможность использования данной SEIRD-модели для прогнозирования распространения эпидемии COVID-19 с учетом появления вирусных вариантов SARS-CoV-2. Показано, что полученные теоретические зависимости хорошо согласуются с имеющимися данными по г. Москве.

Ключевые слова: математическая модель, модель эпидемии COVID-19, SEIRD-модель, SEIRD-модель распространения заболевания COVID-19, система дифференциальных уравнений, свободное программное обеспечение, система компьютерной математики Maxima, штаммы вируса, варианты вируса SARS-CoV-2

SEIRD MODEL DESCRIBING THE DYNAMICS OF THE SPREAD VIRAL INFECTIONS CONSIDERING THE APPEARANCE OF NEW STRAINS

The article was received by the editorial board on 10.10.2022, in the final version – 21.10.2022.

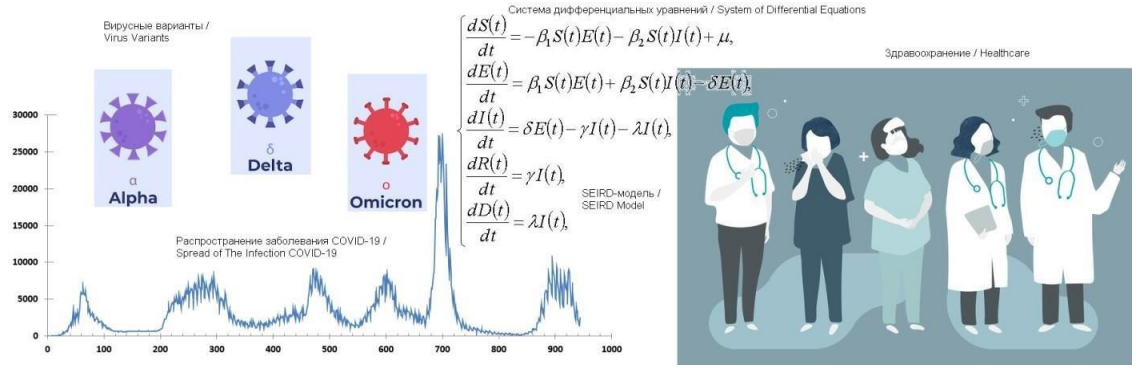
Martyanova Aleksandra Ye., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Engineering), ORCID: 0000-0001-5917-8477, e-mail: mrtnva@rambler.ru
Azhmukhamedov Iskandar M., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Doct. Sci. (Engineering), Dean of the Faculty of Digital Technologies and Cybersecurity, Professor of the Department of Information Security, e-mail: aim_agtu@mail.ru

Deterministic mathematical models of epidemic diseases allow us to study the macroscopic propagation effect of these epidemics spreading in human society. The unequivocal, demonstrativeness and simple nature of these models make them attractive for analysis and provide information for the managing development of the epidemic. The deterministic mathematical models are an instrument for investigating the population dynamics of individuals in an epidemic environment. A mathematical SEIRD model describing the dynamics of the spread of viral infections is proposed, taking into account the emergence of new strains. This SEIRD-model it allows us to take account the ability of infected individuals to contagion others in the latent period of the disease progression, which is very important because the disease spreads covertly. The number of infected individuals is much higher than the number of registered cases. The solving is performed in the Maxima computer algebra system (CAS). The possibility of using this SEIRD model to predict the spread of the infection COVID-19, taking into account viral variants of SARS-CoV-2, is shown. It is shown that the obtained theoretical dependencies agree well with the available data for Moscow.

Keywords: mathematical model, epidemiological model of COVID-19, SEIRD model, SEIRD model the spread of the infection COVID-19, system of differential equations, free software, computer mathematics system Maxima, virus strains, variants of the virus SARS-CoV-2

[1] Исследование выполнено при поддержке гранта фундаментальных научно-исследовательских проектов в рамках реализации стратегических проектов «Программы развития Астраханского государственного университета на 2021–2030» «Методологические основы оценки и управления уровнем комплексной безопасности региона».

Graphical annotation (Графическая аннотация)



Введение. Детерминистские математические модели эпидемий заболеваний позволяют изучать макроскопические явления распространения этих эпидемий в человеческом обществе. Однозначность, наглядность и простота этих моделей делают их привлекательными для анализа и позволяют получить информацию для управления протеканием эпидемии. Н. Бейли заметил, что основное значение этих исследований состоит в том, что они связаны с работой органов общественного здравоохранения [1]. При создании таких моделей делается ряд упрощений: развитие эпидемии изучается в однородной непрерывно и равномерно перемешивающейся большой группе, что позволяет рассматривать общие процессы распространения эпидемии в упрощенной форме. Для успешной борьбы с эпидемиями заразных заболеваний недостаточно одних только профилактических мероприятий или лекарственного лечения, необходимо также учитывать, что существуют эпидемиологические проблемы, касающиеся распространения болезни в целом. Для системы здравоохранения очень важна возможность количественной оценки различных мероприятий по борьбе с эпидемией, например, введения карантина, осуществления вакцинации и др. Рассматривая большие группы, можно получать довольно общие модели распространения эпидемий в больших популяциях, на основе которых и возможно осуществление общей оценки применяемых мероприятий для системы здравоохранения.

В 1927 г. в своей работе W. O. Kermack и A. G. MacKendrick создали и исследовали модель, представляющую собой систему дифференциальных уравнений с начальными условиями, которую называют классической SIR-моделью [2]. Н. Бейли (Norman T. J. Bailey) исследовал модели детерминистского типа, описывающие простые эпидемии, эпидемию общего типа, повторяющиеся эпидемии [1]. L. Edelstein-Keshet подробно рассмотрел SIR-модель (Susceptible – восприимчивые, Infected – инфицированные, Recovered – выздоровевшие индивидуумы) и ее SIRS- и SIS-модификации [3]. Он показал, что при некоторых условиях SIRS-модель приобретает вид SIR-модели Kermack и MacKendrick.

Развитием SIR-модели являются также SEIR- (Exposed – латентные), MSEIR-модели (Maternally derived immunity – наделенные иммунитетом от рождения) [4].

При изучении заболевания COVID-19, вызываемого вирусом SARS-CoV-2, предлагаются к рассмотрению SIRD-модели (Dead – умершие) и SEIRD-модели [5, 6]. Рассматриваемая в [6] SEIRD-модель отличается тем, что параметры, характеризующие заражение и смертность, зависят от времени, но не учитывают способность инфицированных индивидуумов заражать восприимчивых индивидуумов в латентном (инкубационном) периоде. Предложенная в источнике [7] для изучения эпидемии лихорадки Эбола SEIRD-модель отличается тем, что хотя и учитывает наличие индивидуумов, находящихся в латентном периоде, но не учитывает способность этих индивидуумов в латентном периоде к заражению восприимчивых индивидуумов.

Различные детерминистские модели представляют собой инструмент исследования динамики численности индивидуумов в условиях эпидемической обстановки, в частности широко использовались как при изучении геморрагической лихорадки Эбола [7, 8], так и при изучении эпидемии заболеваемости COVID-19 [5, 6].

Постановка задачи. Необходимо разработать SEIRD-модель динамики распространения вирусных инфекций, учитывающую наличие индивидуумов, находящихся в латентном периоде, и восприимчивых индивидуумов, способных к заражению, что важно, поскольку заболевание распространяется скрытно, и число инфицированных индивидуумов больше зарегистрированных случаев. На основе разработанной SEIRD-модели необходимо проанализировать влияние появления разных штаммов вируса (вариантов вируса) SARS-CoV-2 на развитие эпидемии COVID-19. Для оценки адекватности предложенной модели необходимо сравнить теоретические результаты с данными о количестве инфицированных, полученными по г. Москве.

Решение задачи. Анализ данных по распространению COVID-19 в г. Москве. Рассматривая графики заболеваемости COVID-19 в г. Москве (рис.1–3) в период с 6 марта 2020 г. по 6 октября 2022 г. (945 день), можно условно выделить следующие одиннадцать периодов: 1) с 1 по 124 день – первый подъем и спад заболеваемости (так называемая 1-я «волна»); 2) с 125 по 200 день – период между 1-й и 2-й «волнами»; 3) с 201 по 355 день – второй подъем и спад заболеваемости (2-я «волна»); 4) с 356 по 400 день – период между 2-й и 3-й «волнами»; 5) с 401 по 520 день – третий подъем и спад заболеваемости (3-я «волна»); 6) с 521 по 570 день – период между 3-й и 4-й «волнами»; 7) с 571 по 630 день – четвертый подъем и спад заболеваемости (4-я «волна»); 8) с 631 по 670 – период между 4-й и 5-й «волнами»; 9) с 671 по 740 день – пятый подъем и спад заболеваемости (5-я «волна»); 10) с 741 по 860 день — период между 5-й и 6-й «волнами»; 11) с 861 дня – длящийся и, скорее всего, закончившийся на момент публикации этой работы шестой подъем и спад заболеваемости (6-я «волна»).

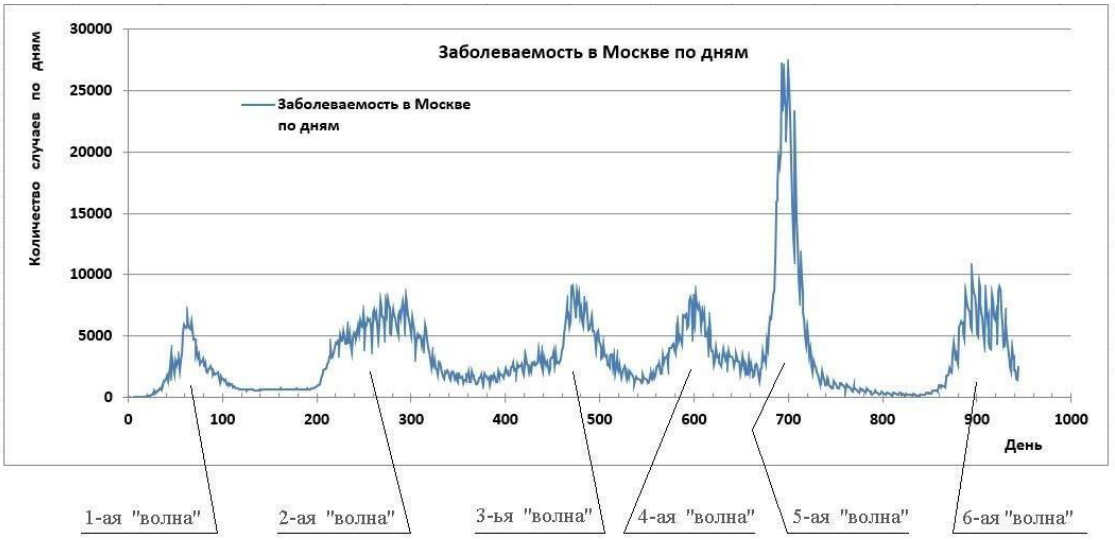


Рисунок 1 – Развитие эпидемии с 6 марта 2020 г. по 6 октября 2022 г. по дням

По графику на рисунке 1 можно увидеть, что пятый период (3-я «волна») состоит из двух частей: I и II, что и показано более наглядно на графике рисунка 2. Начиная с 461 дня (9 июня 2021 г.) наблюдается резкий подъем 3-й «волны» заболевания, который относится ко II части 3-й «волны».

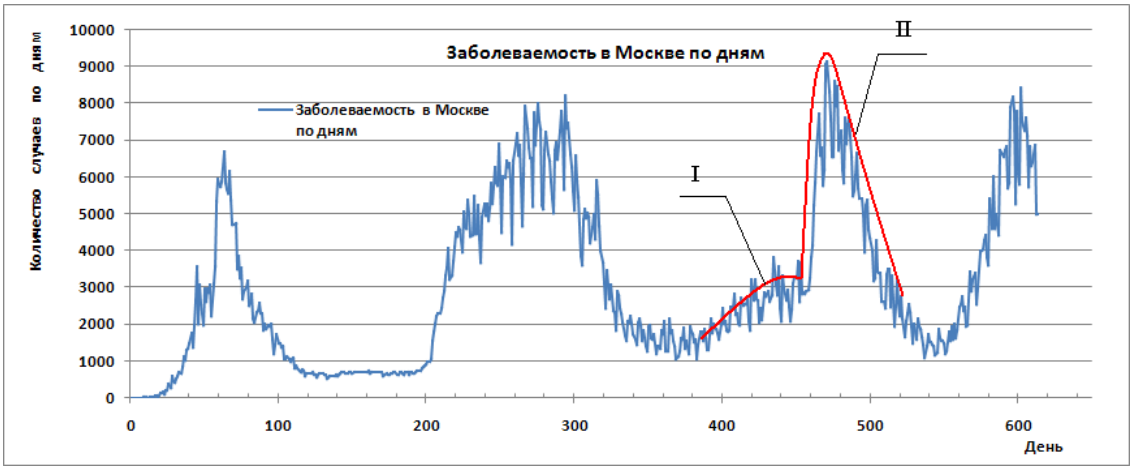


Рисунок 2 – Развитие эпидемии с 6 марта 2020 г. по 8 ноября 2021 г. по дням

Также можно обнаружить, что восьмой период (промежуток между 4-й и 5-й «волнами») может быть рассмотрен как наслоение продолжающегося спада седьмого периода (4-й «волны») и начинающегося уже одновременно подъема девятого периода (5-й «волны»); то есть присутствуют I и II части 4-й «волны», где II часть 4-й «волны», она же восьмой период, – это наслоение двух периодов: седьмого и девятого, что и показано на графике рисунка 3.

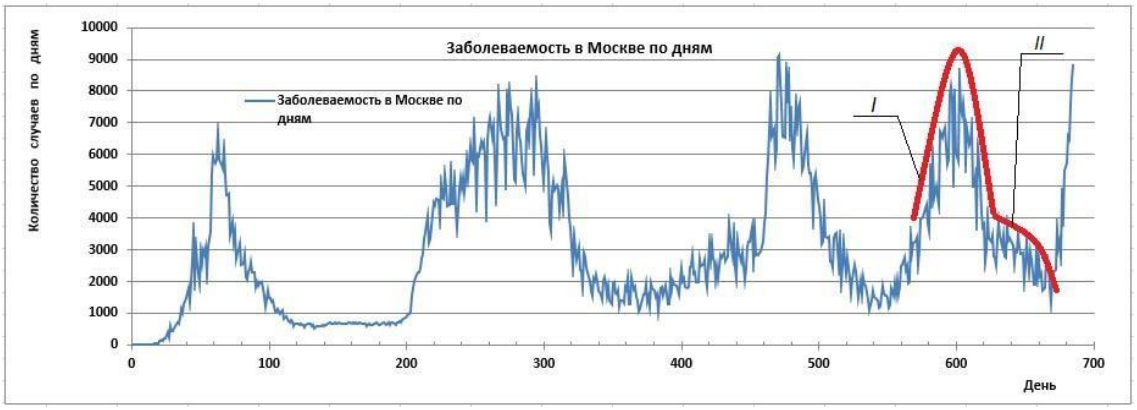


Рисунок 3 – Развитие эпидемии с 6 марта 2020 г. по 19 января 2022 г. по дням

Построение математической модели распространения COVID-19. Рассмотрим детерминистскую математическую SEIRD-модель (S – восприимчивые, E – латентные, I – инфицированные, R – выздоровевшие, D – умершие) эпидемии заболевания.

На рисунке 4 представлена блок-схема процессов рассматриваемой SEIRD-модели, где μ – приток восприимчивых индивидуумов, которыми пополняется группа.

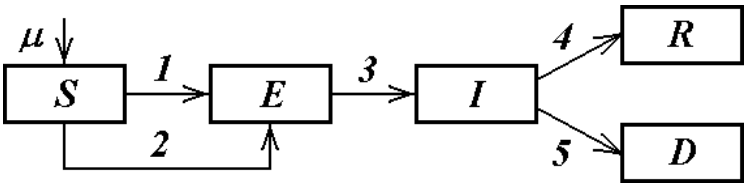


Рисунок 4 – Блок-схема SEIRD-модели

Параметры рассматриваемой SEIRD-модели представлены в таблице ниже.

Таблица – Таблица параметров SEIRD-модели

№ перехода	Переход	Скорость перехода
1	$(S, E) \to (S-1, E+1)$	$\beta_1 S E$,
2	$(S, E) \to (S-1, I+1)$	$\beta_2 S I$
3	$(E, I) \to (E-1, I+1)$	δE
4	$(I, R) \to (I-1, R+1)$	γI
5	$(I, D) \to (I-1, D+1)$	λI

Отличие рассматриваемой здесь SEIRD-модели от подобных детерминистских моделей в том, что данная SEIRD-модель позволяет учитывать способность в латентном периоде инфицированных индивидуумов к заражению восприимчивых индивидуумов. SEIRD-модель сводится к решению задачи Коши для системы пяти обыкновенных дифференциальных уравнений первого порядка с неизвестными $S(t)$, $E(t)$, $I(t)$, $R(t)$, $D(t)$ и начальными условиями $S(0) = n$, $E(0) = a$, $I(0) = b$, $R(0) = c$ и $D(0) = d$.

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta_1 S(t)E(t) - \beta_2 S(t)I(t) + \mu, \\ \dfrac{dE(t)}{dt} = \beta_1 S(t)E(t) + \beta_2 S(t)I(t) - \delta E(t), \\ \dfrac{dI(t)}{dt} = \delta E(t) - \gamma I(t) - \lambda I(t), \\ \dfrac{dR(t)}{dt} = \gamma I(t), \\ \dfrac{dD(t)}{dt} = \lambda I(t). \end{cases}$$

Здесь введены следующие коэффициенты: β_1 и β_2 – характеризуют заболеваемость в однородной группе в латентный и активный периоды заболевания соответственно, которые в сумме образуют полный период; δ – характеризует переход индивидуумов из латентного периода в период с активным протеканием заболевания; γ – характеризует убыль индивидуумов из группы (изолированных, выздоровевших и ставших невосприимчивыми к инфекции в результате иммунизации); λ – характеризует убыль индивидуумов в результате смерти от инфекции в группе; μ – характеризует постоянный приток восприимчивых индивидуумов, которыми пополняется группа.

Коэффициент β_1 – вероятность заражения от инфицированного индивидуума, находящегося в латентном периоде, будет равен $\beta_1 = q_1/(T_1 n)$; коэффициент β_2 – вероятность заражения от индивидуума, находящегося в активном периоде, будет равен $\beta_2 = q_2/(T_2 n)$; q_1 и q_2 – индексы репродукции в латентный и активный периоды заболевания соответственно, $q_1 \neq q_2$; T_1, T_2 и T – латентный, активный и полный временные периоды заболевания; n – объем рассматриваемой группы однородно перемешивающихся индивидуумов. Коэффициент $\delta = 1/T_1$ характеризует скорость перехода из латентного периода в активный период. Коэффициент $\gamma = 1/T$ – скорость выздоровления. Коэффициент μ – число восприимчивых индивидуумов, которыми пополняется группа. Коэффициент λ можно принять как установившийся процент от уже инфицированных индивидуумов.

Приток новых восприимчивых индивидуумов (μ) в общем случае не уравновешивается гибелью индивидуумов, удаленных из популяции (λI), и, таким образом, объем популяции не остается постоянным ($S(t) + E(t) + I(t) + R(t) + D(t) + \mu \neq$ const). В настоящей работе для простоты везде считаем, что постоянный приток восприимчивых индивидуумов отсутствует ($\mu = 0$), но вовлечение таковых индивидуумов происходит по мере их накопления, которое связано с появлением новых штаммов COVID-19 и падением уровня иммунизации индивидуумов с течением времени.

Рассматриваемая здесь SEIRD-модель была апробирована на данных по первой вспышке заболевания, происходившей в городе Ухань провинции Хубей [9, 10]. В период этой вспышки вся провинция Хубей находилась в условиях жестких карантинных мероприятий, а вариант вируса не изменялся с точки зрения контагиозности (заразности). Расчеты выполнялись с допущением, что первоначальная группа имеет объем n = 11 млн восприимчивых индивидуумов, поскольку вспышка происходила в значительной мере в городе Ухань провинции Хубей, население которого составляет примерно 10–12 млн. Временные периоды T = 30, T_1 = 14 и $T_2 = T–T_1$ дней. Коэффициент убыли индивидуумов в результате смерти от инфекции условно принят постоянным и равным 2,5 % от числа зарегистрированных инфицированных индивидуумов – λ = 0,025. Индексы q_1 = 2,0 и q_2 = 5,5. Временной период развития эпидемии – 200 дней. Приток восприимчивых индивидуумов отсутствует ($\mu = 0$), так как почти сразу введены жесткие карантинные мероприятия. Число латентных индивидуумов – a = 100. Было установлено, что максимум модельной кривой динамики численности соответствует максимуму данных, имеющихся для китайской провинции Хубей.

Поскольку индивидуум является распространителем вируса как в латентном, так и в активном периодах заболевания, необходимо учитывать динамику инфицированных индивидуумов в латентном и активном периодах. На графике рисунка 5 представлены: кривая «expos_SEIRD» – динамика инфицированных индивидуумов в латентном периоде заболевания; кривая «inf_SEIRD» – динамика инфицированных в активном периоде заболевания; суммарная кривая «sum_SEIRD» – динамика инфицированных индивидуумов в латентном и активном периодах заболевания по рассматриваемой SEIRD-модели; t – длительность эпидемии в днях. Видно смещение максимума суммарной кривая «sum_SEIRD» в более ранние сроки, нежели кривой «inf_SEIRD», и это указывает на то, что максимальная нагрузка на систему здравоохранения наступает раньше сроков, полученных с помощью моделей, не учитывающих влияние распространения вируса индивидуумами, находящимися в латентном периоде заболевания, а также на то, что эта максимальная нагрузка соответственно будет выше.

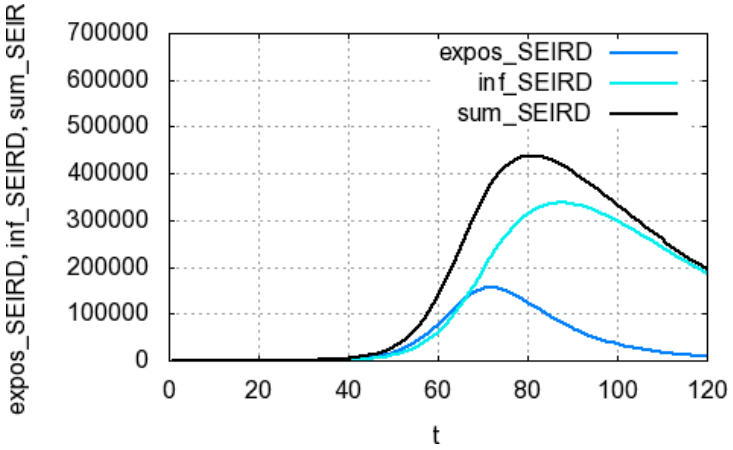


Рисунок 5 – Результаты расчета по SEIRD-модели

Также было установлено, что зарегистрированные случаи составляют около 15 % общего количества инфицированных индивидуумов. Поскольку индивидуум является распространителем вируса как в латентном, так и в активном периодах заболевания, то в модели необходимо учитывать количество инфицированных индивидуумов в латентном и активном периодах, которые являются распространителями заболевания. Заболевание COVID-19 хуже диагностируется в латентном периоде, что учитывается уменьшением влияния зарегистрированных инфицированных индивидуумов в латентном периоде заболевания на 50 % в общем количестве зарегистрированных инфицированных индивидуумов, представляющем собой сумму инфицированных как в латентном, так и в активном периодах заболевания.

Используем рассматриваемую здесь SEIRD-модель для описания развития эпидемии заболевания COVID-19 в Москве. Будем рассматривать временной период развития эпидемии в 941 день (с 6 марта 2020 г. до 2 октября 2022 г. включительно). Время латентного, активного и полного периодов заболевания почти на всем рассматриваемом временном интервале составляет, соответственно, $T = 30$, $T_1 = 14$ и $T_2 = T–T_1$ дней, за исключением того периода, когда появляется штамм «омикрон». Коэффициент убыли индивидуумов в результате смерти от инфекции условно принят также постоянным и равным 2,5 % от числа зарегистрированных инфицированных индивидуумов – $\lambda = 0{,}025$, за исключением периода, когда уже появляется штамм «омикрон».

С появлением штамма «омикрон» временные периоды изменились и приняты следующими: $T = 30$, $T_1 = 6$ и $T_2 = T–T_1$ дней. Было принято, что латентный период для этого штамма в среднем составляет 6 дней. Коэффициент убыли индивидуумов в результате смерти от инфекции с появлением штамма «омикрон» условно принят постоянным и равным 1,0 % от числа зарегистрированных инфицированных индивидуумов – $\lambda = 0{,}01$.

Решение системы уравнений рассматриваемой SEIRD-модели осуществлялось функцией **rk** из библиотеки «dynamics» свободного программного обеспечения – системы компьютерной алгебры CAS Maxima; функция **rk** решает задачу Коши методом Рунге – Кутта четвертого порядка точности [11]. Скриншот начала одного из вариантов решения представлен на рисунке 6.

Для первого периода в качестве начальных условий принято $a = 2000$ – количество латентных индивидуумов в начале развития эпидемии. Начальные условия в части латентных и инфицированных индивидуумов каждого последующего периода определяются предыдущим периодом развития заболевания. Объем n рассматриваемой группы однородно перемешивающихся восприимчивых индивидуумов подбирался для каждого периода. Для первого периода принято $n = 2{,}1$ млн чел., индексы $q_1 = 1{,}5$ и $q_2 = 2{,}5$. Для второго периода – $n = 1{,}0$ млн чел., индексы $q_1 = 0{,}27$ и $q_2 = 0{,}45$. Для третьего периода – $n = 6{,}0$ млн чел, индексы $q_1 = 0{,}69$ и $q_2 = 1{,}15$. Для четвертого периода – $n = 1{,}0$ млн чел., индексы $q_1 = 0{,}27$ и $q_2 = 0{,}45$. В пятый период при рассмотрении распространения штамма «альфа» в качестве прогнозируемого объема группы индивидуумов рассматривался объем $n = 2{,}0$ млн чел., индексы $q_1 = 0{,}42$ и $q_2 = 0{,}70$.

```
--> /* Решение задачи об эпидемии с помощью функции rk. */
    /* Обозначения: S (susceptible) - восприимчивые, */
    /* E (exposed) - латентные, I (infected)- инфицированные, */
    /* R (recovered) - выздоровевшие, D (dead) - умершие, t - время в днях */
    kill(all); fpprintprec:9;

--> /* Загрузка библиотеки dynamics */
    load(dynamics);

--> norma:0.15; norma1:0.15; (norma1/norma); expos:0.5;

--> /* Число латентных, число восприимчивых (1) */
    a:2000.0; n_1:2100000.0-a; T:30.0; T1:14.0; T2:T - T1; q1:1.5; q2:2.5;
    m_1:124-0+1;

--> /* Коэффициенты пропорциональности (1) */
    beta1:q1/(T1*n_1); beta2:q2/(T2*n_1); beta:q/(T*n_1); gamma:1/T; mu:0.0;
    lambda:gamma*0.025; delta:1/T1;

--> /* Вызов функции rk, SEIRD-модель с beta1, beta2 и mu, expos - 0.5 (1) */
    r_1:rk([-S*(beta1*E+beta2*I)+mu,S*(beta1*E+beta2*I)-delta*E,
    delta*E-gamma*I-lambda*I,gamma*I,lambda*I],
    [S,E,I,R,D],[n_1,a,0.0,0.0,0.0],[t,1,m_1,1]);

--> /* Число латентных, число восприимчивых (2) */
    n_2:1000000.0-r_1[m_1][3]; T:30.0; T1:14.0; T2:T - T1; q1:0.27; q2:0.45;
    m_2:200-124+1;
```

Рисунок 6 – Скриншот решения в CAS Maxima

На протяжении пятого периода произошло вытеснение штамма «альфа» штаммом «дельта». Учитывая, что в Москве в конце марта 2021 года появился штамм вируса «дельта», были пересмотрены результаты расчета количества заболевших в пятый период (3-я «волна»). Принято, что на 401 день (10 апреля 2021 г.) развития эпидемии заболеваемость штаммом «альфа» развивалась по варианту n = 2,0 млн чел., начальные условия в части латентных и инфицированных индивидуумов для этого периода для штамма «альфа» определялись по предыдущему периоду.

Одновременно считалось, что на 401 день уже было 250 человек, которые являлись латентными носителями штамма «дельта», поэтому в качестве начальных значений для штамма «дельта» в пятый период принято a = 250 – количество латентных индивидуумов, n = 3,0 млн чел., индексы q_1 = 1,68 и q_2 = 2,80. Суммарный подъем в результате одновременного протекания заболеваемости под действием штаммов «альфа» и «дельта» представлен кривой «Модель для ‘дельта’» на рисунке 7. Кривая «Модель для ‘альфа’» показывает, как заболеваемость под действием штамма «альфа» спадает и вытесняется заболеваемостью под действием штамма «дельта».

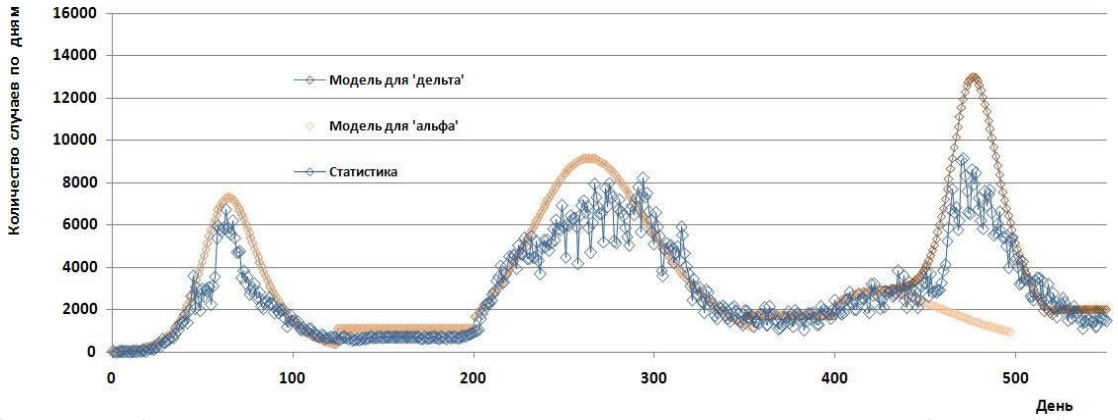


Рисунок 7 – Сравнение расчетных данных со статистическими данными в период с 6 марта 2020 г. до 6 сентября 2021 г.

Развитие шестого, седьмого и восьмого периодов происходит под действием штамма «дельта», так как он вытесняет предыдущие штаммы. Шестой период: n = 1,0 млн чел., индексы q_1 = 0,27 и q_2 = 0,45. Седьмой период: n = 4,0 млн чел., индексы q_1 = 0,84 и q_2 = 1,4. Восьмой период для штамма «дельта»: n = 1,0 млн чел., индексы q_1 = 0,27 и q_2 = 0,45.

Одновременно со штаммом «дельта» в восьмой период появляется штамм «омикрон», для которого в качестве начальных значений в восьмой период на 631 день (26 ноября 2021 г.) принято

a = 5 – количество латентных индивидуумов, n = 6,0 млн чел, индексы q_1 = 1,8 и q_2 = 3,0. Девятый период развивается как продолжение восьмого периода в присутствии практически только одного штамма «омикрон» и представляет собой подъем и спад заболеваемости 5-й «волны». Девятый период – штамм «омикрон»: n = 1,0 млн чел, индексы q_1 = 0,27 и q_2 = 0,45. Десятый период является продолжением девятого периода и развивается в присутствии только штамма «омикрон»: n = 4,5 млн чел, индексы q_1 = 1,02 и q_2 = 1,70.

Общий вид кривых, моделирующих развитие эпидемии на всем протяжении с 6 марта 2020 года по 2 октября 2022 года представлен на рисунке 8. На этом рисунке представлены три расчетные кривые: «Модель для ‘альфа’», «Модель для ‘дельта’» и «Модель для ‘омикрон’». Кривая «Модель для ‘дельта’» построена с учетом одновременного протекания с 401 дня заболеваемостью штаммами «альфа» и «дельта». Кривая «Модель для ‘омикрон’» построена с учетом одновременного протекания с 631 дня заболеваемостью штаммами «дельта» и «омикрон».

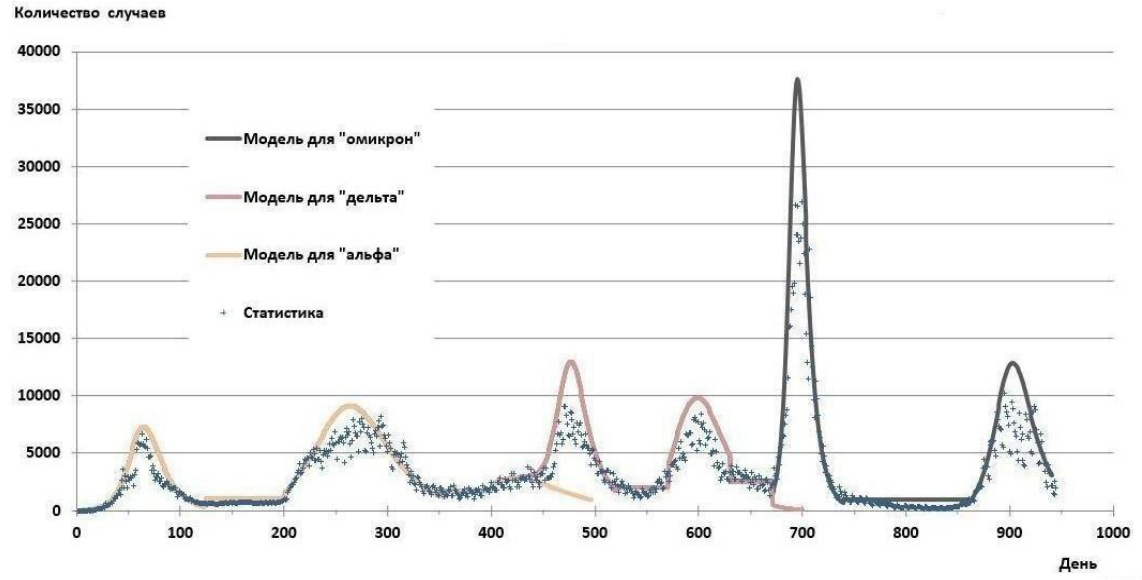


Рисунок 8 – Сравнение расчетных данных со статистическими данными в период до 2 октября 2022 года

Рисунок 8 показывает, что рассматриваемая SEIRD-модель хорошо описывает статистические данные по заболеваемости COVID-19 в Москве в период с 6 марта 2020 года по 2 октября 2022 года и позволяет учитывать влияние на развитие эпидемии новых штаммов вируса SARS-CoV-2.

Заключение. Показана возможность использования на примере города Москвы предлагаемой детерминистской математической SEIRD-модели, учитывающей наличие индивидуумов, находящихся в латентном периоде, и восприимчивых индивидуумов, способных к заражению, для описания развития эпидемии заболевания COVID-19 с учетом влияния на развитие продолжающейся эпидемии разных штаммов вируса SARS-CoV-2. Адекватность предложенной модели оценена на примере имеющихся данных о заболеваемости в г. Москве.

Библиографический список

1. Бейли, Н. Математика в биологии и медицине / Н. Бейли. – Москва : МИР, 1970. – 326 с.
2. Kermack, W. O. A Contribution to the Mathematical Theory of Epidemics / W. O. Kermack, A. G. McKendrick// Proceedings of the Royal Society. – 1927. – Vol. 115, № A771. – P. 700-721.
3. Edelstein-Keshet, L. Mathematical Models in Biology / L. Edelstein-Keshet. – Philadelphia : SIAM, 2005. – 586 p.
4. Hethcote, H. W. The Mathematics of Infectious Diseases / H. W. Hethcote // SIAM Review. – 2000. – Vol. 42, № 4. – P. 599–653.
5. Fanelli, D. Analysis and forecast of COVID-19 spreading in China, Italy and France / D. Fanelli, F. Piazza // arXiv:2003.06031v 1 [q-bio.PE]. – 12 Mar 2020. – Режим доступа: https://arxiv.org/pdf/2003.06031.pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 07.10.2022).
6. Piccolomini E. L. Monitoring Italian COVID-19 spread by an adaptive SEIRD model / E. L. Piccolomini, F. Zama // medRxiv preprint. – Version posted 6 April 2020. Режим доступа: https://www.medrxiv.org/content/10.1101/2020.04.03.20049734v1 (дата обращения 07.10.2022), свободный. – Заглавие с экрана. – Яз. англ.
7. Якушева, О. А. Математическая модель эпидемии лихорадки Эбола / О. А. Якушева // Электронная библиотечная система открытого доступа «Научный корреспондент». – Режим доступа:

https://nauchkor.ru/pubs/matematicheskaya-model-epidemii-lihoradki-ebola-587d36545f1be77c40d58cd2, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.10.2022).

8. Уракова, К. А. Математическое моделирование развития эпидемии геморрагической лихорадки Эбола в Западной Африке / К. А. Уракова, П. В. Храпов // Альманах современной науки и образования. – 2017. – № 4–5 (118). – С. 97–99. – Режим доступа: https://www.gramota.net/articles/issn_1993-5552_2017_4-5_25.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.10.2022).

9. Мартьянова, А. Е. Математическая модель эпидемии заболевания COVID-19 / А. Е. Мартьянова // 64-я Международная научная конференция АГТУ, посвященная 90-летнему юбилею со дня образования АГТУ. Астрахань, 20–25 апреля 2020 года : сб. ст. – Астрахань : Изд-во АГТУ, 2020.

10. Martianova, A. E. Mathematical Model of the COVID-19 Epidemic / A. E. Martianova, V. Yu. Kuznetsova, I. M. Azhmukhamedov // Advances in Social Science, Education and Humanities Research. – 2020. – Vol. 486. – Режим доступа: https://www.atlantis-press.com/proceedings/rtcov-20/125945667, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 07.10.2022).

11. Maxima, A. Computer Algebra System / A. Maxima. – Режим доступа: https://maxima.sourceforge.io/index.html, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 07.10.2022).

References

1. Beyli, N. *Matematika v biologii i medicine* [Mathematics in Biology and Medicine]. Moscow, MIR Publ., 1970. 326 p.

2. Kermack, W. O., McKendrick, A. G. A Contribution to the Mathematical Theory of Epidemics. *Proceedings of the Royal Society*, 1927, vol. 115, no. A771, pp. 700–721.

3. Edelstein-Keshet, L. *Mathematical Models in Biology*. Philadelphia, SIAM, 2005. 586 p.

4. Hethcote, H. W. The Mathematics of Infectious Diseases. *SIAM Review*, 2000, vol. 42, no. 4, pp. 599–653.

5. Fanelli, D., Piazza, F. Analysis and forecast of COVID-19 spreading in China, Italy and France. *arXiv:2003.06031v 1 [q-bio.PE]*, 12 Mar 2020. Available at: https://arxiv.org/pdf/2003.06031.pdf (accessed 07.10.2022).

6. Piccolomini, E. L., Zama, F. *Monitoring Italian COVID-19 spread by an adaptive SEIRD model*. *medRxiv preprint*, version posted 6 April 2020. Available at: https://www.medrxiv.org/content/10.1101/2020.04.03.20049734v1 (accessed 07.10.2022).

7. Yakusheva, O. A. *Matematicheskaya model epidemii likhoradki Ebola* [Mathematical model of the Ebola epidemic]. *Elektronnaya bibliotechnaya sistema otkrytogo dostupa "Nauchnyy correspondent"* [Electronic library system of open access "Scientific correspondent"]. Available at: https://nauchkor.ru/pubs/matematicheskaya-model-epidemii-lihoradki-ebola-587d36545f1be77c40d58cd2 (accessed 07.10.2022).

8. Urakova, K. A, Khrapov, P. V. *Matematicheskoe modelirovanie razvitiya epidemii gemorragicheskoy likhoradki Ebola v Zapadnoy Afrike* [Mathematical modeling of the development of the Ebola hemorrhagic fever epidemic in West Africa]. *Almanakh sovremennoy nauki i obrazovaniya* [Almanac of modern science and education]. Available at: https://www.gramota.net/articles/issn_1993-5552_2017_4-5_25.pdf (accessed 07.10.2022).

9. Martyanova A. Ye. *Matematicheskaya model epidemii zabolevaniya COVID-19* [Mathematical model of the COVID-19 disease epidemic]. *64-ya Mezhdunarodnaya nauchnaya konferentsiya AGTU, posvyashchennaya 90-letnemu yubileyu so dnya obrazovaniya AGTU. Astrakhan, 20–25 aprelya 2020 goda* [64th International Scientific Conference of ASTU, dedicated to the 90th anniversary of ASTU]. Astrakhan, AGTU Publ., 2020.

10. Martyanova A. E., Kuznetsova V. Yu., Azhmukhamedov I. M. Mathematical Model of the COVID-19 Epidemic. *Advances in Social Science, Education and Humanities Research*, 2020, vol. 486. Available at: https://www.atlantis-press.com/proceedings/rtcov-20/125945667 (accessed 07.10.2022).

11. Maxima, A. *Computer Algebra System*. Available at: https://maxima.sourceforge.io/ru/index.html (accessed 07.10.2022).

УДК 51-74

РАЗРАБОТКА МЕХАНИЗМА ОБОСНОВАНИЯ ВЫБОРА ТЕХНИЧЕСКИХ РЕШЕНИЙ ДЛЯ ОБЪЕКТА ИНФРАСТРУКТУРЫ, ПОЗВОЛЯЮЩЕГО ОЦЕНИТЬ УРОВЕНЬ ЕГО ОСНАЩЕННОСТИ С УЧЕТОМ ТРЕБОВАНИЙ МАЛОМОБИЛЬНЫХ ГРУПП НАСЕЛЕНИЯ

Статья поступила в редакцию 28.09.2022, в окончательном варианте – 03.10.2022.

Овчинников Ярослав Алексеевич, Пермский национальный исследовательский политехнический университет, 614990, Российская Федерация, г. Пермь, Комсомольский проспект, 29,
магистрант, ORCID: 0002-7963-2574, e-mail: yaroslove.ovch@gmail.com
Кривогина Дарья Николаевна, Пермский национальный исследовательский политехнический университет, 614990, Российская Федерация, г. Пермь, Комсомольский проспект, 29,
кандидат технических наук, доцент, ORCID: 0001-6453-3701, e-mail: darya.krivogina @gmail.com

В данной работе представлен новый подход к решению задач оценки приспособленности объектов недвижимости для маломобильных групп населения. Автором представлен новый подход оценки доступности общественных зданий для маломобильного населения, который отличается тем, что уровень доступности определяется не комплексно, как в современных методиках, а поэлементно. Ведь, как показывает практика, отсутствие одного элемента может стать решающим фактором в реальной возможности применения и использования благ объекта человеком. Проведено комплексное исследование физкультурно-оздоровительного комплекса, выявлены недостатки в качестве необходимости установки некоторых элементов и отсутствия ряда тренажеров, что является основным показателем качества доступности среды для объектов спорта. Были предложены рекомендации в отношении улучшения параметров с низкой комплексной оценкой.

Ключевые слова: разработка механизма, обоснование выбора, технические решения, маломобильные группы населения, комплексное оценивание

DEVELOPMENT OF A MECHANISM FOR JUSTIFYING THE CHOICE OF TECHNICAL SOLUTIONS FOR AN INFRASTRUCTURE FACILITY, ALLOWING ASSESSING THE LEVEL OF ITS EQUIPMENT, TAKING INTO ACCOUNT THE REQUIREMENTS OF LOW-MOBILITY GROUPS OF THE POPULATION

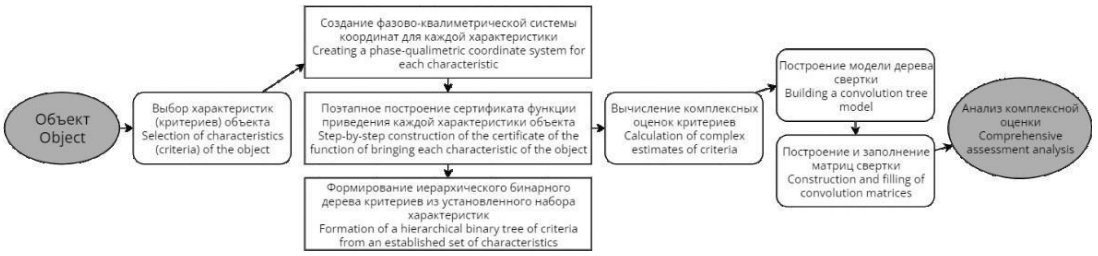
The article was received by the editorial board on 28.09.2022, in the final version – 03.10.2022.

Ovchinnikov Yaroslav A., Perm National Research Polytechnic University, 29 Komsomolsky prospekt, Perm, 614990, Russian Federation,
undergraduate, ORCID: 0002-7963-2574, e-mail: yaroslove.ovch@gmail.com
Krivogina Darya N., Perm National Research Polytechnic University, 29 Komsomolsky prospekt, Perm, 614990, Russian Federation,
Candidate Sciences (Engineering), Associate Professor, ORCID: 0001-6453-3701, e-mail: darya.krivogina@gmail.com

This paper presents a new approach to solving the problems of assessing the fitness of real estate for low-mobility groups of the population. The author presents a new approach to assessing the accessibility of public buildings for the low-mobility population, which differs in that the level of accessibility is not determined comprehensively, as in modern methods, but piecemeal. After all, as practice shows, the absence of one element can become a decisive factor in the real possibility of using and using the benefits of the object by a person. A comprehensive study of the sports and recreation complex was conducted, shortcomings were identified as the need to install some elements and the absence of a number of simulators, which is the main indicator of the quality of accessibility of the environment for sports facilities. Recommendations were proposed for improving parameters with a low integrated assessment.

Keywords: development of the mechanism, justification of the choice, technical solutions, low-mobility groups of the population, comprehensive assessment

Graphical annotation (Графическая аннотация)



Введение. Одним из актуальных направлений на сегодняшний момент является развитие доступной городской среды для всех категорий населения. С 1990 г. производятся научные исследования в области создания комфортной городской среды для маломобильных групп населения (МГН), а именно архитектурно-планировочных решений. На основании полученных исследований созданы определенные нормативные комплексы, позволяющие обеспечивать необходимые требования для формирования комфортной инфраструктуры для людей с ограниченными возможностями. С 2011 г. в Российской Федерации осуществляется государственная программа «Доступная среда», посвященная проектированию безбарьерной городской среды для МГН. К 2025 г. планируется обустроить объекты инженерной, социальной и транспортной инфраструктуры в процентном соотношении до 61,8 %.

Многие фундаментальные теоретические труды посвящены проблемам обеспечения доступной среды для инвалидов. Результаты и выводы исследования сущности, содержания и особенностей обеспечения доступной среды для маломобильных групп населения описаны в работах философов, социологов, организаторов, экономистов и практиков управления А.В. Щеголевой, А.А. Сальниковой, О.А. Никифорова, С.М. Мочалина, К.Э. Сафронова, О.П. Конышевой, С.В. Калошиной, С.А. Сазоновой, Е.А. Полуяновой, С.С. Смородиновой, М.А. Семенкиной, Н.А. Муковниной, Р.В. Николаевой, Л.Ф. Султановой, А.В. Игнатова, Д.В. Лобычева, Л.Г. Бабенко, В.Н. Армейскова, А.М. Богословенко, Е.В. Подлипинской, М.А. Танской, Т.С. Кучерововой [1–10]. Но, как показывает практика, многие объекты градостроительства, несмотря на заявленное обеспечение, не являются доступными в полной мере для МГН. Это связано с тем, что при проектировании объектов инфраструктуры отсутствует методика комплексной оценки важности приобретения (наличия) тех или иных элементов для конкретного объекта городской среды, влияющих на уровень комфортности объекта для МГН населения в целом. Порой отсутствие какого-то одного элемента доступной среды делает невозможным ее использование для целой группы МГН. К маломобильному населению относятся инвалиды-колясочники, инвалиды с нарушением опорно-двигательного аппарата, инвалиды по зрению (слепые и слабовидящие), инвалиды по слуху (глухие и слабослышащие), люди с временным нарушением здоровья, беременные женщины, люди преклонного возраста, люди с детскими колясками.

Основной задачей данного исследования является разработка нового подхода, основанного на применении специальных информационных технологий (механизмов), направленного на оценивание градостроительного объекта с позиции степени удовлетворенности уровнем его оснащенности элементами «доступной среды» МГН. Данный подход позволит на основе комплексного оценивания градостроительного объекта с позиции степени удовлетворенности уровнем его оснащенности элементами «доступной среды» принимать управленческие решения специалистам, направленные на улучшение ее эксплуатационных свойств, что повысит уровень комфортности проживания людей. Предложенный подход позволит эффективно реализовывать управленческие решения по вопросам формирования и дальнейшего обеспечения доступной среды для МГН на основе принципа «разумного приспособления». В рамках предложенного подхода необходимо объект градостроительства рассмотреть как систему «доступной среды», подразделяющуюся на ее компоненты и элементы. Это позволит комплексно оценить соответствие объекта социальной инфраструктуры критериям доступности, безопасности, информативности и комфортности, обеспечить меры предупреждения причинения вреда при формировании и дальнейшем обеспечении доступной среды.

Описание процедуры обоснования выбора технических решений объекта инфраструктуры, позволяющего оценить уровень его оснащенности с учетом требований МГН. На первоначальном этапе необходимо выбрать объект исследования. В данной работе в качестве объекта исследования выбран физкультурно-оздоровительный комплекс (ФОК), расположенный на территории Пермского края (рис. 1).

Рисунок 1 – Проект физкультурно-оздоровительного комплекса в Пермском крае

На следующем этапе необходимо провести анализ проекта ФОК, представить его в качестве системы, включающей в себя компоненты и элементы, представляющие собой необходимые приспособления и оборудование, соответствующее требованиям «доступная среда», построить данную систему как модель с деревом критериев.

Затем необходимо выполнить оценку наличия и уровня оснащенности исследуемого объекта этими элементами в соответствии со СП 59.13330.2020 «Доступность зданий и сооружений для маломобильных групп населения». Данную оценку необходимо проводить следующим образом:

- проанализировать группы маломобильного населения и выделить потребности в основных элементах «доступной среды» для ФОК и сопоставить их с требованиями СП 59.13330.2020 «Доступность зданий и сооружений для маломобильных групп населения»;
- провести социологический опрос людей, относящихся к МГН и являющихся посетителями данного ФОК на предмет удовлетворенности уровнем обеспеченности объекта приспособлениями и оборудованием;
- провести комплексное оценивание объекта и сформировать рекомендации по улучшению качества пребывания МГН в исследуемом объекте.

С целью реализации предложенного подхода необходимо разработать процедуру (механизм) комплексного оценивания, результатом которой будут рекомендации по принятию управленческих решений на основе моделирования предпочтений субъектов, относящихся к МГН. Схема обработки информации при комплексном оценивании представлена на рисунке 2.

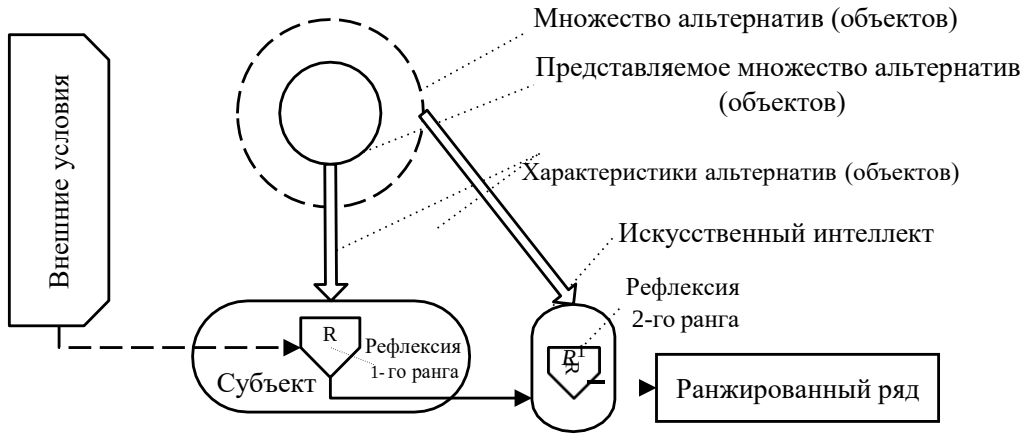


Рисунок 2 – Схема обработки информации субъектом выбора

Данный механизм комплексного оценивания должен обладать принципам неманипулируемости результатами. Для этого целесообразно сначала построить модель предпочтений субъекта выбора, а уже потом осуществлять процесс ранжирования и квантирования характеристик исследуемого объекта. Процесс построения модели предпочтений представлен на рисунке 3. Предлагаемый

механизм должен быть оснащен возможностью комплексного оценивания параметров развития как исследуемой системы в целом, так и ее отдельного элемента. Поэтому на первоначальном этапе необходимо оценить каждый элемент системы, а уже затем определить степень его влияния на комплексную оценку всей системы. С этой целью процедура комплексной оценки должна строиться на основе линейной и матричной свертках. Последовательность выполнения комплексного оценивания в программном комплексе «Джобс-Декон», основанного на линейной свертке, представлена на рисунках 3.

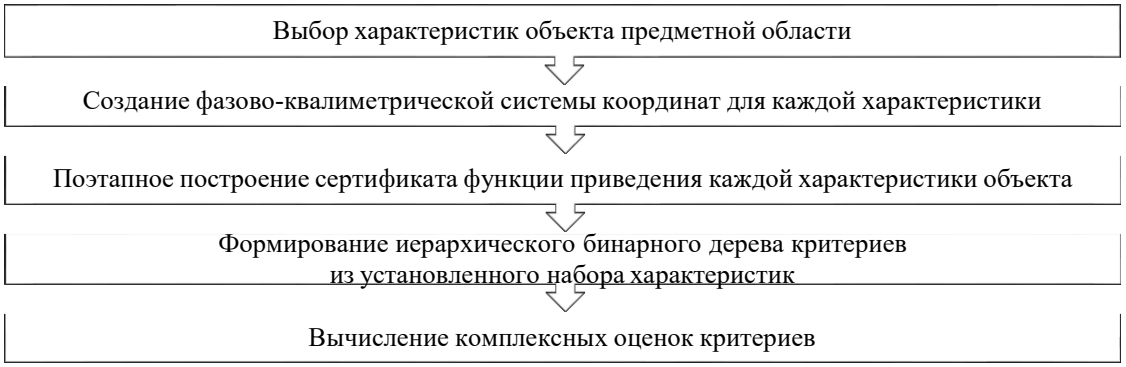


Рисунок 3 – Последовательность выполнения комплексного оценивания объектов в программном комплексе «Джобс-Декон»

После выполнения процедуры комплексного оценивания, основанного на линейной свертке, получим оценку каждого элемента в зависимости от его степени важности для конкретного объекта недвижимости. После чего осуществим комплексное оценивание всей системы и определим, какие элементы в большей степени обеспечивают ее развитие.

Последовательность выполнения комплексного оценивания в программном комплексе «Декон-Табл», основанного на матричной свертке, представлена на рисунке 4.

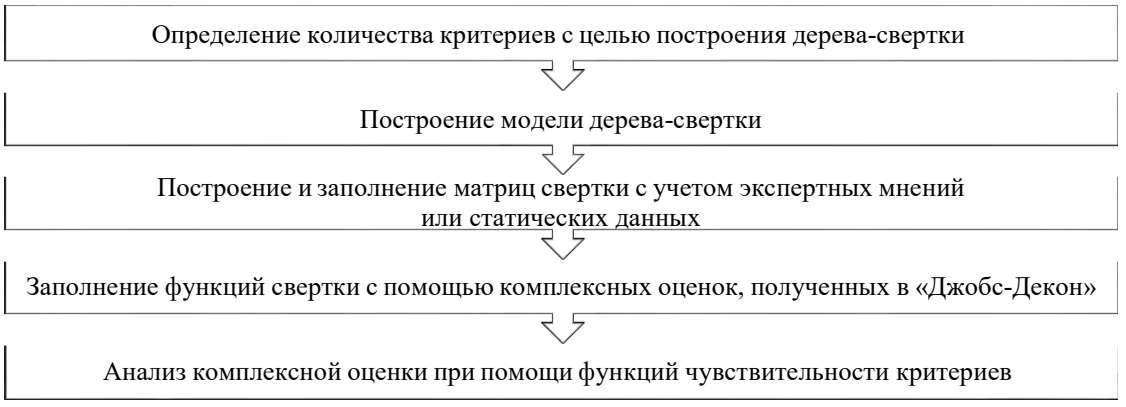


Рисунок 4 – Последовательность выполнения комплексного оценивания объектов в программном комплексе «Декон-Табл»

Построение процедуры обоснования выбора технических решений объекта инфраструктуры, позволяющего оценить уровень его оснащенности с учетом требований МГН. На сегодняшний день в Российской Федерации существует огромное количество препятствий для МГН при посещении спортивных объектов, считающихся соответствующими требованиям «доступной среды». Рассмотрим работу предложенного подхода на конкретном примере. В качестве системы рассмотрим объект, представляющий собой физкультурно-оздоровительный комплекс, недавно введенный в эксплуатацию на территории Пермского края, и оценим его на предмет доступности.

Для построения процедуры комплексного оценивания выбранный объект будем исследовать по определенным критериям (характеристикам), выявленным в ходе анализа нормативной документации и визуального осмотра здания и указанным в таблице 1.

Таблица 1 – Критерии ФОК с учетом требований МГН

Обозначение критерия	Критерий ФОК	Имеется	Имеется частично	Отсутствует	Комплексная оценка критерия
x_1	Звуковая сигнализация	+			3,77 (отлично)
x_2	Знаки для МГН	+			3,83 (отлично)
x_3	П-образные ручки на дверях	+			4,0 (отлично)
x_4	Санитарно-бытовые помещения		+		3,96 (отлично)
x_5	Колесоотбойники для предотвращения скольжения	+			4,0 (отлично)
x_6	Зоны отдыха в общественных местах		+		1,0 (неудовлетворительно)
x_7	Подъемные платформы	+			3,65 (отлично)
x_8	Парковка для инвалидов	+			3,74 (отлично)
x_9	Поручни на лестницах	+			4,0 (отлично)
x_{10}	Пандусы и (или) подъемные устройства	+			2,89 (хорошо)
x_{13}	Радиомаяки для слепых и слабовидящих		+		3,61 (отлично)
x_{14}	Зоны для МГН в спортивном зале		+		2,34 (удовлетворительно)
x_{15}	Оборудование для МГН в тренажерном зале	+		+	1,43 (неудовлетворительно)

На основе выявленных критериев построим систему «ФОК» в форме дерева критериев, в совокупности формирующих уровень доступности среды (рис. 5). Каждый из критериев сворачивается попарно, образуя новый совокупный критерий.

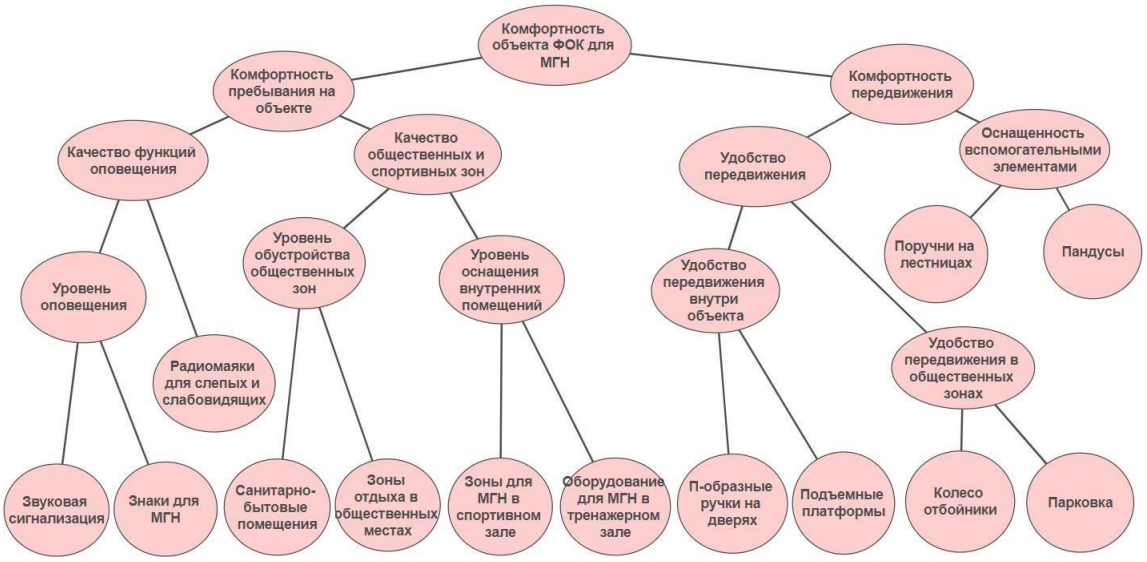


Рисунок 5 – Последовательность выполнения комплексного оценивания объектов в программном комплексе «Декон-Табл»

Из таблицы 1, полученной в ходе обследования ФОК, можно сделать вывод, что объект в большей степени приспособлен для МГН. Однако, чтобы понять, насколько элементы влияют на качество системы, необходимо каждый элемент оценить индивидуально. Для этого необходимо определить комплексные оценки каждого из критериев таблицы 1. Каждый приведенный критерий имеет свои характеристики и интервалы варьирования в фазовом (физическом) пространстве в соответствии с техническим паспортом.

Для построения модели комплексного оценивания, основанного на линейной свертке, необходимо определить взвешенные коэффициенты для этих характеристик. Это позволит определить степень важности каждого элемента в системе с позиции заинтересованных лиц. Для этого можно провести социологический опрос, который позволит определить на основе статистической обработки результатов взвешенные коэффициенты для каждого элемента и проранжировать их. В качестве респондентов были приняты посетители данного ФОК, в состав которых также входят МГН.

Для примера построения модели комплексной оценки конкретного критерия, возьмем критерий «Звуковая сигнализация»:

1. Зададим наименование критерия и определим основные характеристики (рис. 6).

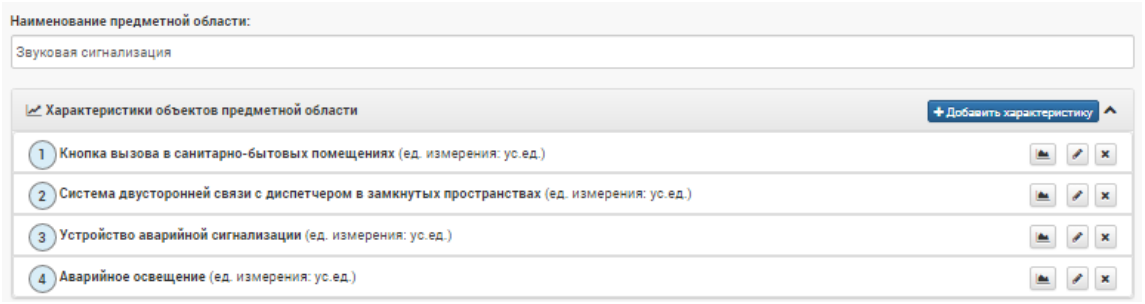


Рисунок 6 – Выбор основных характеристик объекта для МГН

2. На следующем этапе на основе нормативных документов [СП] и учета предпочтений заинтересованных лиц (респондентов ФОК) построим функции приведения для каждой выбранной характеристики. Функции приведения позволяют перевести физические значения характеристик в квалиметрическое пространство с интервалом от 1 до 4, где 1 – неудовлетворительно, 2 – удовлетворительно, 3 – хорошо и 4 – отлично. На рисунке 7 представлена функция приведения для компонента «Система двусторонней связи с диспетчером в замкнутых пространствах», где «полное отсутствие системы двусторонней связи» – оценка 1, наличие двусторонней связи только в лифте – оценка 2, наличие двусторонней связи в лифте и раздевалках – оценка 3, наличие двусторонней связи во всех замкнутых помещениях – оценка 4. Для всех критериев, представленных на рисунке 5, строятся аналогичные функции.

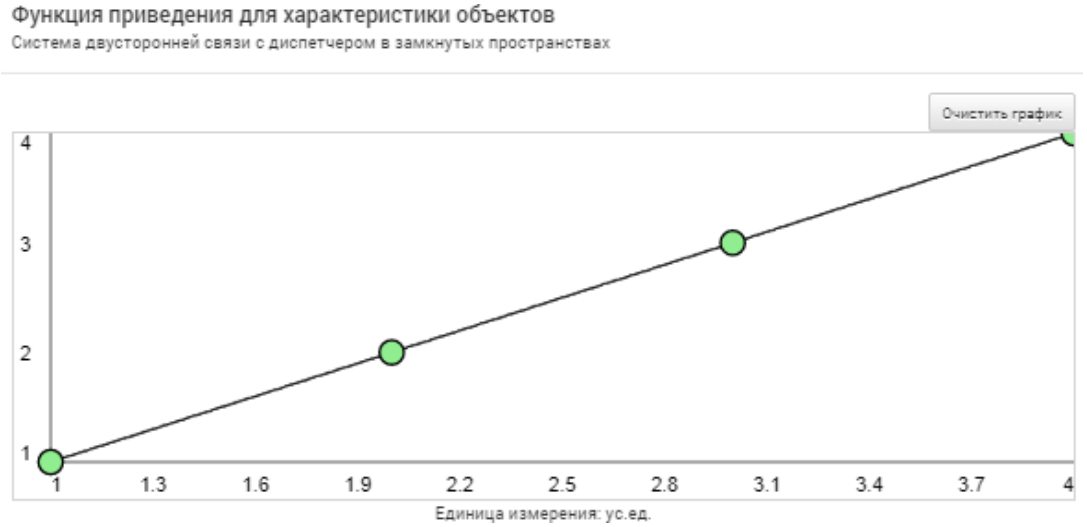


Рисунок 7 – Функция приведения для компонента «Система двусторонней связи с диспетчером в замкнутых пространствах»

3. Далее, на основе статистических данных, позволяющих определить степень важности каждого элемента, выстраиваем процедуру ранжирования (рис. 8) и определяем взвешенные коэффициенты в модели комплексного оценивания (рис. 9). Степень важности каждого элемента определяем в шкале от 0 до 10 баллов.

Рисунок 8 – Ранжирование характеристик критерия

Рисунок 9 – Определение взвешенных коэффициентов характеристик

На данном этапе можно считать, что процедура построения модели комплексной оценки для первого критерия закончена (рис. 10). Далее вводим поочередно реальные значения характеристик каждого критерия и получаем его комплексную оценку. Комплексная оценка критерия «Звуковая сигнализация» равна 3,77, что интерпретируется как «отлично». Построение моделей комплексного оценивания всех остальных критериев объекта проводится аналогично, полный перечень комплексных оценок представлен поэлементно в таблице 1.

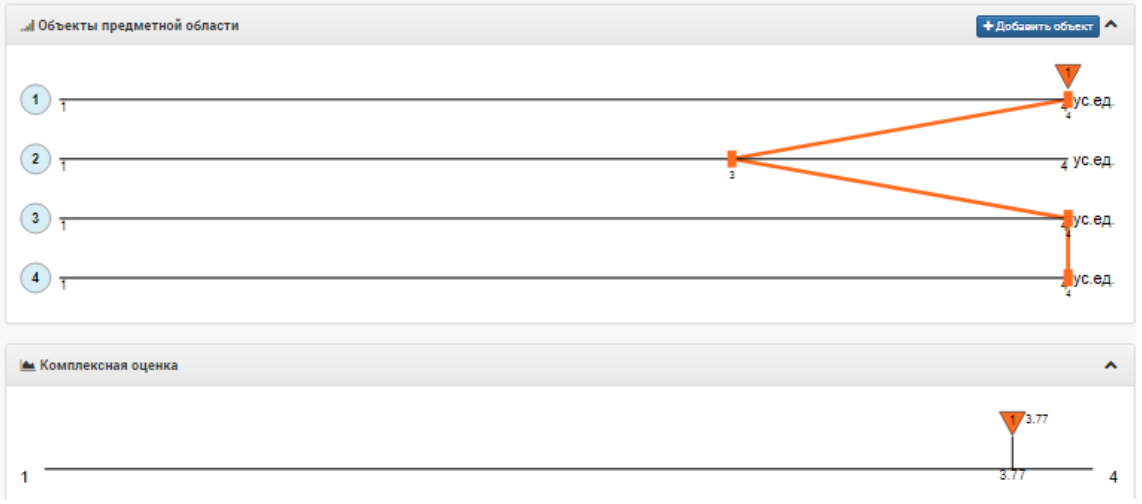
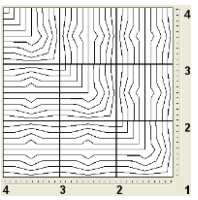
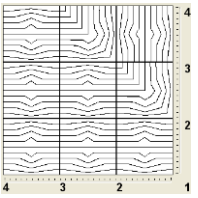
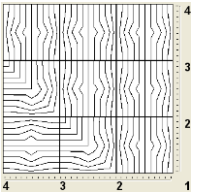
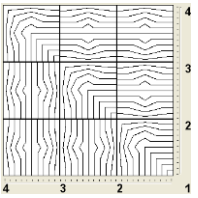
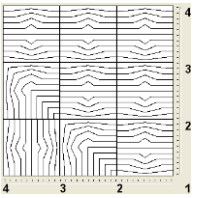
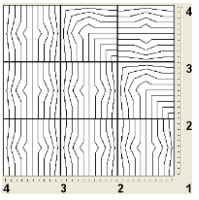
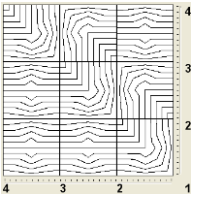
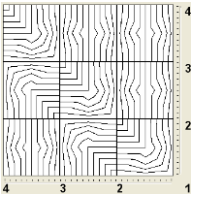


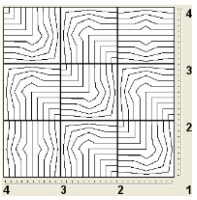
Рисунок 10 – Комплексная оценка критерия «Звуковая сигнализация»

Следующим шагом необходимо оценить уровень качества эксплуатации человеком совокупности всех перечисленных элементов в объекте. Для этого построим модель комплексного оценивания в программном комплексе «Декон-Табл», в основе которого лежит механизм матричных сверток [11]. Существует 12 базовых матриц, позволяющих описать любую ситуацию (табл. 2).

Таблица 2 – Базовые матрицы и их интерпретации

Поддержка развития обоих критериев	
Равноправное развитие критериев X1 4 3 2 1 3 3 2 1 2 2 2 1 1 1 1 1 X2	
Приоритет первого критерия X1 4 4 3 2 3 3 3 2 2 2 2 2 1 1 1 1 X2	
Приоритет второго критерия X1 4 3 2 1 4 3 2 1 3 3 2 1 2 2 2 1 X2	
Поддержка развития хотя бы одного критерия	
Равноправное развитие критериев X1 4 4 4 3 4 3 3 3 4 3 2 2 4 3 2 1 X2	
Приоритет первого критерия X1 4 4 4 4 3 3 3 3 3 2 2 2 3 2 1 1 X2	
Приоритет второго критерия X1 4 3 3 3 4 3 2 2 4 3 2 1 4 3 2 1 X2	
Поддержка развития обоих критериев с компромиссом на одного из них	
Первого X1 4 3 3 3 3 3 2 2 2 2 2 1 1 1 1 1 X2	
Второго X1 4 3 2 1 3 3 2 1 3 2 2 1 3 2 1 1 X2	

Продолжение таблицы 2

Любого X1 4 3 3 3 3 3 2 2 3 2 2 1 3 2 1 1 X2	

Следующим шагом внесем реальные значения комплексных оценок каждого критерия, полученных в программном комплексе «Джобс-Декон» (рис. 11).

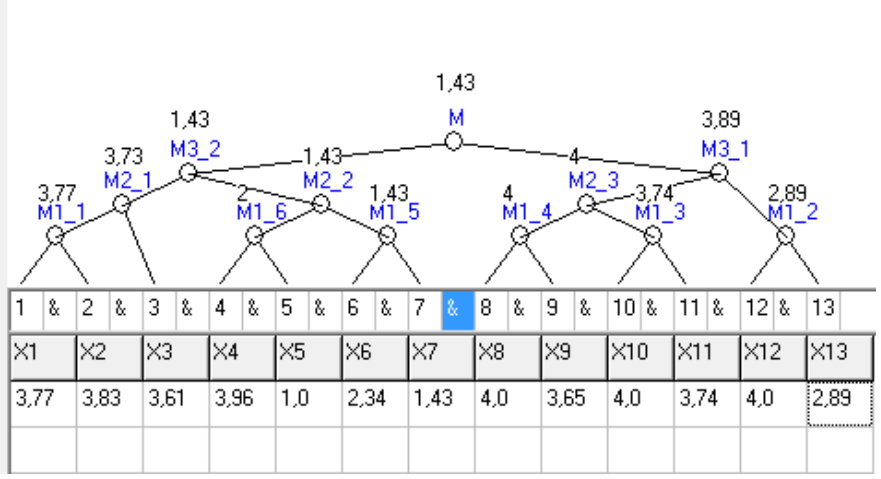


Рисунок 11 – Дерево-свертка модели комплексного оценивания

1. После построения дерева подходим ко второму этапу построения модели – построение матриц свертки.

Разберем сворачивание матриц на примере матрицы М (комфортность объекта ФОК для МГН). У данной матрицы есть два критерия: комфортность передвижения и комфортность пребывания на объекте. Матрица заполняется с учетом экспертных мнений (статистических данных). Для наиболее благоприятных условий нам необходимо увеличение обоих критериев. Поэтому заполняем матрицы следующим образом (рис. 12).

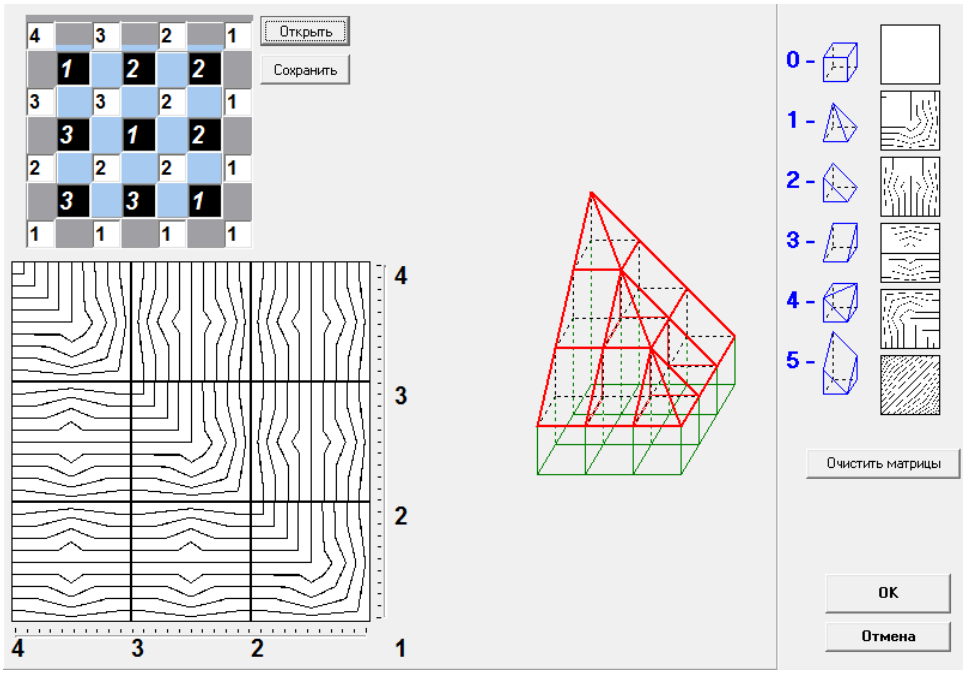


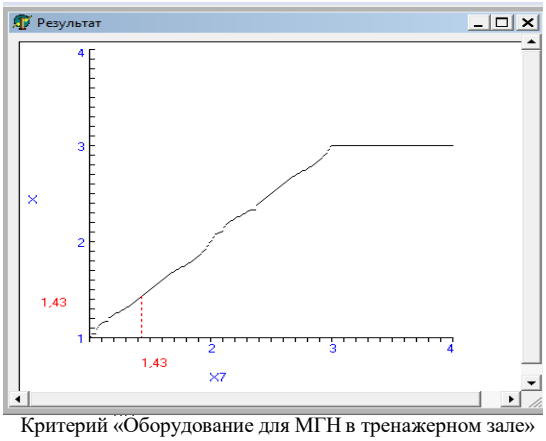
Рисунок 12 – Матрица свертки вершины М

Для вершин M1_1– M1_5 матрицы будут заполняться, как указано на рисунке 12. Такое заполнение матриц обусловлено статистическими данными.

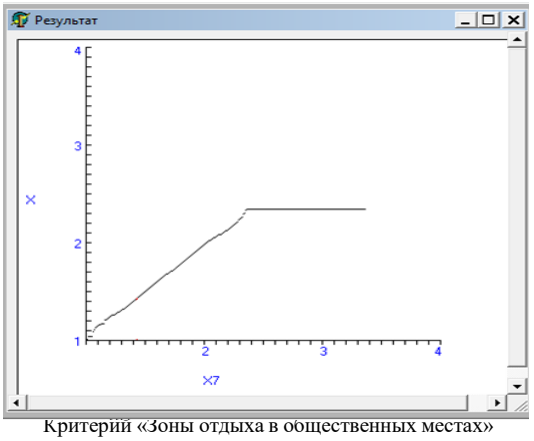
Функция свертки. Функция свертки необходима для получения комплексной оценки модели. В поле критериев заполняем табличную форму. Получаем значения свертки критериев, которые указываются у матриц свертки.

Из результатов вычислений видно, что комплексная оценка, описывающая комфортность объекта для МГН, равна 1,43. Это показывает его текущее состояние. На сегодняшний момент ФОК не развит по некоторым показателям.

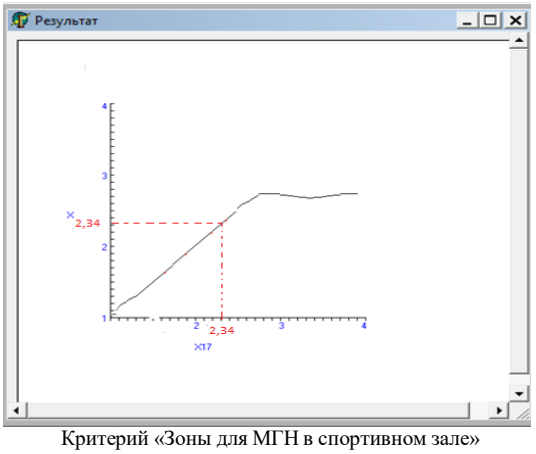
Далее мы проанализируем пути улучшения проекта ФОК с учетом требований МГН, с помощью использования инструментальных средств программного комплекса «Декон-Табл», позволяющих проанализировать функции чувствительности. На рисунке 13 представлены функции чувствительности критериев, которыми можно управлять.



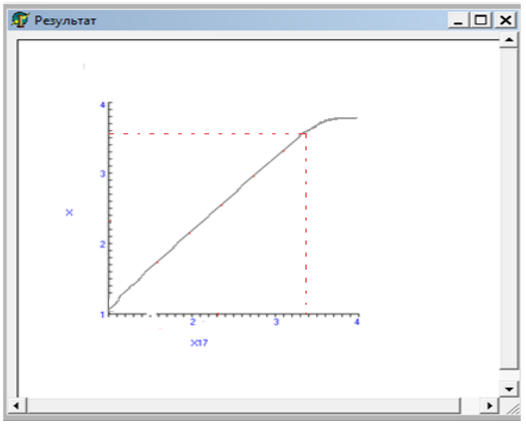
Критерий «Оборудование для МГН в тренажерном зале»



Критерий «Зоны отдыха в общественных местах»



Критерий «Зоны для МГН в спортивном зале»



Критерий «Радиомаяки для слепых и слабовидящих»

Рисунок 13 – Функция чувствительности критериев, которыми можно управлять

На основе применения данного механизма можно сделать следующие рекомендации в отношении улучшения данных критериев (рис. 14):

1. Критерий «Оборудование для МГН в тренажерном зале»: переоснащение тренажерного зала с учетом требований для МГН за счет установки специализированного тренажерного оборудования.

2. Критерий «Зоны отдыха в общественных местах»: устройство мест отдыха на территории ФОК при помощи специальных скамей.

3. Критерий «Зоны для МГН в спортивном зале»: организация дополнительных мест для МГН в спортивном зале ФОК.

4. Критерий «Радиомаяки для слепых и слабовидящих»: дооснащение объекта звуковыми маяками с беспроводной кнопкой.

Рисунок 14 – Рекомендации в отношении улучшения критериев

Заключение. В данной научной работе была рассмотрена и оценена существующая на данном этапе инфраструктура для маломобильных групп населения, а именно: были проанализированы группы маломобильного населения и была выделена группа определенных потребностей в основных элементах инфраструктуры города, которые необходимы для обеспечения комфортного пребывания на объекте. Также было отмечено, что улучшение качества доступной среды позволит избежать негативных последствий физического и социального барьера для маломобильных групп населения и улучшит качество проживания всего населения города.

В качестве примера был выбран объект ФОК, находящийся в Пермском крае, для исследования и проведения анализа критериев объекта инфраструктуры на наличие необходимых элементов социальной инфраструктуры.

Были построены две модели комплексного оценивания, позволяющие оценить необходимый объект на соответствие требованиям маломобильных групп населения и наличие конкретных элементов доступной среды. С помощью полученных оценок и использования инструментальных средств программного комплекса «Декон-Табл», позволяющих проанализировать функции чувствительности, сделаны рекомендации по повышению комфортности пребывания маломобильных групп населения на объекте ФОК.

Перспективными направлениями продолжения научной работы можно считать увеличение количества критериев в процедуре комплексного оценивания, а также репрезентативность выборки социального опроса для более точной комплексной оценки.

Библиографический список

1. Щеголева, А. В. Формирование доступной среды для маломобильных групп населения (на примере учебных корпусов ННГАСУ) / А. В. Щеголева, А. А. Сальникова // Приволжский научный журнал. – 2020. – № 1 (53). – С. 253–264.

2. Никифоров, О. А. О цифровизации маршрутов передвижения маломобильных групп населения / О. А. Никифоров, С. М. Мочалин, К. Э. Сафронов // III Бетанкуровский международный инженерный форум : сборник трудов, Санкт-Петербург, 02–03 декабря 2021 года. – Санкт-Петербург : Петербургский государственный университет путей сообщения Императора Александра I, 2021. – С. 49–51.

3. Конышева, О. П. Анализ проблемы доступности городской среды для маломобильной группы населения (МГН) / О. П. Конышева // Научному прогрессу – творчество молодых. – 2021. – № 3. – С. 59–61.

4. Калошина, С. В. Анализ доступности жилых и общественных зданий для маломобильных групп населения на территории города Перми / С. В. Калошина, С. А. Сазонова, Е. А. Полуянова // Известия Казанского государственного архитектурно-строительного университета. – 2020. – № 4 (54). – С. 204–213.

5. Смородина, С. С. Оценка состояния доступности объектов социальной инфраструктуры для маломобильных групп населения / С. С. Смородина // Техника и технологии строительства. – 2021. – № 1 (25). – С. 19–23.

6. Семенкина, М. А. Развитие услуг транспортной инфраструктуры для маломобильных групп населения / М. А. Семенкина, Н. А. Муковнина // Наука и образование транспорту. – 2019. – № 1. – С. 169–172.

7. Николаева, Р. В. Формирование доступной городской среды с учетом жизнедеятельности маломобильных групп населения / Р. В. Николаева, Л. Ф. Султанова // Техника и технология транспорта. – 2021. – № 3 (22).

8. Игнатов, А. В. К вопросу об оценке доступности городского наземного пассажирского транспорта для маломобильных групп населения / А. В. Игнатов, Д. В. Лобычев // Техническое регулирование в транспортном строительстве. – 2022. – № 2 (53). – С. 83–89.

9. Исследование условий доступности городской среды для маломобильных групп населения на примере города шахты Ростовской области / Л. Г. Бабенко, В. Н. Армейсков, А. М. Богословенко, Е. В. Подлипинская // Перспективные технологии в строительстве и техносферной безопасности : сборник научных трудов. Шахты, 25 ноября 2020 года / Институт сферы обслуживания и предпринимательства (филиал) федер. гос. бюджет. образоват. учреждения высш. образования «Донской государственный технический университет» в г. Шахты Ростовс. обл. – Шахты : ИСОиП (филиал) ДГТУ в г. Шахты, 2020. – С. 4–10.

10. Танская, М. А. Оценка доступности территории и адаптация городского пространства для маломобильных групп населения на примере города Омска / М. А. Танская, Т. С. Кучерова // Человек. Социум. Общество. – 2021. – № 4. – С. 58–64.

11. Харитонов В. А. Функциональные возможности механизмов комплексного оценивания с топологической интерпретацией матриц свертки / В. А. Харитонов, И. Р. Винокур, А. А. Белых // Управление большими системами : сборник трудов. – 2007. – № 18. – С. 129–140.

References

1. Shchegoleva, A. V., Salnikova, A. A. Formirovanie dostupnoy sredy dlya malomobilnykh grupp naseleniya (na primere uchebnykh korpusov NNGASU) [Creating an accessible environment for people with limited mobility (by the example of the nngasu academic buildings)]. *Privolzhskiy nauchnyy zhurnal* [Volga Scientific Journal], 2020, no. 1(53), pp. 253–264.

2. Nikiforov, O. A., Mochalin, S. M., Safronov, K. E. O tsifrovizatsii marshrutov peredvizheniya malomobilnykh grupp naseleniya [About digitalization of routes of movement of low-mobility groups of the population]. *III Betankurovskiy mezhdunarodnyy inzhenernyy forum : sbornik trudov, Sankt-Peterburg, 02–03 dekabrya 2021 goda* [III Betancourt International Engineering Forum : Proceedings, St. Petersburg, 02–03 December 2021. – St. Petersburg, St. Petersburg State University of Railways of Emperor Alexander I, 2021, pp. 49–51.

3. Konysheva, O. P. Analiz problemy dostupnosti gorodskoy sredy dlya malomobilnoy gruppy naseleniya (MGN) [Analysis of the problem of accessibility of the urban environment for a low-mobility group of the population (MGN)]. *Nauchnomu progressu – tvorchestvo molodykh* [Scientific progress – creativity of the young], 2021, no. 3, pp. 59–61.

4. Kaloshina, S. V., Sazonova, S. A., Poluyanova, E. A. Analiz dostupnosti zhilykh i obshchestvennykh zdaniy dlya malomobilnykh grupp naseleniya na territorii goroda Permi [Analysis of accessibility of residential and public buildings for low-mobility groups of the population on the territory of the city of Perm]. *Izvestiya Kazanskogo gosudarstvennogo arhitekturno-stroitelnogo universiteta* [Proceedings of the Kazan State University of Architecture and Civil Engineering], 2020, no. 4 (54), pp. 204–213.

5. Smorodina, S. S. Otsenka sostoyaniya dostupnosti obektov socialnoy infrastruktury dlya malomobilnykh grupp naseleniya [Assessment of the state of accessibility of social infrastructure facilities for low-mobility groups of the population]. *Tekhnika i tekhnologii stroitelstva* [Technique and Technologies of Construction], 2021, no. 1 (25), pp. 19–23.

6. Semenkina, M. A., Mukovnina, N. A. Razvitie uslug transportnoy infrastruktury dlya malomobilnykh grupp naseleniya [Development of transport infrastructure services for low-mobility groups of the population]. *Nauka i obrazovanie transport* [Science and Education for Transport], 2019, no. 1, pp. 169–172.

7. Nikolaeva, R. V., Sultanova, L. F. Formirovanie dostupnoy gorodskoy sredy s uchetom zhiznedeyatelnosti malomobilnykh grupp naseleniya [Formation of an accessible urban environment taking into account the vital activity of low-mobility groups of the population]. *Tekhnika i tekhnologiya transporta* [Transport Equipment and Technology], 2021, no. 3 (22).

8. Ignatov, A. V., Lobychev, D. V. K voprosu ob otsenke dostupnosti gorodskogo nazemnogo passazhirskogo transporta dlya malomobilnykh grupp naseleniya [On the issue of assessing the accessibility of urban ground passenger transport for low-mobility groups of the population]. *Tekhnicheskoe regulirovanie v transportnom stroitelstve* [Technical Regulation in Transport Construction], 2022, no. 2 (53), pp. 83–89.

9. Babenko, L. G., Armeyskov, V. N., Bogoslovenko, A. M., Podlipinskaya, E. V. Issledovanie usloviy dostupnosti gorodskoy sredy dlya malomobilnykh grupp naseleniya na primere goroda shakhty Rostovskoy oblasti [Study of the conditions of accessibility of the urban environment for low-mobility groups of the population on the example of the city of Shakhty, Rostov region]. *Perspektivnye tekhnologii v stroitelstve i tekhnosfernoy bezopasnosti : sbornik nauchnykh trudov, Shakhty, 25 noyabrya 2020 goda* [Promising technologies in construction and technosphere safety : collection of scientific papers. Shakhty, November 25, 2020]. Shakhty, ISOiP (branch) of DSTU in Shakhty, 2020, p. 4–10.

10. Tanskaya, M. A., Kucherova, T. S. Otsenka dostupnosti territorii i adaptatsiya gorodskogo prostranstva dlya malomobilnykh grupp naseleniya na primere goroda Omska [Assessment of accessibility of the territory and adaptation of urban space for low-mobility groups of the population on the example of the city of Omsk]. *Chelovek. Sotsium. Obshchestvo* [Human. Socium. Society], 2021, no. 4, pp. 58–64.

11. Kharitonov, V. A., Vinokur, I. R., Belykh, A. A. Funktsionalnye vozmozhnosti mekhanizmov kompleksnogo otsenivaniya s topologicheskoy interpretatsiey matrits svertki [Functional capabilities of complex estimation mechanisms with topological interpretation of convolution matrices]. Upravlenie bolshimi sistemami : sbornik trudov [Management of large systems : proceedings], 2007, no. 18, pp. 129–140.

DOI 10.54398/20741707_2022_4_59
УДК 004.001

АВТОМАТИЗАЦИЯ ПОИСКА ТЕХНОЛОГИЧЕСКИХ ПАРТНЕРОВ ДЛЯ ПРОВЕДЕНИЯ НИОКР[1]

Статья поступила в редакцию 28.09.2022, в окончательном варианте – 17.10.2022.

Коробкин Дмитрий Михайлович, Волгоградский государственный технический университет, 400005, Российская федерация, г. Волгоград, пр. имени В.И. Ленина, 28,
кандидат технических наук, доцент, ORCID: 0000-0002-4684-1011, e-mail: dkorobkin80@mail.ru
Фоменков Сергей Алексеевич, Волгоградский государственный технический университет, 400005, Российская федерация, г. Волгоград, пр. имени В.И. Ленина, 28,
доктор технических наук, профессор, ORCID: 0000-0001-9907-4488, e-mail: saf550@yandex.ru
Бородин Николай Юрьевич, Волгоградский государственный технический университет, 400005, Российская федерация, г. Волгоград, пр. имени В.И. Ленина, 28,
студент, ORCID: 0000-0003-3561-1111, e-mail: mr.kolyamba99@yandex.ru
Верещак Григорий Алексеевич, Волгоградский государственный технический университет, 400005, Российская федерация, г. Волгоград, пр. имени В.И. Ленина, 28,
аспирант, ORCID: 0000-0002-4545-6306, e-mail: grigoryg37@gmail.com

В настоящее время компании по-прежнему в значительной степени полагаются на экспертные знания при выборе партнеров по исследованиям и разработкам (НИОКР), но технологии развиваются, и возникает возможность автоматизировать данный процесс. Автоматизация процесса позволит компаниям или частным лицам самостоятельно искать коллег, ведущих работу в смежной предметной области, экономя ресурсы, которые обычно тратятся на анализ патентных данных экспертом. В данной работе предложен метод извлечения из патентных документов USPTO семантических структур Subject-Action-Object и поиска на их основе потенциальных технологических партнеров. Описаны алгоритмы парсинга патентных массивов, извлечения структур SAO и формирования структур «Проблема – Решение», определения схожести технологических проблем и поиска технологических партнеров. Поиск технологических партнеров выполняется на основе технологических проблем и структур «Проблема – Решение». Предложенный метод реализован в виде программного модуля и апробирован на патентах ведомства по патентам и товарным знакам США.

Ключевые слова: патенты, обработка текстов на естественном языке, извлечение информации, SAO

AUTOMATION OF THE SEARCH FOR TECHNOLOGICAL PARTNERS FOR R&D

The article was received by the editorial board on 28.09.2022, in the final version – 17.10.2022.

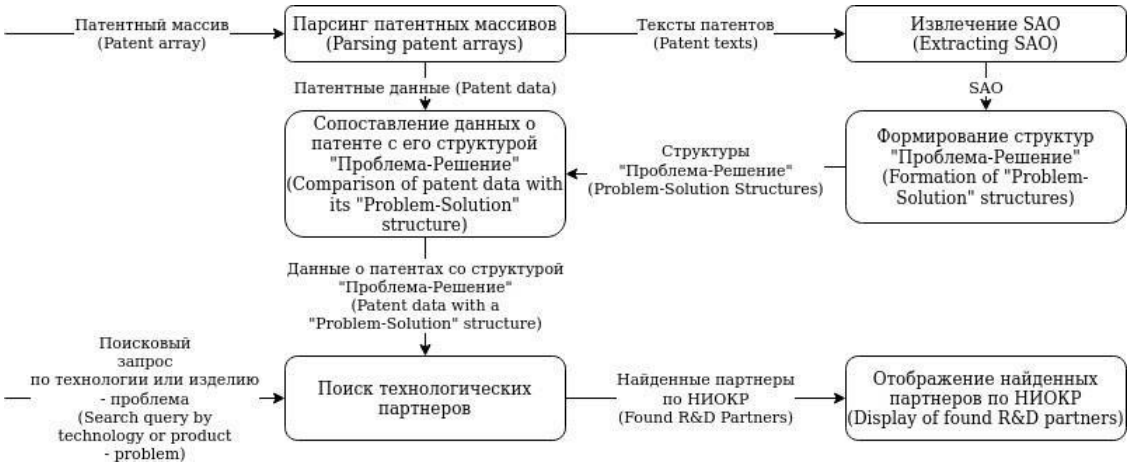
Korobkin Dmitry M., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-4684-1011, e-mail: dkorobkin80@mail.ru
Fomenkov Sergey A., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
Doct. Sci. (Engineering), Professor, ORCID: 0000-0001-9907-4488, e-mail: saf550@yandex.ru
Borodin Nikolay Yu., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
student, ORCID: 0000-0003-3561-1111, e-mail: mr.kolyamba99@yandex.ru
Vereschak Grigory A., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
post-graduate student, ORCID: 0000-0002-4545-6306, e-mail: grigoryg37@gmail.com

Currently, companies still rely heavily on expert knowledge when choosing research and development (R&D) partners, but technologies are evolving and it is possible to automate this process. Automation of the process will allow companies or individuals to independently search for colleagues working in a related subject area, saving resources that are usually spent on the analysis of patent data by an expert. In this paper, a method is proposed for extracting Subject-Action-Object semantic structures from USPTO patent documents and searching for potential technological partners based on them. Algorithms for parsing patent arrays, extracting SAO structures and forming "Problem – Solution" structures, determining the similarity of technological problems and searching for technological partners are described. The search for technological partners is carried out on the basis of technological problems and "Problem – Solution" structures. The proposed method is implemented in the form of a software module and tested on patents of the U.S. Patent and Trademark Office.

Keywords: patents, natural language processing, information extraction, SAO

[1] Исследование выполнено за счет гранта Российского научного фонда № 22-21-20125, https://rscf.ru/project/22-21-20125/, и от Волгоградской области.

Graphical annotation (Графическая аннотация)



Введение. Процесс генерации новых технических решений, поиск аналогов на разработанную технологию и анализ технологических трендов могут быть упрощены за счет анализа существующей патентной базы [1, 2]. Но в настоящее время компании по-прежнему в значительной степени полагаются на экспертные знания при выборе партнеров по исследованиям и разработкам (НИОКР). От экспертов требуется выполнять патентный поиск, который в настоящее время осуществляется с помощью электронных информационно-поисковых систем. В силу большого количества и сложности электронных баз поиск является трудоемким процессом. Несмотря на то, что поиск при помощи электронных баз в сети Интернет считается достаточно полным и объективным, существует потребность в ручном поиске путем детального анализа полученной информации. На ознакомление с проблемой и анализ патентов экспертом затрачиваются такие ресурсы, как время и деньги заинтересованного лица. Существующий поисковый процесс изображен на рисунке 1.

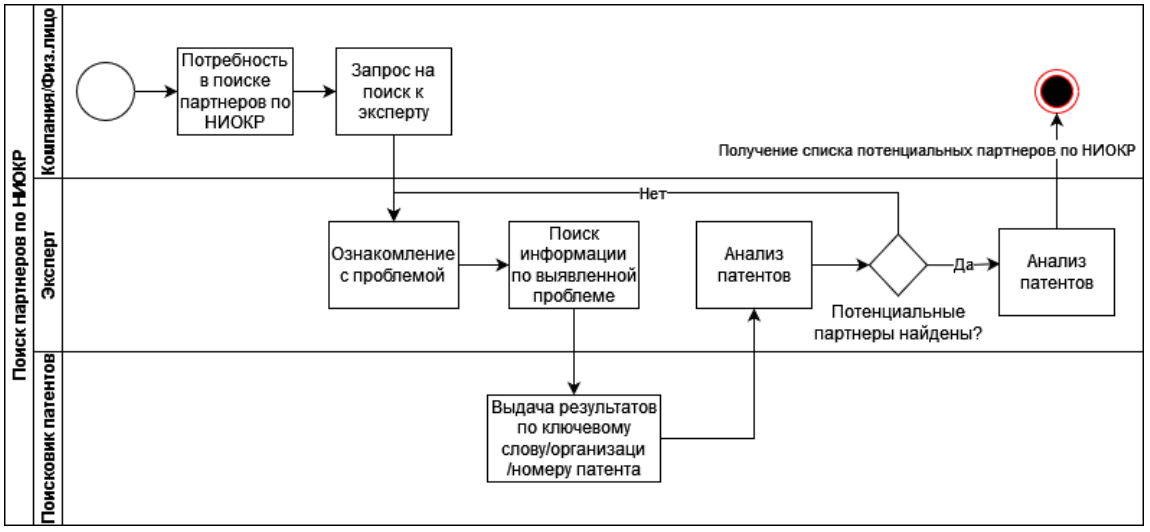


Рисунок 1 – Процесс поиска партнеров по НИОКР на текущий момент

С развитием технологий возникает возможность в автоматизации процесса поиска партнеров по НИОКР. Автоматизация процесса поиска позволит компаниям или частным лицам самостоятельно искать коллег, ведущих работу в смежной предметной области, экономя ресурсы, которые обычно тратятся экспертом на анализ патентных данных. На рисунке 2 изображен автоматизированный процесс поиска партнеров по НИОКР.

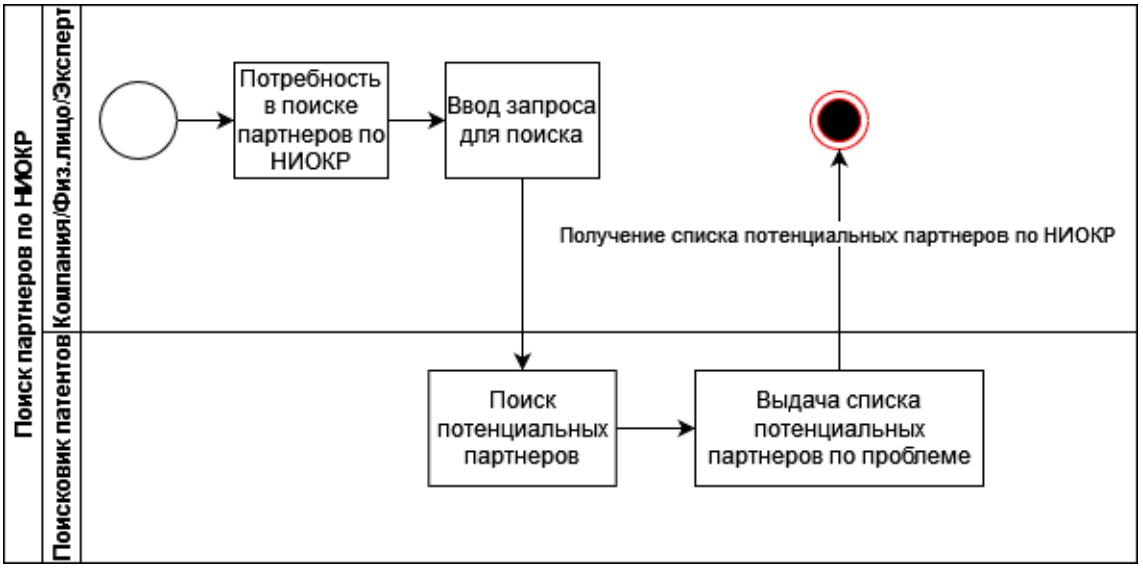


Рисунок 2 – Автоматизированный процесс поиска партнеров по НИОКР

Автоматизированный процесс позволит компаниям или физическим лицам избавиться от посредника в виде эксперта при поиске технологических партнеров по НИОКР, а экспертам, в свою очередь, ускорить процесс нахождения потенциальных единомышленников для клиентов.

Для повышения качества извлечения данных в [3] отмечается необходимость изучения структуры патентного документа. В [4] анализировались пользовательские отзывы к патенту для определения инновационного потенциала. Из пользовательских отзывов можно извлечь информацию о технологии, указанной в патенте, и окрас реакции пользователей. В [5] предложен метод определения инновационного потенциала в виде опросного листа по патенту – «Инновационный радар». Инновационный потенциал определяется в виде опросного листа по патенту. В [6] описывается методика определения технологии с высоким потенциалом, закрепленной в патенте, – Technology Opportunity Discovery. Для этого используется кластеризация патентов по ключевым словам.

Одним из распространенных способов извлечения и анализа технологии, закрепленной в патенте, является использование модели Subject-Action-Object (SAO). Модель SAO для извлечения информации из англоязычных патентов используется в [7, 8, 9]. В [10] проверяется близость технологии к технологическому тренду посредством извлечения матричных векторов, состоящих из структур SAO. В [11] создаются терм-документные матрицы на основе структур SAO, где документами являются патенты, а термами – структуры SAO. Инновационный потенциал представлен относительным размером тематического кластера.

В данной работе предлагается метод извлечения из патентных документов USPTO [12] семантических структур SAO, использующихся для формирования структур «Проблема – Решение», и поиска на их основе потенциальных технологических партнеров.

Основная идея разработанного метода заключается в том, что поиск партнеров по НИОКР будет выполняться на основе сходства технологической проблемы, задаваемой в поисковом запросе, и заранее подготовленных структур «Проблема – Решение», извлеченных из патентного массива и хранящихся в базе данных. В ответ на поисковый запрос будет предоставляться список схожих проблем и решений, представленных другими компаниями. На основе этого списка предполагается дальнейшее взаимодействие и сотрудничество. На рисунке 3 изображена диаграмма потоков данных.

Разработанный метод включает в себя парсинг патентных массивов, извлечение структур SAO и формирование структур «Проблема – Решение», определение схожести технологических проблем.

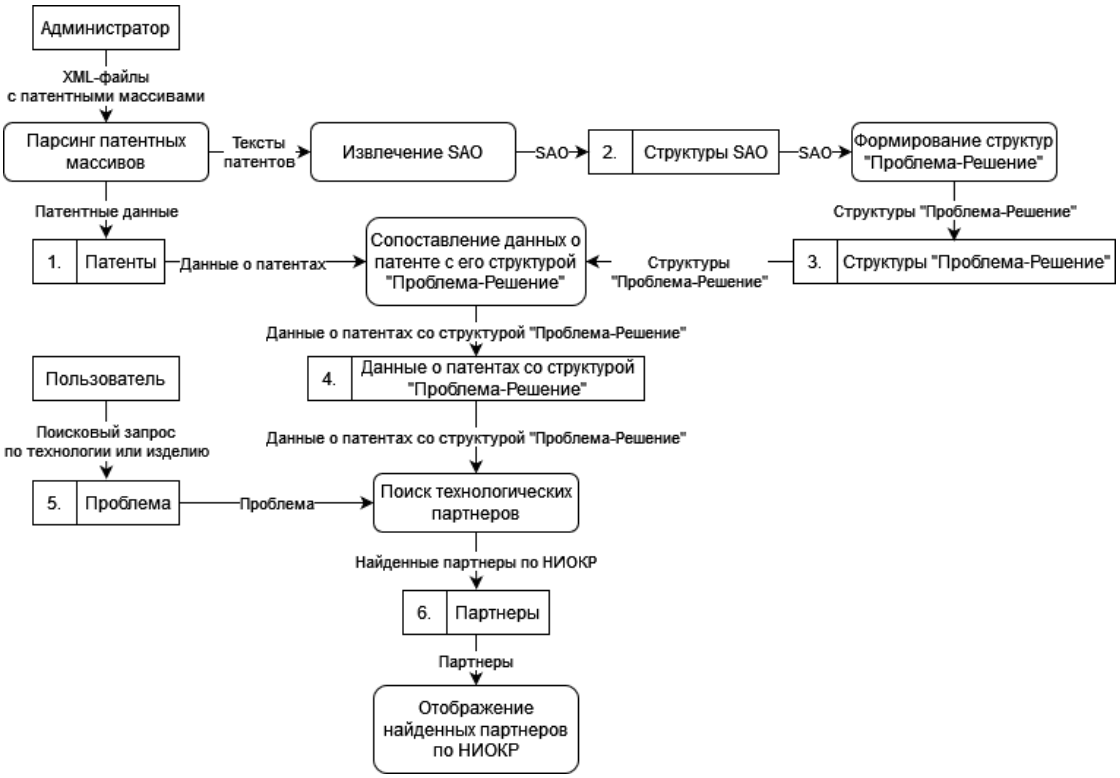


Рисунок 3 – Диаграмма потоков данных

Алгоритм парсинга патентных массивов. На вход алгоритма поступает список загруженных патентных массивов USPTO в формате XML. Каждый такой патентный массив содержит в себе описания патентных документов в XML-формате, где перед каждый новым патентным документом есть объявление, что это XML. Именно поэтому изначальный патентный массив не является валидным XML-файлом.

Данные, извлекаемые из патентных документов, – текст, фирма-регистратор, номер, класс патента, изобретатели. Данные извлекаются из соответствующих тегов. Текст патентного документа извлекается из тегов abstract, claim, description. Фирма-регистратор патента указана в теге orgname внутри тега assignes. Уникальным номером патента считается номер из тега doc_number тега application-reference. На рисунке 4 изображен алгоритм парсинга патентных массивов.

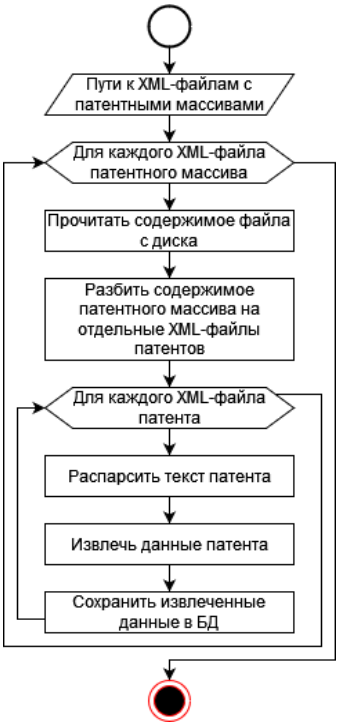


Рисунок 4 – Алгоритм парсинга патентных массивов

Извлеченная информация сохраняется в базу данных для дальнейшей обработки.

Алгоритм извлечения структур SAO. На вход алгоритма поступают извлеченные на предыдущем этапе данные – тексты тегов abstract и description патентных документов. Из текстов указанных тегов извлекаются структуры «Subject-Action-Object».

Для извлечения структур SAO необходима предварительная обработка текста. Предобработка текста включает в себя разбиение текста на предложения; токенизацию предложений; фильтрацию предложений, содержащих запрещенные слова; сегментацию предложений, при которой отсекается та часть предложения, которая не имеет ценность при извлечении структур SAO. Сегментированные предложения разбираются при помощи StanzA. Анализируются связи между токенами и принадлежность токенов к определенным частям речи. Принимается, что Action – это VERB; Object – nmod, obj, obl и их дочерние элементы; Subject – nsubj и его дочерние элементы. На рисунке 5 можно увидеть пример разбора предложения с помощью Stanza.

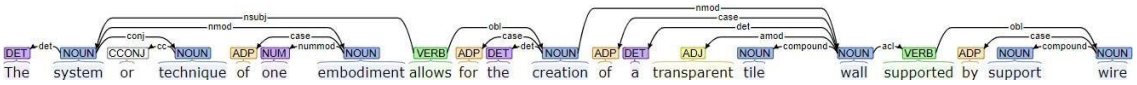


Рисунок 5 – Разбор предложения с помощью Stanza

Извлеченные структуры SAO сохраняются в базу данных. Общий алгоритм извлечения структур SAO изображен на рисунке 6.

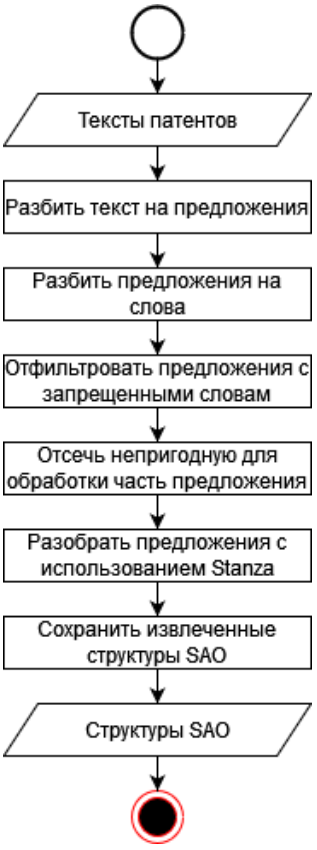


Рисунок 6 – Алгоритм извлечения структур SAO

Для формирования структур «Проблема – Решение» используются сохраненные структуры SAO. Принимается, что «Проблема» состоит из двух частей – Action и Object структуры SAO, а «Решение» – Subject. Таким образом, каждый извлеченный триплет SAO содержит в себе описание проблемы и ее решение. Алгоритм формирования структур «Проблема – Решение» изображен на рисунке 7.

Рисунок 7 – Алгоритм формирования структур «Проблема – Решение»

Алгоритм определения схожести технологических проблем. На вход алгоритма поступает поисковый запрос с описанием искомой проблемы. Строка с поисковым запросом разбирается при помощи Stanza. Аналогично поиску структур «Проблема – Решение», из поискового запроса извлекаются Action и Object. Алгоритм определения схожести технологических проблем представлен на рисунке 8.

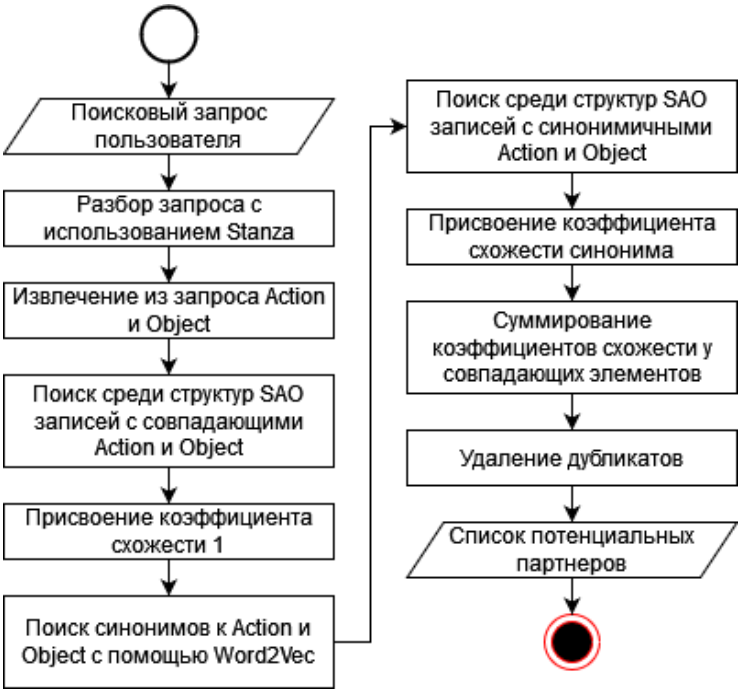


Рисунок 8 – Алгоритм определения схожести технологических проблем

Сохраненные ранее триплеты SAO сопоставляются с Action и Object поискового запроса. Если соответствующие строки Action совпадают с Action поискового запроса, то присваивается коэффициент схожести со значением 1. Аналогично для Object – если соответствующие строки Object совпадают, то присваивается коэффициент схожести со значением 1.

Помимо точного совпадения выполняется поиск по синонимам с помощью модели Word2Vec. При нахождении синонимов для Object поискового запроса из таблицы SAO по полю Object присваивается коэффициент схожести контекстного синонима к исходному слову. Аналогично для Action – если найден синоним Action из поискового запроса в поле Action таблицы SAO, то присваивается коэффициент схожести контекстного синонима к исходному слову.

Найденные записи SAO, соответствующие поисковому запросу, дополнительно обрабатываются. При нахождении повторяющихся SAO их коэффициенты суммируются. Поскольку из одного патентного документа может быть извлечено несколько записей SAO, найденные записи SAO необходимо отфильтровать по уникальному идентификатору патента. Если были найдены несколько SAO, соответствующих одному и тому же патенту, оставляется только SAO с наибольшим коэффициентом схожести, остальные удаляются.

На выходе алгоритма список потенциальных партнеров, работавших над искомой проблемой.

Результаты. Разработанный метод реализован в виде программного модуля. Программный модуль включает в себя 4 блока:

1) блок парсинга патентного xml-массива;
2) блок формирования структур «Проблема – Решение»;
3) блок поиска технологических партнеров;
4) веб-интерфейс пользователя.

На рисунке 9 изображена архитектура разработанного программного модуля.

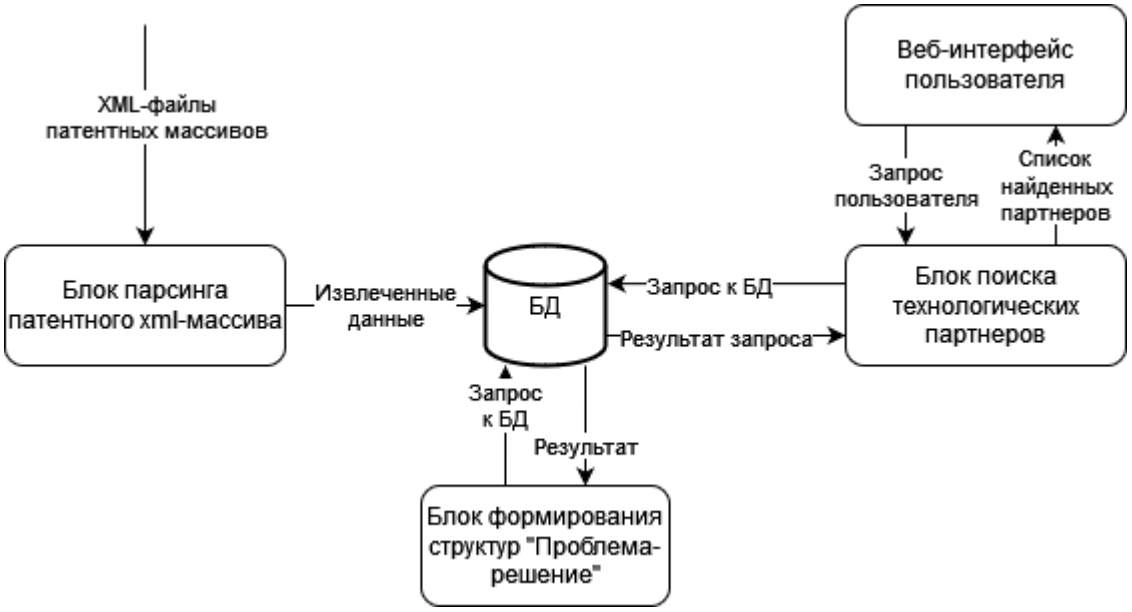


Рисунок 9 – Архитектура программного модуля

Программный модуль реализован на языке программирования Python. Для парсинга xml-файлов использована библиотека Beautiful Soup. Структуры SAO извлекаются при помощи Stanza – библиотеки для анализа естественного языка на Python. Для создания модели, необходимой для поиска синонимов и выявления схожести технологических проблем, использована библиотека тематического моделирования Gensim. Визуальная составляющая реализована на фреймворке Django в виде веб-приложения с использованием CSS-фреймворка Bootstrap. Для структуризации и хранения данных используется реляционная база данных PostgreSQL.

Программный модуль был апробирован на патентных документах USPTO за 2010–2020 гг. На рисунке 10 изображен результат работы модуля на введенный пользовательский запрос «reducing capacity».

Поиск технологических партнеров

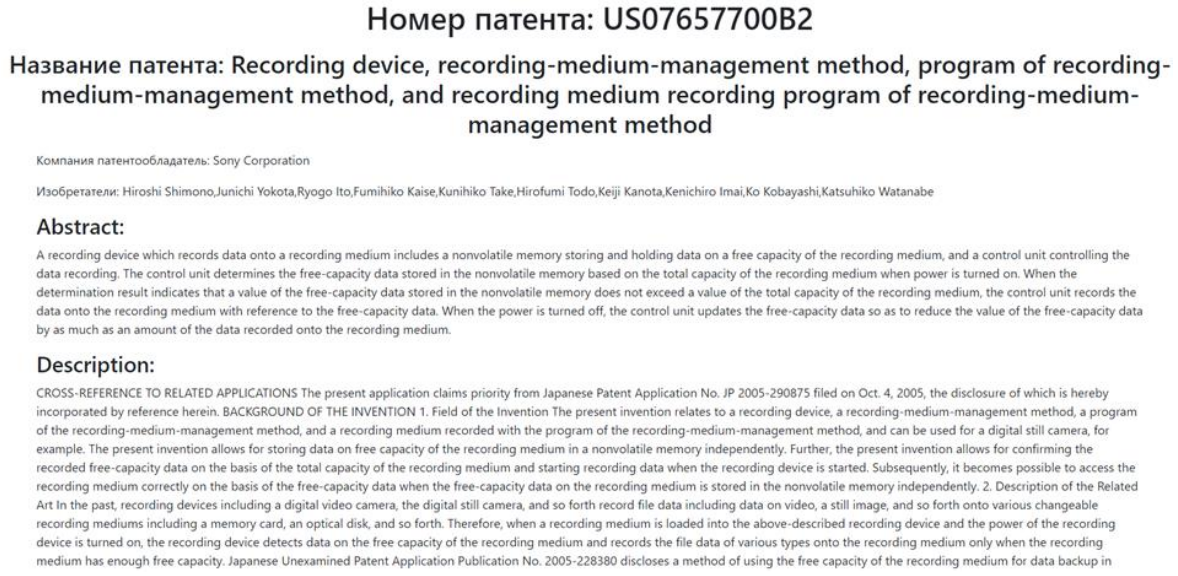
Введите наименование изделия или технологии для поиска партнеров: Поиск

Введенный запрос: reducing capacity

Компания	Изобретатели	Название патента	Номер патента	Проблема
Sony Corporation	Hiroshi Shimono,Junichi Yokota,Ryogo Ito,Fumihiko Kaise,Kunihiko Take,Hirofumi Todo,Keiji Kanota,Kenichiro Imai,Ko Kobayashi,Katsuhiko Watanabe	Recording device, recording-medium-management method, program of recording-medium-management method, and recording medium recording program of recording-medium-management method	US07657700B2	updates the free-capacity data stored in the nonvolatile memory so as to reduce the value of the free-capacity data stored in the nonvolatile memory by as much as the amount of the desired data recorded onto the recording medium
Toyota Jidosha Kabushiki Kaisha	Yasushi Iwazaki	Abnormality diagnostic device and abnormality diagnostic method for air-fuel ratio sensor	US07751966B2	reduced Therefore , the calculation load or the memory capacity involved in the parameter identification are
Petróleo Brasileiro S.A. - Petrobras	Vladimir Mate Paz,Elisabeth de Campos Porto,Cipriano José De Medeiros, Júnior	Deep water high capacity anchoring system and method of operation thereof	US07752989B2	concerns an anchoring system by jetting applied to light anchors , with a high load capacity ,

Рисунок 10 – Результат поискового запроса с найденными технологическими партнерами

На рисунке 11 можно увидеть страницу с описанием патентного документа.



Номер патента: US07657700B2

Название патента: Recording device, recording-medium-management method, program of recording-medium-management method, and recording medium recording program of recording-medium-management method

Компания патентообладатель: Sony Corporation

Изобретатели: Hiroshi Shimono,Junichi Yokota,Ryogo Ito,Fumihiko Kaise,Kunihiko Take,Hirofumi Todo,Keiji Kanota,Kenichiro Imai,Ko Kobayashi,Katsuhiko Watanabe

Abstract:

A recording device which records data onto a recording medium includes a nonvolatile memory storing and holding data on a free capacity of the recording medium, and a control unit controlling the data recording. The control unit determines the free-capacity data stored in the nonvolatile memory based on the total capacity of the recording medium when power is turned on. When the determination result indicates that a value of the free-capacity data stored in the nonvolatile memory does not exceed a value of the total capacity of the recording medium, the control unit records the data onto the recording medium with reference to the free-capacity data. When the power is turned off, the control unit updates the free-capacity data so as to reduce the value of the free-capacity data by as much as an amount of the data recorded onto the recording medium.

Description:

CROSS-REFERENCE TO RELATED APPLICATIONS The present application claims priority from Japanese Patent Application No. JP 2005-290875 filed on Oct. 4, 2005, the disclosure of which is hereby incorporated by reference herein. BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to a recording device, a recording-medium-management method, a program of the recording-medium-management method, and a recording medium recorded with the program of the recording-medium-management method, and can be used for a digital still camera, for example. The present invention allows for storing data on free capacity of the recording medium in a nonvolatile memory independently. Further, the present invention allows for confirming the recorded free-capacity data on the basis of the total capacity of the recording medium and starting recording data when the recording device is started. Subsequently, it becomes possible to access the recording medium correctly on the basis of the free-capacity data when the free-capacity data on the recording medium is stored in the nonvolatile memory independently. 2. Description of the Related Art In the past, recording devices including a digital video camera, the digital still camera, and so forth record file data including data on video, a still image, and so forth onto various changeable recording mediums including a memory card, an optical disk, and so forth. Therefore, when a recording medium is loaded into the above-described recording device and the power of the recording device is turned on, the recording device detects data on the free capacity of the recording medium and records the file data of various types onto the recording medium only when the recording medium has enough free capacity. Japanese Unexamined Patent Application Publication No. 2005-228380 discloses a method of using the free capacity of the recording medium for data backup in

Рисунок 11 – Страница с описанием патентного документа

Заключение. В данной работе описан разработанный метод извлечения из патентных документов USPTO семантических структур Subject-Action-Object и поиска на их основе потенциальных технологических партнеров. Метод включает в себя алгоритмы парсинга патентных массивов, извлечения структур SAO и формирования структур «Проблема – Решение», определения схожести технологических проблем и поиска технологических партнеров. Разработанный метод реализован в виде программного модуля на Python и апробирован на патентных документах USPTO за 2010–2020 гг.

Внедрение программного модуля позволит облегчить и ускорить процесс поиска потенциальных партнеров по НИОКР по сравнению с ручной обработкой данных.

Библиографический список

1. Korobkin, D. The software for computation the criteria-based assessments of the morphological features of technical systems / D. Korobkin, S. Fomenkov, M. Fomenkova, I. Vayngolts, A. Kravets // Cyber-Physical Systems. – Springer, Cham, 2021. – P. 161–172.

2. Korobkin, D. The Formation of Morphological Matrix Based on an Ontology “Patent Representation of Technical Systems” for the Search of Innovative Technical Solutions / D. Korobkin, S. Fomenkov, G. Vereschak, S. Kolesnikov, D. Tolokin, A. Kravets // Cyber-Physical Systems. – Springer, Cham, 2021. – P. 149–160.

3. Souili A. et al. Starting from patents to find inputs to the problem graph model of IDM-TRIZ // Procedia Engineering. – 2015. – Vol. 131. – P. 150–161.

4. Roh, T. Technology opportunity discovery by structuring user needs based on natural language processing and machine learning / T. Roh et al. // PloS one. – 2019. – Vol. 14, № 10. – P. e0223404.

5. De Prato, G. Innovation radar: Identifying innovations and innovators with high potential in ICT FP7, CIP & H2020 projects / G. De Prato et al. // JRC Scientific and Policy Reports – EUR. – 2015. – Vol. 27314. – P. 11–15.

6. Feng, L. Discovering technology opportunity by keyword-based patent analysis: a hybrid approach of morphology analysis and USIT / L. Feng et al. // Sustainability. – 2019. – Vol. 12, № 1. – P. 136.

7. Guo, J. Subject-action-object-based morphology analysis for determining the direction of technological change / J. Guo, X. Wang, Q. Li, D. Zhu // Technological Forecasting and Social Change. – 2016. – Vol. 105. – P. 27–40.

8. Wang X., Qiu, P., Zhu, D., Mitkova, L., Lei, M., Porter, A. Identification of technology development trends based on subject-action-object analysis: The case of dye-sensitized solar cells // Technological forecasting and social change. – 2015. – Vol. 98. – P. 24–46.

9. Yang C., Zhu D., Wang X. SAO semantic information identification for text mining // International Journal of Computational Intelligence Systems. – 2017. – Vol. 10, № 1. – P. 593.

10. Yang C., Huang C., Su J. An improved SAO network-based method for technology trend analysis: A case study of graphene // Journal of Informetrics. – 2018. – Vol. 12, № 1. – P. 271–286.

11. Kim S., Park I., Yoon B. SAO2Vec: Development of an algorithm for embedding the subject-action-object (SAO) structure using Doc2Vec // Plos one. – 2020. – Vol. 15, № 2. – P. e0227930.

12. Bulk Data Storage System (BDSS) Version 1.1.0 // United States Patent and Trademark Office : официальный сайт. – Режим доступа: https://bulkdata.uspto.gov/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.08.2022).

References

1. Korobkin, D., Fomenkov, S., Fomenkova, M., Vayngolts, I., & Kravets, A. G. The software for computation the criteria-based assessments of the morphological features of technical systems. *Cyber-Physical Systems*. Springer, Cham., 2021, pp. 161–172.

2. Korobkin, D., Fomenkov, S., Vereschak, G., Kolesnikov, S., Tolokin, D., & Kravets, A. G. The Formation of Morphological Matrix Based on an Ontology "Patent Representation of Technical Systems" for the Search of Innovative Technical Solutions. *Cyber-Physical Systems*. Springer, Cham., 2021, pp. 149–160.

3. Souili, A., Cavallucci, D., Rousselot, F., & Zanni, C. Starting from patents to find inputs to the problem graph model of IDM-TRIZ. *Procedia Engineering*, 2015, vol. 131, pp. 150–161.

4. Roh, T., Jeong, Y., Jang, H., & Yoon, B. Technology opportunity discovery by structuring user needs based on natural language processing and machine learning. *PloS one*, 2019, vol. 14(10), e0223404.

5. De Prato, G., Nepelski, D., & Piroli, G. Innovation radar: Identifying innovations and innovators with high potential in ICT FP7, CIP & H2020 projects. *JRC Scientific and Policy Reports – EUR*, 2015, vol. 27314, pp. 11–15.

6. Feng, L., Niu, Y., Liu, Z., Wang, J., & Zhang, K. Discovering technology opportunity by keyword-based patent analysis: a hybrid approach of morphology analysis and USIT. *Sustainability*, 2019, vol. 12 (1), p. 136.

7. Guo, J., Wang, X., Li, Q., & Zhu, D. Subject-action-object-based morphology analysis for determining the direction of technological change. *Technological Forecasting and Social Change*, 2016, vol. 105, pp. 27–40.

8. Wang, X., Qiu, P., Zhu, D., Mitkova, L., Lei, M., & Porter, A. L. Identification of technology development trends based on subject-action-object analysis: The case of dye-sensitized solar cells. *Technological forecasting and social change*, 2015, vol. 98, pp. 24–46.

9. Yang, C., Zhu, D., & Wang, X. SAO semantic information identification for text mining. *International Journal of Computational Intelligence Systems*, 2017, vol. 10 (1), p. 593.

10. Yang, C., Huang, C., & Su, J. An improved SAO network-based method for technology trend analysis: A case study of graphene. *Journal of Informetrics*, 2018, vol. 12 (1), pp. 271–286.

11. Kim, S., Park, I., & Yoon, B. SAO2Vec: Development of an algorithm for embedding the subject–action–object (SAO) structure using Doc2Vec. *Plos one*, 2020, vol. 15 (2), p. e0227930.

12. *Bulk Data Storage System (BDSS) Version 1.1.0. United States Patent and Trademark Office*. Available at: https://bulkdata.uspto.gov/ (accessed 19.08.2022).

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

УДК 004.72

ОБЕСПЕЧЕНИЕ ИЗБЫТОЧНОСТИ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Статья поступила в редакцию 17.10.2022, в окончательном варианте – 18.10.2022.

Самохвалов Алексей Владимирович, Тамбовский государственный университет имени Г.Р. Державина, 392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,
кандидат педагогических наук, доцент, ORCID: 0000-0002-3151-3250, e-mail: samohvalov@gmail.com

Соловьев Денис Сергеевич, Тамбовский государственный университет имени Г.Р. Державина, 392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,
кандидат технических наук, доцент, ORCID: 0000-0001-6613-3218, e-mail: solovjevdenis@mail.ru

Соловьева Инна Александровна, Тамбовский государственный университет имени Г.Р. Державина, 392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,
ассистент, ORCID: 0000-0002-1798-1859, e-mail: good.win32@yandex.ru

Скворцов Александр Александрович, Тамбовский государственный университет имени Г.Р. Державина, 392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,
кандидат педагогических наук, доцент, ORCID: 0000-0003-2041-4000, e-mail: skvor_88@mail.ru

В работе рассматривается проблема обеспечения надежности функционирования корпоративной компьютерной сети передачи информации. Представлены технологии резервирования на уровнях ядра, распределения и сетевого доступа. Для обеспечения избыточности построена модель топологии сети, произведена настройка сетевого оборудования и проведены эксперименты по повышению надежности работы сети. На основе анализа результатов экспериментов сформулированы рекомендации по повышению надежности функционирования корпоративной компьютерной сети передачи информации.

Ключевые слова: передача информации, надежность, компьютерная сеть, избыточность, протокол, GLBP, EtherChannel, STP

PROVIDING REDUNDANCY TO IMPROVE THE RELIABILITY OF THE CORPORATE COMPUTER NETWORK FOR INFORMATION TRANSMISSION

The article was received by the editorial board on 17.10.2022, in the final version – 18.10.2022.

Samokhvalov Alexey V., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392000, Russian Federation,
Cand. Sci. (Pedagogics), Associate Professor, ORCID: 0000-0002-3151-3250, e-mail: samohvalov@gmail.com

Solovjev Denis S., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392000, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-6613-3218, e-mail: solovjevdenis@mail.ru

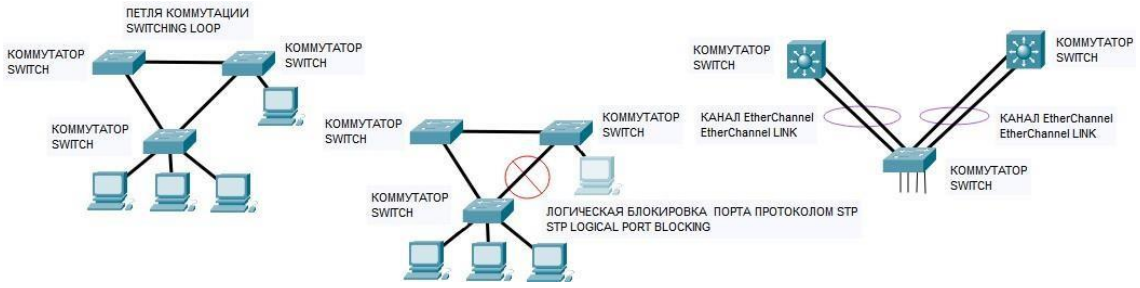
Solovjeva Inna A., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392000, Russian Federation,
Assistant, ORCID: 0000-0002-1798-1859, e-mail: good.win32@yandex.ru

Skvortsov Alexander A., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392000, Russian Federation,
Cand. Sci. (Pedagogics), Associate Professor, ORCID: 0000-0003-2041-4000, e-mail: skvor_88@mail.ru

This paper discusses the problem of ensuring the reliability of a corporate computer network for information transmission. It presents redundancy technologies at the core, distribution and network access levels. To ensure the redundancy of the corporate computer network for information transmission, a model of the logical network topology is built, the necessary settings of network equipment are made and experiments to improve the reliability of the network are conducted. Based on the analysis of experimental results, recommendations to improve the reliability of the corporate computer network are formulated.

Keywords: information transmission, reliability, computer network, redundancy, protocol, GLBP, EtherChannel, STP

Graphical annotation (Графическая аннотация)



Введение. Функционирование современного информационного общества требует от отдельных лиц и предприятий постоянного доступа к базам данных и различным сетевым ресурсам. В свою очередь, от организации информационного пространства и внедрения современных быстро развивающихся технологий сбора, обработки и передачи данных во многом зависит эффективная работа предприятия [1, 2]. В настоящее время являются актуальными и востребованными задачи проектирования и обеспечения отказоустойчивости компьютерных сетей передачи информации на предприятиях с учетом развития сетевых технологий. Так, в работе [3] предложен метод оценки показателей надежности компьютерных сетей специального назначения с применением нейронных сетей. Исследование вероятности связности двух выбранных узлов компьютерной сети или одного из узлов сети со всеми остальными проводится в работе [4]. Работа [5] описывает программный продукт, позволяющий обеспечить требуемый уровень надежности компьютерной сети путем определения максимально допустимого количества компьютеров в ней. В работе [6] представлены упрощенные формулы для оценки доступности компьютерной сети и примеры ее расчетов для типичных иерархических топологий. Работа [7] посвящена исследованию проблемы обеспечения эффективности совместной работы узлов в сети и рассмотрению возможности использования для этой цели вероятностного сетевого протокола канального уровня. От типа топологии компьютерной сети во многом зависит эффективность процесса управления сетевыми потоками и возможность альтернативной маршрутизации с целью обеспечения надежности передачи информации. Модернизация компьютерной сети осуществляется в среднем каждые 3–5 лет, что обусловливается расширением границ предприятия и применением современных информационных и коммуникационных технологий. В связи с этим актуальна задача оптимизации топологии корпоративной компьютерной сети передачи информации по критериям надежности и стоимостных затрат. Построив оптимальную топологию корпоративной компьютерной сети и соответствующим образом настроив сетевое оборудование, можно значительно повысить ее надежность.

Целью работы является повышение надежности функционирования корпоративной компьютерной сети передачи информации при допустимой стоимости ее внедрения.

Материалы и методы. На многих предприятиях удовлетворение потребностей бизнеса в значительной степени зависит от доступности сети. Иерархическая модель компьютерной сети, как правило, содержит три уровня: доступа, распределения и ядра. Каждый уровень выполняет свои функции. Уровень доступа предоставляет конечным устройствам и пользователям прямой доступ к сети. Уровень распределения объединяет устройства уровня доступа и обеспечивает возможность подключения к устройствам уровня ядра. Наконец, уровень ядра обеспечивает связь между уровнями распределения для крупных компьютерных сетей. Пользовательский трафик создается на уровне доступа и проходит через другие уровни, если для передачи необходимы функции этих уровней.

Избыточность – важная часть проектирования сети, поскольку она защищает от перебоев в работе сетевых служб в случае отказа одной точки [8]. Установка дублирующего оборудования и каналов является одним из способов реализации резервирования для введения избыточности сети.

Классическим примером реализации резервирования в корпоративной компьютерной сети передачи информации может являться топология, показанная на рисунке 1.

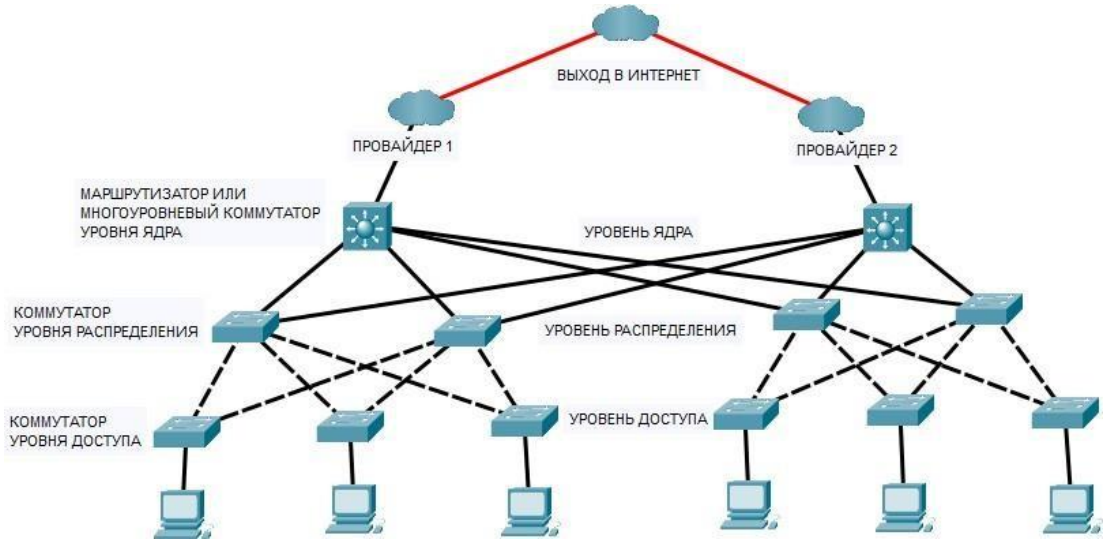


Рисунок 1 – Пример реализации резервирования в корпоративной компьютерной сети

В данной топологии обеспечивается наличие резервных каналов между сетевыми устройствами уровня распределения и уровня доступа, а также резервирование на уровне ядра с распределением нагрузки с использованием каналов доступа в интернет нескольких провайдеров. Вместе с тем избыточное резервирование требует дополнительных финансовых затрат и не всегда является эффективным с экономической точки зрения, ведь стоимость одной единицы активного сетевого оборудования может достигать десятков или даже сотен тысяч рублей.

Для разрешения данной проблемы сформулируем задачу оптимизации. Предположим, что компьютерная сеть:

$$G = (N, L, P), \tag{1}$$

где N, L, P – набор сетевых узлов и каналов в сети, а также их надежность.

При моделировании компьютерной сети примем следующие допущения [9]:

1) учитывается случайный отказ сетевого узла или канала;

2) состояние любых узлов не зависит от архитектуры компьютерной сети;

3) отсутствует прямая зависимость между длиной канала и надежностью компьютерной сети;

4) отсутствует прямая зависимость между проблемами сетевого оборудования и передачей данных по сети, т.е. есть только два состояния сети и сетевого канала: нормальная работа и неисправность;

5) минимальный разрез графа (1), который необходимо вычислить, является связным, т.е. цикл не образуется.

Когда вся сеть G доступна, то компьютеры в ней могут быть соединены друг с другом, т.е. каждый узел в нормальном состоянии может образовать остовное дерево графа G, чтобы обеспечить нормальную работу сети. При этом канал сети $L' \subseteq L$ находится в нормальном состоянии передачи информации в любой момент нормальной работы сети G.

Пусть имеется матрица стоимостей соединения узлов компьютерной сети:

$$C_0 = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix}, \tag{2}$$

где c_{ij} – стоимость соединения между i-м и j-м узлами компьютерной сети, причем c_{ij} равен 0 для $i = j$.

Тогда расчет стоимости сетевого соединения имеет вид:

$$C = \sum_{i=1}^{N} \sum_{j=1}^{i} c_{ij} g_{ij} , \tag{3}$$

Значение g_{ij} в (3) равно 1, если существует прямая связь между узлами i и j, а значение g_{ij} равно 0, когда прямой связи между узлами i и j нет.

Сформулируем задачу оптимизации надежности компьютерной сети. Отыскать такую структуру графа G^*, которая обеспечивает максимальную надежность компьютерной сети:

$$P\left(G^*\right) \to \max , \tag{4}$$

при ограничениях на ее стоимость:

$$C \le C_{\max}, \quad (5)$$

где $C_{\max}$ – максимально допустимая стоимость сети.

Таким образом, требуется получить структуру компьютерной сети, которая обеспечивает максимальную надежность передачи информации при допустимой стоимости ее внедрения.

Экспериментальная часть. Рассмотрим схему компьютерной сети предприятия $G = (N, L, P)$, показанную на рисунке 2. Моделирование сети осуществляется в системе *Cisco Packet Tracer* [10].

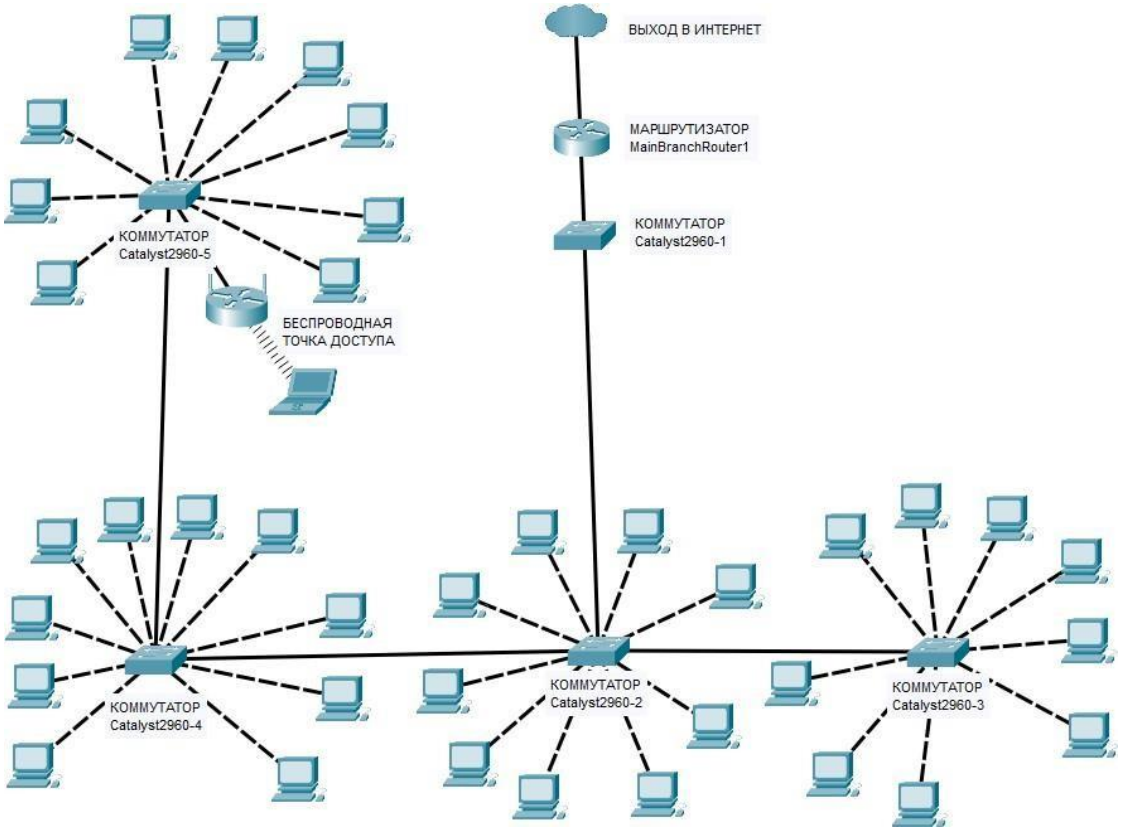


Рисунок 2 – Схема корпоративной компьютерной сети предприятия

Схема содержит 4 коммутатора Cisco Catalyst 2960, 1 маршрутизатор Cisco 2911, 1 беспроводную точку доступа LinkSys WRT300N, 37 компьютеров, подключенных по технологии FastEthernet и несколько мобильных устройств, подключенных по технологии Wi-Fi. Доступ в интернет реализуется через сеть провайдера Ростелеком, скорость – 1000 Мбит/с.

Согласно спецификациям устройств, среднее время наработки на отказ (*MTBF*) коммутаторов *Cisco Catalyst* 2960 составляет 233 370 ч, маршрутизаторов *Cisco* 2911 – 300 000 ч. При расчетах принято экспоненциальное распределение вероятности безотказной работы, для расчета которой воспользуемся формулами последовательного и параллельного соединения элементов [11].

Расчет надежности последовательного соединения элементов осуществляется согласно:

$$P_n(t) = \prod_{i=1}^{n} P_i(t) = e^{-\lambda_n t}, \quad (6)$$

$$\lambda_n = \sum_{i=1}^{n} \lambda_i, \quad (7)$$

где n – количество последовательно соединенных элементов; λ_n – интенсивность отказов системы.

Для параллельного соединения формула расчета надежности имеет вид:

$$P_n(t) = 1 - \prod_{i=1}^{n} [1 - P_i(t)], \quad (8)$$

где t – наблюдаемый момент времени.

Для компьютерной сети на рисунке 2 вероятность безотказной работы P в течение года эксплуатации (t = 8760 ч) составляет 0,83581. Руководством предприятия выделен бюджет в размере $C_{\max}$ = 90 000 руб для повышения надежности функционирования сети. Данной суммы недостаточно

для покупки нужного количества оборудования с лучшим значением *MTBF*, поэтому проблема повышения надежности функционирования сети будет решаться путем обеспечения избыточности за счет добавления резервных каналов передачи данных и соответствующей настройки оборудования.

Результаты и их обсуждение. Для топологии, показанной на рисунке 2, была найдена оптимальная структура графа G^*, которая обеспечивает максимальную надежность компьютерной сети с учетом ограничений стоимости $C_{\max}$ (рис. 3).

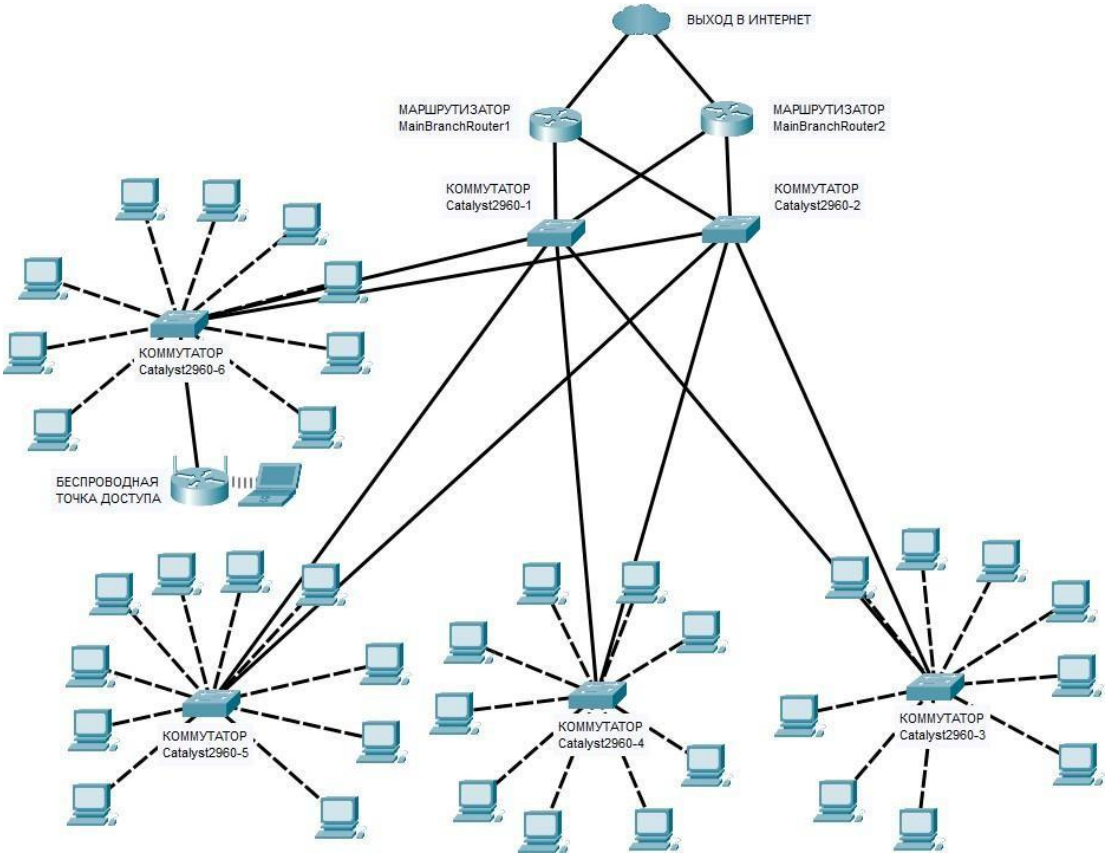


Рисунок 3 – Топология, обеспечивающая необходимую надежность функционирования сети с учетом ограничения $C_{\max}$

Для обеспечения резервирования с целью повышения надежности функционирования компьютерной сети добавлены коммутатор *Cisco Catalyst* 2960 и маршрутизатор *Cisco* 2911, проложены дополнительные линии связи, организован резервный канал доступа в интернет, выполнена соответствующая настройка устройств. На устройствах уровня ядра произведена настройка маршрутизации с распределением нагрузки через резервный канал доступа, что позволит не только повысить надежность функционирования компьютерной сети, но и существенно увеличить скорость доступа в интернет.

Между сетевыми устройствами уровня доступа и уровня распределения проложены дополнительные каналы связи, обеспечивающие наличие резервных каналов связи. Защитить сеть от единой точки отказа возможно с применением избыточности, повышающей доступность топологии сети. При этом могут возникать петли коммутации, показанные на рисунке 4, что приведет к возникновению неполадок при передаче данных в сети.

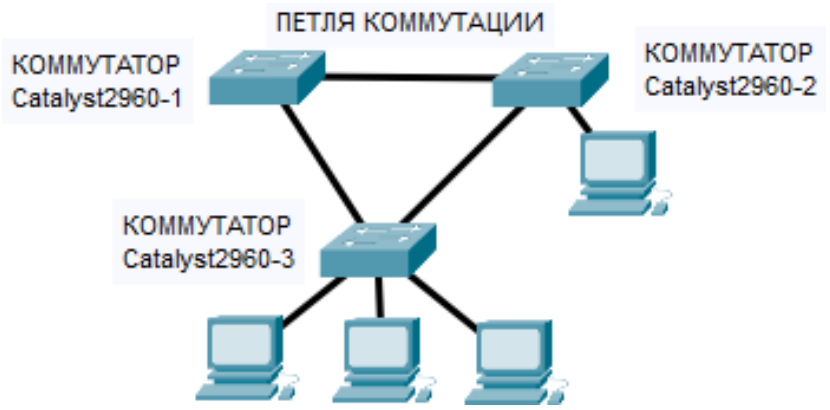


Рисунок 4 – Сегмент сети с резервным каналом и петлей коммутации

Для устранения петель коммутации на всех коммутаторах корпоративной компьютерной сети активирован протокол *STP* [12]. Он блокирует каналы, которые могут вызвать петлю, обеспечивая наличие только одного логического пути между всеми пунктами назначения в сети (рис. 5). Если канал доступа потребуется для компенсации неисправности, протокол *STP* повторно рассчитает пути и снимет блокировку с требуемых портов.

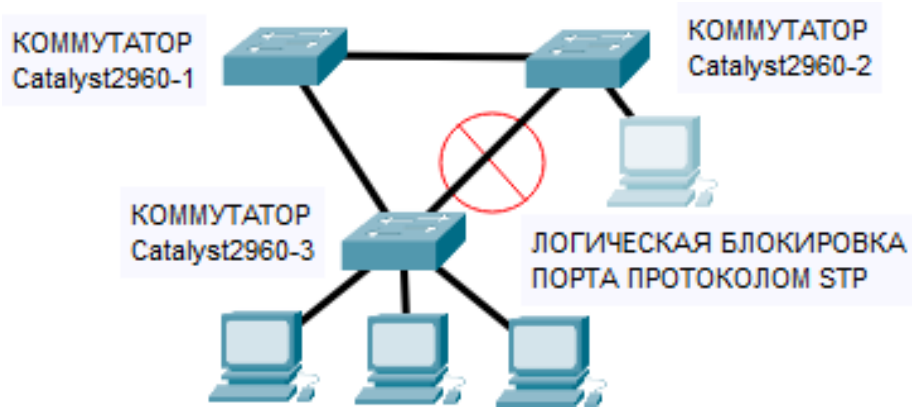


Рисунок 5 – Сегмент сети с резервным каналом без петли коммутации

Ниже показан пример работы протокола *STP* на коммутаторе *Cisco Catalyst* 2960 в сегменте спроектированной сети:

Catalyst2960-1# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 0002.E425.A0BA
Cost 19
Port 2(FastEthernet0/2)
Bridge ID Priority 12284 (priority 12283 sys-id-ext 1)
Address 000B.F382.480C

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- ---------- -------- --------------------------------
Fa0/2 Root FWD 19 128.2 P2p
Fa0/1 Altn **BLK** 19 128.1 P2p

Как показано выше, имеются альтернативные физические каналы *(Fa* 0/1), которые могут быть использованы для резервирования маршрутов в сети в случае возникновения неполадок. На время корректной работы каналов сети передачи информации порт переводится в состояние *BLK* и логически разрывает петлю.

Вторым примером резервирования на уровне распределения является технология *EtherChannel*, которая позволяет не только использовать резервные каналы для повышения надежности функционирования сети, но и существенно повысить скорость передачи данных между двумя устройствами [13]. Пример реализации технологии *EtherChannel* продемонстрирован на рисунке 6. Технология *EtherChannel* обеспечивает балансировку нагрузки между физическими каналами вместо блокировки одного или нескольких из них посредством создания единого логического канала между двумя устройствами с использованием нескольких физических каналов.

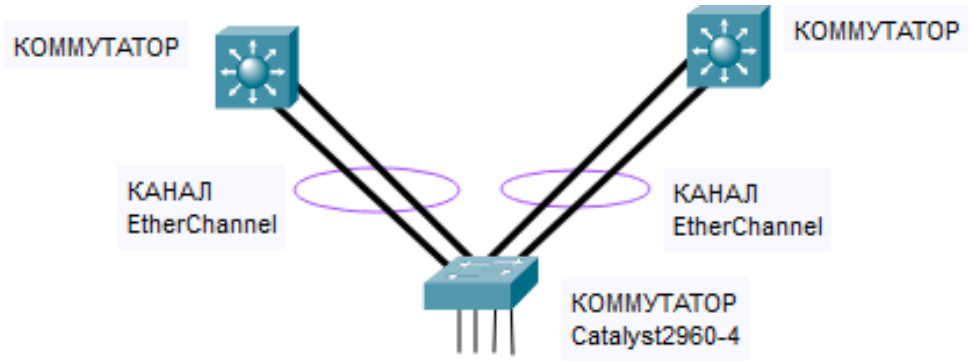


Рисунок 6 – Пример реализации технологии *EtherChannel*

В спроектированной сети между коммутаторами *Cisco Catalyst* 2960 создан канал *EtherChannel* пропускной способностью 2000 МБитс/с:

Catalyst2960-4(config)# **interface range g 0/1-2**
Catalyst2960-4(config-if-range)# **channel-group 5 mode active**
Catalyst2960-4(config-if-range)# **interface port-channel 5**
Catalyst2960-4(config-if)# **switchport mode trunk**

Таким образом, созданный канал увеличенной пропускной способности более устойчив к внешним воздействиям по сравнению со стандартным за счет резервирования линий связи:

Catalyst2960-4# **show interfaces port-channel 5**
Port-channel1 is up, line protocol is up (connected)
MTU 1500 bytes, BW 2000000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Full-duplex, 2000Mb/s
Members in this channel: **G 0/1** , **G 0/2** ,

Несмотря на существование альтернативных физических путей, настроенный на использование шлюза хост будет изолирован от внешних сетей при выходе из строя маршрутизатора по умолчанию. Это объясняется настройкой конечных устройств с одним *IP*-адресом для шлюза, который остается постоянным при изменении топологии компьютерной сети. В связи с этим устройство по умолчанию будет отключено от сети при недоступности *IP*-адреса шлюза. Введение виртуального маршрутизатора является одним из подходов к устранению единой точки отказа на шлюзе. Виртуальный маршрутизатор обеспечивает функционирование совокупности маршрутизаторов как единое целое, использующее общие *MAC*- и *IP*-адреса.

С адресом *IPv*4 виртуального маршрутизатора, настроенным в качестве шлюза по умолчанию для пользовательских компьютеров, была создана группа маршрутизаторов *GLBP*. Конечные устройства отправляют трафик на адреса виртуального маршрутизатора. Физический маршрутизатор, который пересылает данный трафик, является «прозрачным» для конечных устройств, и, в случае отказа одного из физических маршрутизаторов, его функции в автоматическом режиме берет на себя другой маршрутизатор из *GLBP*-группы.

Для обеспечения резервирования основного шлюза настроена *GLBP*-группа маршрутизаторов:

MainBranchRouter1(config)# interface g0/1
MainBranchRouter1(config-if)# glbp 1 ip 192.168.1.252
MainBranchRouter1(config-if)# glbp 1 load-balancing round-robin
MainBranchRouter1(config-if)# glbp 1 priority 120
MainBranchRouter1(config-if)# glbp 1 preempt

```
MainBranchRouter2(config)# interface g0/1
MainBranchRouter2(config-if)# glbp 1 ip 192.168.1.252
MainBranchRouter2(config-if)# glbp 1 load-balancing round-robin
```

Результат настройки:

```
MainBranchRouter1# show glbp 1
GigabitEthernet0/1 - Group 1 (version 2)
State is Active
4 state changes, last state change 0:00:30
Virtual IP address is 192.168.1.252
```

Таким образом, для повышения надежности функционирования рассматриваемой компьютерной сети установлены коммутатор *Cisco Catalyst* 2960 и маршрутизатор *Cisco* 2911, проложены дополнительные линии связи в локальном сегменте сети, организован резервный канал доступа в интернет, выполнена соответствующая настройка устройств. На устройствах уровня ядра произведена настройка маршрутизации с распределением нагрузки через резервный канал доступа, что позволило не только повысить надежность, но и существенно увеличить скорость доступа в интернет. Создана *GLBP*-группа маршрутизаторов для обеспечения резервирования основного шлюза с распределением нагрузки. На устройствах уровня распределения и уровня доступа активирован протокол *STP*, предотвращающий возникновение петель коммутации.

Согласно расчетам по формулам (6)–(8), для сети G^* вероятность безотказной работы P в течение года эксплуатации составит 0,96105.

Отметим, что дальнейшее повышение надежности функционирования сети также возможно, но потребует покупки оборудования с существенно лучшим значением *MTBF*, что потребует увеличения финансовых затрат на модернизацию сети как минимум на 1 порядок. Увеличение максимально допустимой стоимости C_{max} является целесообразным только в том случае, если ее величина гораздо меньше стоимости простоя предприятия, вызванного неработоспособностью корпоративной компьютерной сети.

Заключение. Компьютерные сети представляют собой сложные системы, содержащие множество элементов, в связи с чем отказы сети неизбежны. Анализ надежности дает проверку «пригодности» предполагаемым проектным ожиданиям инфраструктуры или соответствующих компонентов корпоративной компьютерной сети. В работе построена топология корпоративной компьютерной сети передачи информации, которая обеспечивает максимальную надежность функционирования при допустимой стоимости ее внедрения. Для повышения надежности функционирования корпоративной компьютерной сети реализована избыточность каналов передачи информации как на уровне распределения, так и на уровне ядра. Произведены необходимые настройки сетевого оборудования. Создана *GLBP*-группа маршрутизаторов для обеспечения резервирования основного шлюза с использованием алгоритма распределения нагрузки *Round-robin*. На уровне распределения для обеспечения избыточности и предотвращения возникновения петель активирован протокол *STP*. Указанные выше меры позволили повысить надежность функционирования корпоративной компьютерной сети на 12,6 % в рамках ограниченного бюджета в 90 000 руб. Дальнейшее повышение надежности функционирования возможно, но в текущей конфигурации потребует покупки сетевого оборудования, обладающего улучшенным значением *MTBF*, что повлечет финансовые затраты, значительно превышающие стоимость резервирования.

Предложенные в работе методы оптимизации топологии сети, технологии могут быть использованы для проектирования надежных, отказоустойчивых сегментов корпоративных компьютерных сетей передачи информации для предприятий.

Библиографический список

1. Кузьменко, Н. Г. Компьютерные сети и сетевые технологии / Н. Г. Кузьменко. – Санкт-Петербург : Наука и техника, 2013. – 368 с.

2. Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл. – Санкт-Петербург : Питер, 2018. – 512 с.

3. Иванов, Д. В. Оперативная оценка показателей надежности компьютерной сети для специального применения / Д. В. Иванов // Естественные и технические науки. – 2009. – № 5 (43). – С. 306–307.

4. Андреев, А. М. Моделирование надёжности компьютерной сети / А. М. Андреев, Г. П. Можаров // Инженерный журнал: наука и инновации. – 2013. – № 1 (23). – С. 62.

5. Володин, В. А. Программная реализация системы поддержки принятия решений варианта профилактического обслуживания компьютерной сети / В. А. Володин, С. Ю. Лысенко // Решетневские чтения. – 2013. – Т. 2. – С. 194–196.

6. Каяшев, А. И. Анализ показателей надежности локальных компьютерных сетей / А. И. Каяшев, П. А. Рахман, М. И. Шарипов // Вестник Уфимского государственного авиационного технического университета. – 2013. – Т. 17, № 5 (58). – С. 140–149.

7. Азизов, Р. Ф. Определение оптимальных характеристик алгоритма конкурентного доступа к среде для минимизации времени передачи данных в децентрализованных беспроводных сетях / Р. Ф. Азизов, Д. А. Аминев, С. У. Увайсов, Н. К. Юрков // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 1 (29). – С. 139–145.

8. Шувалов, В. П. Обеспечение показателей надежности телекоммуникационных систем и сетей / В. П. Шувалов, М. М. Егунов, Е. А. Минина. – Москва : Горячая линия-Телеком, 2015. – 168 с.

9. Anuradha Calculation and Evaluation of Network Reliability using ANN Approach / Anuradha, A. K. Solanki, H. Kumar, K. K. Singh // Procedia Computer Science. – 2020. – Vol. 167. – P. 2153–2163.

10. Якимов, И. М. Имитационное моделирование компьютерной сети в системе Cisco Packet Tracer / И. М. Якимов, А. П. Кирпичников, К. Д. Валова, В. Н. Анишкина // Вестник Технологического университета. – 2019. – Т. 22, № 8. – С. 145–149.

11. Шишмарев, В. Ю. Надежность технических систем / В. Ю. Шишмарев. – Москва : Academia, 2010. – 304 с.

12. Макаренко, С. И. Модель функционирования коммутатора в сети с использованием протокола покрывающего дерева STP и исследование устойчивости сети в условиях ограниченной надёжности каналов связи / С. И. Макаренко, Р. Л. Михайлов // Радиотехнические и телекоммуникационные системы. – 2013. – № 2 (10). – С. 61–68.

13. Бобров, А. В. Использование EtherChannel: что это такое и в чем его преимущества / А. В. Бобров, Д. А. Семёнов // Вопросы науки и образования. – 2018. – № 8 (20). – С. 39–42.

References

1. Kuzmenko, N. G. *Kompyuternye seti i setevye tekhnologii* [Computer networks and network technologies]. St. Petersburg, Nauka i tekhnika Publ., 2013. 368 p.

2. Tanenbaum, A. S., Wetherall, D. J. *Kompyuternye seti* [Computer networks]. St. Petersburg, Piter Publ., 2018. 512 p.

3. Ivanov, D. V. Operativnaya otsenka pokazateley nadezhnosti kompyuternoy seti dlya spetsialnogo primeneniya [Rapid assessment of computer network reliability indicators for special applications]. *Estestvennye i tekhnicheskie nauki* [Natural and Technical Sciences], 2009, vol. 5, no. 43, pp. 306–307.

4. Andreev, A. M., Mozharov, G. P. Modelirovanie nadyozhnosti komp'yuternoj seti [Modelling of computer network reliability]. *Inzhenernyj zhurnal: nauka i innovatsii* [Engineering Journal: Science and Innovation], 2013, vol. 1, no. 23, p`. 62.

5. Volodin, V. A., Lysenko, S. Yu. Programmnaya realizatsiya sistemy podderzhki prinyatiya resheniy varianta profilakticheskogo obsluzhivaniya kompyuternoy seti [Program realization of decision-making support system of option of the computer network preventive maintenance]. *Reshetnevskie chteniya* [Reshetnev Readings], 2013, vol. 2, pp. 194–196.

6. Kayashev, A. I., Rakhman, P. A., Sharipov, M. I. Analiz pokazateley nadezhnosti lokalnykh kompyuternykh setey [Reliability analysys of local area networks]. *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta* [Vestnik of Ufa State Aviation Technical University], 2013, vol. 17, no. 5 (58), pp. 140–149.

7. Azizov, R. F., Aminov, D. A., Uvaysov, S. U., Yurkov, N. K. Opredelenie optimalnykh kharakteristik algoritma konkurentnogo dostupa k srede dlya minimizatsii vremeni peredachi dannykh v detsentralizovannkyh besprovodnykh setyakh [Determination of the optimal characteristics of the CSMA/CA algorithm for minimize transmission time in decentralized wireless networks]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2015, no. 1 (29), pp. 139–145.

8. Shuvalov, V. P., Egunov M. M., Minina, E. A. *Obespechenie pokazateley nadezhnosti telekommunikatsionnykh sistem i setey* [Providing indicators of reliability of telecommunication systems and networks]. Moscow, Goryachaya liniya-Telekom Publ., 2015. 168 p.

9. Anuradha, Solanki, A. K., Kumar, H., Singh, K. K. Calculation and Evaluation of Network Reliability using ANN Approach. *Procedia Computer Science*, 2020, vol. 167, pp. 2153–2163.

10. Yakimov, I. M., Kirpichnikov, A. P., Valova, K. D., Anishkina, V. N. Imitatsionnoe modelirovanie kompyuternoy seti v sisteme Cisco Packet Tracer [Simulation modeling of a computer network in Cisco Packet Tracer]. *Vestnik Tekhnologicheskogo universiteta* [Bulletin of the Technological University], 2019, vol. 22, no. 8, pp. 145–149.

11. Shishmarev, V. Yu. *Nadezhnost tekhnicheskikh sistem* [Reliability of technical systems]. Moscow, Academia Publ., 2010. 304 p.

12. Makarenko, S. I., Mikhaylov, R. L. Model funktsionirovaniya kommutatora v seti s ispolzovaniem protokola pokryvayushchego dereva STP i issledovanie ustojchivosti seti v usloviyakh ogranichennoy nadyozhnosti kanalov svyazi [The Model of the Switch Functioning in the Network Which Applies the Spanning Tree Protocol and the Net Stability Analysis in the Conditions of the Communication Channels Limited Reliability]. *Radiotekhnicheskie i telekommunikatsionnye sistemy* [Radio and Telecommunication Systems], 2013, no. 2 (10), pp. 61–68.

13. Bobrov, A. V., Semyonov, D. A. Ispolzovanie EtherChannel: chto eto takoe i v chem ego preimushchestva [Using EtherChannel: what is it and what are its advantages]. *Voprosy nauki i obrazovaniya* [Questions of Science and Education], 2018, no. 8 (20), pp. 39–42.

УДК 004.001

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОНИТОРИНГА И РЕДАКТИРОВАНИЯ ИНФОРМАЦИИ О СТУДЕНТАХ

Статья поступила в редакцию 05.06.2022, в окончательном варианте – 21.10.2022.

Шельпук Михаил Игоревич, Российский технологический университет МИРЭА, 119454, Российская Федерация, г. Москва, проспект Вернадского, 78,
студент, ORCID: 0000-0001-5450-4376, e-mail: maestrochess18@mail.ru
Микаева Светлана Анатольевна, Российский технологический университет МИРЭА, 119454, Российская Федерация, г. Москва, проспект Вернадского, 78,
доктор технических наук, доцент, ORCID: 0000-0001-6992-455X, e-mail: mikaeva_s@mirea.ru
Журавлева Юлия Алексеевна, Российский технологический университет МИРЭА, 119454, Российская Федерация, г. Москва, проспект Вернадского, 78,
кандидат технических наук, доцент, ORCID: 0000-0003-3919-5127, e-mail: ulypil@mail.ru
Шигапова Вера Александровна, Российский технологический университет МИРЭА, 119454, Российская Федерация, г. Москва, проспект Вернадского, 78,
преподаватель, ORCID: 0000-0001-9967-4520, e-mail: twinkle17@bk.ru
Коваленко Ольга Юрьевна, Мордовский государственный университет им. Н. П. Огарёва, 430005, Российская Федерация, г. Саранск, ул. Большевистская, 68/1,
доктор технических наук, доцент, ORCID: 0000-0003-3919-5127, e-mail: crystall2000@mail.ru

В ходе работы была создана программа, которая позволяет реализовать следующие способы работы с данными: хранение информации об обучающихся, редактирование данных в случае их изменения или неправильного ввода, сортировка списков на основании параметров, защита данных современными криптографическими моделями. Программа работает исправно даже при вводе неправильных данных, что обеспечивает её устойчивость. В данной программе предусмотрена защита личных данных, которые содержатся в базе, а ключ доступа для дешифровки данных формируется случайным образом и доступен только лицам с соответствующим уровнем допуска. Основой разработки является работа с массивами данных как с использованием динамической, так и статической памяти. Продукт ориентирован на различные сферы деятельности, подразумевающие в своём использовании взаимодействие с большим количеством данных как в упорядоченном, так и в запрашиваемом формате. Также предусмотрена сортировка данных о пользователях в алфавитном порядке с учётом пола.

Ключевые слова: списки, программное обеспечение, оперативная память, шифрование

SOFTWARE DEVELOPMENT FOR MONITORING AND EDITING INFORMATION ABOUT STUDENTS

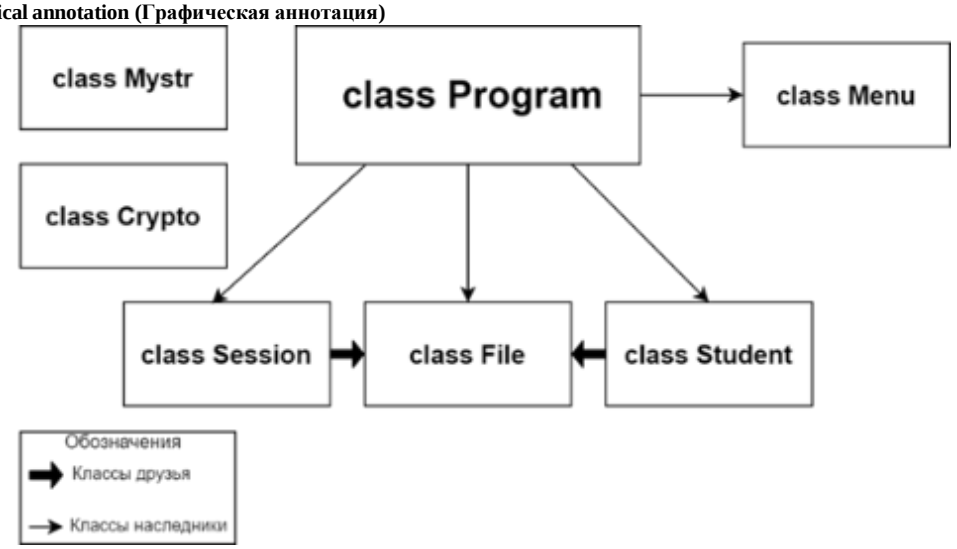
The article was received by the editorial board on 05.06.2022, in the final version – 21.10.2022.

Shelpuck Mikhail I., Russian Technological University MIREA, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
student, ORCID: 0000-0001-5450-4376, e-mail: maestrochess18@mail.ru
Mikaeva Svetlana A., Russian Technological University MIREA, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
Doct. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-6992-455X, e-mail: mikaeva_s@mirea.ru
Zhuravleva Yulia A., Russian Technological University MIREA, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-3919-5127, e-mail: ulypil@mail.ru
Shigapova Vera A., Russian Technological University MIREA, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
teacher, ORCID: 0000-0001-9967-4520, e-mail: twinkle17@bk.ru
Kovalenko Olga Yu., Ogarev Mordovia State University, 68/1 Bolshevistskaya St., Saransk, 430005, Russian Federation,
Doct. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-3919-5127, e-mail: crystall2000@mail.ru

In the course of the work, a program was created that allows you to implement the following ways of working with data: storing information about students, editing data in case of changes or incorrect input, sorting lists based on parameters, data protection with modern cryptographic models. The program works properly even when entering incorrect data, which ensures its stability. This program provides for the protection of personal data contained in the database, and the access key for decrypting data is generated randomly and is available only to persons with the appropriate level of access. The basis of the development is working with data arrays using both dynamic and static memory. The product is focused on various fields of activity, implying in its use interaction with a large amount of data both in an ordered and in the requested format. It also provides sorting of user data in alphabetical order, taking into account gender.

Keywords: lists, software, RAM, encryption

Graphical annotation (Графическая аннотация)



Введение. Проблемой оценивания результатов обучения в настоящее время широко занимаются как отечественные, так и зарубежные ученые. Работы многих исследователей показывают, что если при проектировании основной образовательной программы влияние субъективности не является очевидным, то при оценивании ее освоения фактор субъективизма становится критическим, так как результат оценивания непосредственно наблюдаем и используется, зачастую в неизменном виде, в задачах управления развитием образовательных и трудовых ресурсов [1]. Разработки программ для электронной информационно-образовательной среды (ЭИОС) ведутся во многих вузах. Так в Мордовском госуниверситете разработана программа для ЭИОС, которая позволяет составлять портфолио участников образовательного процесса (в том числе публикации, электронные образовательные ресурсы, участие в грантах и т.д.) с возможностью верификации, заполнять рейтинг план дисциплин, фиксировать и производить мониторинг хода образовательного процесса, обеспечивать общение между участниками образовательного процесса, сохранять отчетности обучающихся с отзывами и обеспечивать доступ к внешним ресурсам [2]. В настоящее время существуют программные обеспечения для анкетирования, тестирования, мониторинга и управления работой студентов [3–6]. Однако данные программы, как правило, имеют узкую область использования и не всегда используют важные преимущества составляющих компонентов. В базе данных, как и в любой другой целостной системе должны быть согласованы все её компоненты, а именно: данные в файле меняться по ходу их замены в программе, участки памяти являться когерентными, а функции работать исправно с расчётом на влияние человеческого фактора (не только вмешательства извне, но и опечатки). Современные базы данных должны иметь возможность изменения во времени. Для этого используется динамическая оперативная память. Предлагаемая программа использует как динамическую оперативную память, элементной базой которых являются конденсаторы, так и статическую, роль основных элементов которой играют триггеры. Такое совмещение типов памяти позволяет повысить общую производительность системы, поскольку набор триггеров в микросхеме значительно превосходит по скорости передачи импульсов аналогичный набор конденсаторов, что определяет как практическую ценность, так и актуальность работы.

Однако, как было сказано ранее, полностью отказаться от динамической памяти невозможно, так как без неё редактирование информации, к примеру, аксиоматически невозможно. Ранее было принято разрабатывать базы данных на различных языках программирования в связке, так как имелась необходимость максимально автоматизировать процессы формирования запросов и возврата необходимых данных. Однако они имеют много недостатков. Задачей была не эффективность и защищённость такого приложения, а максимальная простота в использовании и распространённость. Представленный программный продукт является уникальным в своей области, поскольку ранее никто ещё не разрабатывал базу данных в виде единого полноценно функционирующего приложения, не использующего связок с другими приложениями. Использование новых паттернов позволяет считать его не менее качественным и широким по функционалу, чем разработки прошлых лет. Стоит отметить, что работа по проектированию систем имеет большую историю, связанную с появлением разных языков программирования.

Описание составляющих программы. Предлагаемая программа представляет собой реализацию абстрактной базы данных, оснащённой основными принципами использования оперативной памяти (рис. 1). Не менее важным является само понятие динамической памяти, которая реализуется в программе, например, в виде создания определённых полей и свойств классов с выделением им определённого количества ячеек (байт). Основополагающим в концепции динамической памяти является её определение как полупроводниковой памяти. Современные персональные компьютеры включают в себя практически всю элементную базу. Обращаясь к ней можно выделить детальные особенности принципа построения памяти. Память подключена к шине, обеспечивающей питание (так как динамическая память является энергозависимой) и другие функции. В плату поступают потоки команд и данных, для которых непосредственно определяется понятие адресации (по строкам и столбцам). Первыми важными элементами являются входной и выходной регистры данных. Далее на микросхеме можно увидеть дешифраторы как базовые элементы, формирующие пространственную систему горизонтальных и вертикальных линий, в состав которых входят запоминающие элементы.

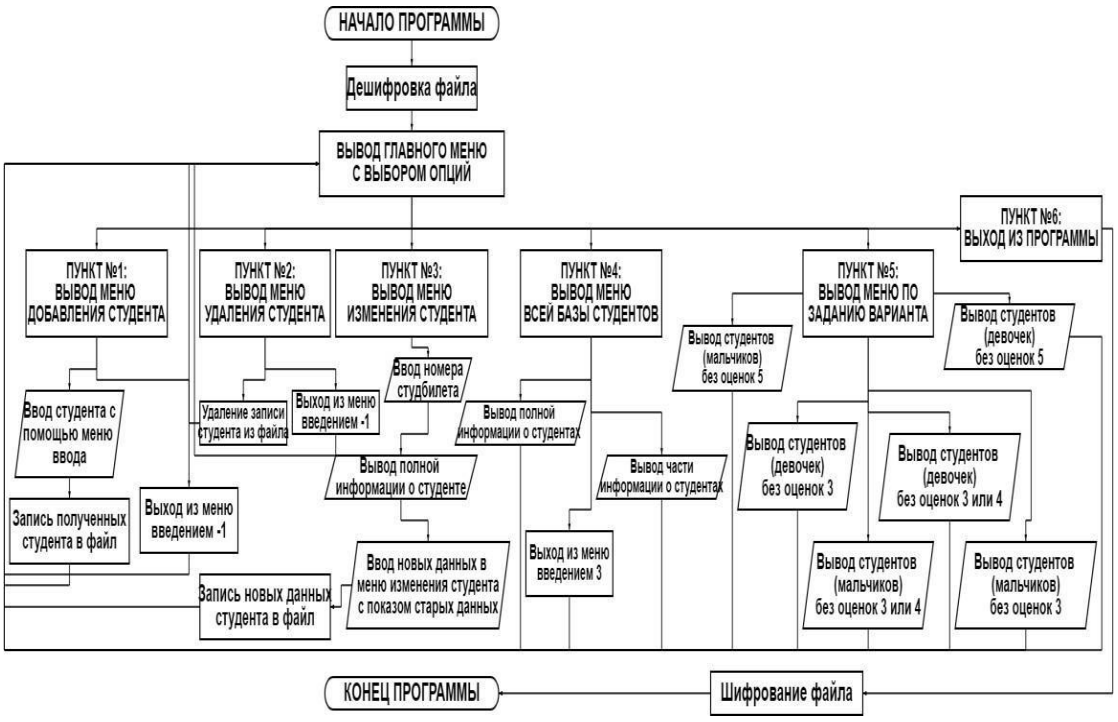


Рисунок 1 – Блок-схема работы приложения

Вертикальные и горизонтальные линии пересекаются, а их пересечением является запоминающий элемент, к которому также подходит вертикальный провод, вместе с запоминающим элементом он называется строкой. Также в микросхеме присутствует вертикальный провод, который в совокупности со всеми запоминающими элементами, подходящими к нему, называется столбцом. Для строк и столбцов сформированы регистры адреса. Данные адреса передаются в соответствующие дешифраторы адресов строк и столбцов. Устройства синхронизации и управления в совокупности с усилителями считывания и записи образуют дополнительную физическую систему. Усилители в совокупности с массивом запоминающих элементов и входными/выходными регистрами данных образуют полноценную связанную структуру. Однако большая интегральная схема запоминающего устройства также включает в себя дешифратор команд, счетчик регенерации, буфер адреса, матрицу элементов памяти, а также банки памяти, сюда же можно отнести схемы коммутации данных и схему управления. Чтение и запись (каждая по отдельности) занимают как минимум пять тактов процессора, что обусловлено установкой адреса столбца, формированием сигнала RAS, а также возвратом этих сигналов в неактивное состояние. Корреляция между записью данных в память и её управлением на уровне компилируемого языка C++ находится именно на уровне записи в файл (взаимодействие с криптографическими системами защиты находится на аналогичном уровне). Строгость в оформлении работы с памятью в вышеприведённом языке программирования позволяет прослеживать каждый шаг в выполнении поставленных задач (чтения, записи, изменения или удаления информации в файле). Существует такое понятие, как указатель, который является ссылкой на то место в памяти, на котором находится необходимая нам информация. Суть функций

чтения и записи заключается в последовательном извлечении из файла информации по указателям, при этом присутствует определённая семантика, от которой зависит всё прохождение по данным (например, математическая формула перехода от одних данных к другим будет зависеть от того, сколько байт памяти мы выделили под определённый вид данных). В программе приведён бинарный способ чтения и записи информации. Сделано это для того, чтобы не возникало проблем со служебными символами, такими как табуляция, перенос строки и нуль-символ, которые могут быть прочитаны как обычный текст и тем самым вызвать ошибку в работе программы. Возвращаясь к динамической памяти стоит уточнить, что программа выполняется последовательно, что означает опять же динамическое изменение записанных данных, что приводит нас к проблеме когерентности, которая усиленно решается всё более эффективными методами и сегодня. Само понятие когерентности означает, что участки памяти (не обязательно динамической) должны быть связаны не только с микропроцессором, но и сами с собой. Это необходимо для того, чтобы динамически изменяющиеся данные принимали новое значение и в других участках, а точнее, у этих участков должна быть информация о соответствующих изменениях. В противном случае возникнет так называемый «конфликт по данным», который, помимо всего прочего, может быть не обнаружен процессором и управляющими программами сразу [7–9].

Классы, методы и код, используемые в программе. При выполнении задачи были созданы некоторые экземпляры классов, затем к программе был подключён файл, в котором будут храниться все данные. После последовательно считывается информация о каждом студенте и проверяется его пол и фамилия для реализации разделения группы студентов на две другие: женскую и мужскую, сортированные по алфавиту.

В данном случае под классами-наследниками понимаются классы, наследующие основной функционал от классов-родителей (класс Program – родительский по отношению к классам File, Session, Student). Классы-друзья – классы, связанные с другими и имеющие определённые параметры доступа, в то время как не связанные не будут иметь таких прав. Концепция программы складывается в первую очередь из задач, постановленных перед любой базой данных: хранением, изменением (при необходимости), удалением и защищённостью (как критерий) системы в целом, они решаются благодаря различным способам работы с памятью, ниже приведены некоторые из них.

Функционал:

Student – класс для хранения основной информации о студенте, является дочерним классом Program. Является дружественным классом File.

bool Check_book () – метод класса Student для проверки существования студента с таким же номером зачетной книжки. Если не существует, возвращает истину, в противном случае – ложь.

Public: Student () – конструктор класса. Вызывается при создании объекта. Создает указатели на все необходимые переменные, описанные в области private.

~ Student () – деструктор класса, удаляет всю информацию, хранящуюся в объекте класса. Вызывается при уничтожении класса (пример очистки ненужной памяти, ссылки на которые были удалены или потеряли свою востребованность в семантическом плане).

Program – основной класс программы, он наследуется другими классами, содержит функции вывода на экран, а также методы, позволяющие правильно работать программе в любых ситуациях.

void print () – функция класса Program, перегружаемая функция для вывода информации в консоль. Виды функции: void print (char* val) – служит для вывода массива символов; void print (int val) – служит для вывода целочисленной информации; void print (const char val []) – служит для вывода массива символов.

Их использование обусловлено предназначением для различного функционала (об этом говорят различные типы переменных, от которых вызываются функции).

inline void Wait () – INLINE-функция, которая ждет нажатия клавиши ВВОД для продолжения выполнения программы.

virtual void print_v (char* val) – виртуальная функция, переопределяемая в классах-наследователях. Получает указатель на массив символов в переменную val в результате своего выполнения вывода val в консоль.

Sub – структура для описания предмета в какой-либо сессии студента, содержит имя предмета и оценку.

Session – класс для хранения информации о сессиях студента, является дочерним классов Program. Является дружественным классом File.

Crypto – класс для шифровки, дешифровки файла с данными.

File – класс, наследник Program, предназначен для работы с файлом.

int* pos – указатель на переменную целого типа, хранящую порядковый номер студента в файле.

int* count – указатель на переменную целого типа, хранящую количество студентов, записанных в файл.

char* gbn_t – указатель на массив символов, в котором записывается номер зачетной книжки студента, информацию о котором нужно удалить или изменить.

void Read_student() – метод для считывания информации о студенте из файла.

virtual void print_v(bool Full) – виртуальная переопределяемая функция класса File, которая выводит на экран информацию о студентах. Параметр Full отвечает за то, какую информацию выводить.

void Print_students (int rez, bool Task) – метод класса File для вызова функции print_v. Параметр rez отвечает за то, какую информацию выводить, параметр Task – также за информацию, которую мы хотим вывести.

Menu – класс, который отвечает за навигацию в программе и отрисовку меню, является наследником от класса Program.

int* ans – указатель на целочисленную переменную, которая отвечает за то, в какой пункт меню перейдет пользователь. Вводится с клавиатуры.

Mystr – класс для обработки массива символов.

void operator += (const char other []) – метод класса Mystr перегрузки оператора +=, в результате своего выполнения происходит конкатенация строки в data и строки, которая подается вторым параметром.

Указатели обеспечивают правильный (в совокупности с функциями) доступ к данным, во избежание конфликта по данным каждому было присвоено строго определённое значение длины, поскольку и динамическое, и статическое изменения затруднили или вовсе сделали бы невозможным обращение к требуемым участкам памяти. При написании программы были задействованы различные паттерны проектирования и основы объектно-ориентированного программирования, использованы принципы прямого доступа к памяти, приоритетности прерываний и параллелизма процессора.

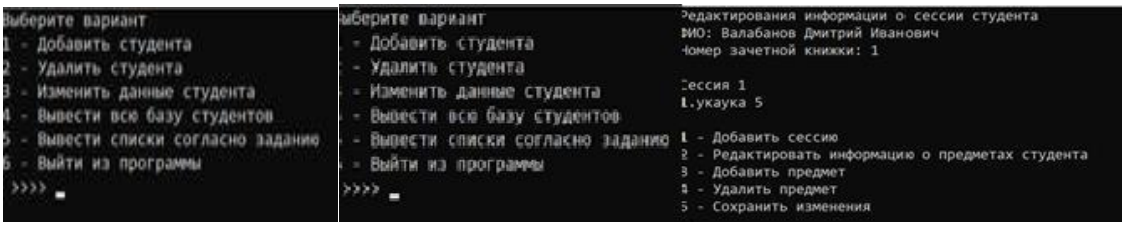
Фрагмент кода программы представлен в приложении.

При попытке считать данные без прав доступа злоумышленник получит лишь защищённый код (рис. 2).

```
▯   9t53Sjn6GHg7gyo3 ,Њ(▯1НИ1=1 ▯9Л<џ$t▯UЁЂт¤дTBSgOvqr…b”`™Йюр>▯Єзб¦Рц_Д·cXH€хБ-хм!¤l3#№»/
7|№Т™▯)▯ыГ+У,Bb
¶v©      ЋJЉП#♠р7&:wЧкљКЯШ ▯Ќ▯^ќ\Г«а€[єJЁ)туj&NцеДЧ·Б°S  MB▯ЩIв0▯¦¶е¤jpe
„ЧЦвΦR▯µ¦‹Ќ,▯?;ДЯ®gЌr@в#‰~4!Ф$Ф‘aCсйrlьыurc▯h▯E®iGd3)9MBйGC$ъ;JТоИ▯-м\hЏЬЭ;;ZyЂPc–¬PA=▯ma§Ус,;
s№O9HvЙрЎ€▯®RV®–ИµЕжЦw°ЂЛоGЌZ»љK=Ju¦X
```

Рисунок 2 – Пример вывода защищенного кода

Главное меню имеет упрощённый вид – нумерованный список (рис. 3а). При необходимости возможно добавление и удаление студентов (рис. 3б). В программе предусмотрена полноценная работа с информацией. Меню редактирования информации представлено на рисунке 3в.



а) б) в)

Рисунок 3 – Окна программы

Важным моментом является то, что определённые классы и методы могут быть написаны в любом порядке, а связано это в первую очередь с тем, что перед непосредственным выполнением программы происходит проверка её синтаксиса и последовательности действий (на этой стадии выполнения могут быть обнаружены ошибки или вызваны исключения).

Результаты и обсуждения. Структура языка C++ такова, что после выполнения функций данные, ссылки на которые обрываются, должны быть удалены, это как раз и необходимо для соблюдения принципов когерентности, ведь сюда в ходе последующего выполнения программы будут записаны новые данные. Также это необходимо, очевидно, для того, чтобы не засорять свободную память, тем самым понижая производительность системы. Такое отношение к данным обусловлено ориентированностью языка на более точные программные разработки, в которых необходима точность. В дополнение ко всему управление самой памятью происходит пользователем (разработчиком) вручную. Такой способ работы с памятью занимает большое количество времени, однако позволяет более

точно оформить взаимодействие структур данных, файлов, баз данных и реализацию потоков. По этой причине C++ является высокопроизводительным (по сравнению с другими языками), что иной раз доказывает рациональное использование ресурсов процессора.

Как и во многих других случаях для обеспечения работоспособности кода к программе были подключены пространства имён и действующие библиотеки других разработчиков, обеспечивающих сокращение написания кода, а также дающих дополнительные возможности. Для повышения производительности и работоспособности программы был использован принцип совмещения операций в обоих своих проявлениях.

Параллелизм здесь заключается в работе функций (методов) не с самими ссылками на объекты, а с их копиями, в данном случае все данные меняются в ходе выполнения, в связи с этим непосредственная работа с данными по прямым ссылкам является затруднительной, а в некоторых случаях даже невозможной. Конвейеризация заключается в работе с копиями ссылок на объекты в последовательном формате. Для конвейеров, в зависимости от его типа, можно математически вычислить его загруженность, время работы и производительность. Его использование оправдано в том случае, если загруженность будет близка к максимальной, поскольку малое количество данных хоть и будет обрабатываться чуть быстрей, но вызовет дополнительные потери из-за обращения к процессору и другим инструкциям, необходимым для целостной работы конвейера.

В результате проведённой работы была написана программа, основной функционал которой: работа с потоками команд и данных, статическая и динамическая виды памяти. С её помощью удобно хранить информацию об обучающихся, редактировать её по мере необходимости, а удобный интерфейс позволяет наглядно оценить полный или краткий список информации о конкретном студенте, также есть алфавитная сортировка и разделение в зависимости от пола. Поскольку программа должна иметь достойное практическое значение, в ней были использованы функции, защищающие от опечаток (например, если вместо оценки будет введена какая-то буква), а также от информации, ошибки в которой могут быть не замечены на протяжении длительного периода времени (например, введён 20002 год рождения). Использование современных криптографических моделей и методов защиты гарантирует целостность, достоверность введённой информации и отсутствие возможности хищения личных данных обучающихся. Программа может эффективно применяться разными людьми: от школьников до специалистов по работе с информацией.

Работа над программой может быть продолжена в направлении ее совершенствования, например, для ее адаптации к образовательной деятельности высших учебных заведений. Так как следует учитывать, что в настоящее время электронную информационно-образовательную среду современного университета рассматривают как средство реализации различных видов обратной связи между участниками информационно-образовательного процесса, фактор внедрения инструментов информационного-образовательного взаимодействия [10]. Эти требования с учетом запросов хорошо подготовленных пользователей могут привести к необходимости изменения концепции программы, исходя из потребности установления обратной связи «образовательное учреждение-студент». Для этого по списку главного меню «4-Вывести всю базу студентов» следует предусмотреть переход к окну «Информация для группы». В данном окне можно предусмотреть предоставление списка предметов (дисциплин) в зависимости от направления подготовки, курса, семестра. При переходе к конкретной дисциплине можно предусмотреть возможность просмотра следующих материалов, предоставляемых преподавателем (кафедрой) по данной дисциплине: рабочая программа дисциплины, рейтинг-план дисциплины, тестовые задания, ведомость текущей успеваемости, контактная среда для общения преподавателя со студентом в форме письменных сообщений. Можно также обеспечить среду для передачи файлов: учебных материалов от преподавателя студентам и отчетов от студентов преподавателю. Для осуществления связи «образовательное учреждение – студент» необходимо организовать защищенный и персонифицированный вход в программу как преподавателей, так и студентов. Добавление новых функций возможно путем усовершенствования предложенной блок-схемы, а не путем создания нового проекта, так как программа использует как динамическую, так и статическую оперативную память.

Заключение. Рассмотренный подход совершенствования программы с установлением обратной связи «образовательное учреждение – студент» позволит, оставляя в своей основе принцип, что современные базы данных должны иметь возможность изменения во времени, обеспечить появление в программе новых функций. При этом важно, что добавление новых функций возможно путем усовершенствования предложенной блок-схемы, а не путем создания нового проекта. Таким образом, предлагаемая программа, которая использует как динамическую, так и статическую оперативную память, дает возможность системно решать проблему согласованности всех её компонентов, как существующих, так и вновь введенных, с учетом меняющихся условий окружающей среды.

Библиографический список

1. Кунц, Е. Ю. Использование компетентностной модели образовательной программы для принятия управленческих решений в образовательной организации / Е. Ю. Кунц, П. С. Ложников // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 2 (58). – С. 27–34.

2. Федин, М. В. Электронная информационно-образовательная среда / М. В. Федин, М. В. Панкратов, К. А. Лещанкин // Свидетельство о регистрации программы для ЭВМ RU 2019615133, 18.04.2019. – Заявка № 2019613801 от 10.04.2019.

3. Федин, М. В. Программный модуль для системы анкетирования в электронной информационной-образовательной среде / М. В. Федин, М. В. Панкратов, К. А. Лещанкин // Свидетельство о регистрации программы для ЭВМ RU 2019665955, 03.12.2019. – Заявка № 2019664591 от 20.11.2019.

4. Федин, М. В. Программный модуль для подсистемы тестирования электронной информационной-образовательной среды / М. В. Федин, М. В. Панкратов, К. А. Лещанкин // Свидетельство о регистрации программы для ЭВМ RU 2019665806, 28.11.2019. – Заявка № 2019664661 от 20.11.2019.

5. Астахова, И. Ф. Разработка моделей и методов автоматизации обучения и контроля знаний студентов с помощью искусственного интеллекта / И. Ф. Астахова, А. А. Пшеничных // Фундаментальные исследования. – 2011. – № 12–1. – С. 77–80.

6. Рыбанов, А. А. Разработка web-ориентированной информационной системы мониторинга и управления процессом прохождения производственной практики / А. А. Рыбанов, А. В. Рыльков // Молодой ученый. – 2013. – № 7 (54). – С.34–36.

7. Гради, Б. Объектно-ориентированный анализ и проектирование с примерами приложений на C++. Второе издание / Б. Гради. – 2008. – 720 с.

8. Герберд, Ш. Полный справочник по C++ : пер. с англ. / Ш. Герберд. – 4-е изд. – Москва : Издательский дом «Вильямс», 2006. – 800 с.

9. Бьюли, А. Изучаем SQL / А. Бьюли // Символ. – 2007. – 311 с.

10. Рулиене, Л. Н. Электронная информационно-образовательная среда современного университета : монография / Л. Н. Рулиене, Н. Б. Сэкулич, С. Д. Намсараев. – Улан-Удэ : Изд-во Бурятского госуниверситета. 2018. – 148 с.

References

1. Kunts, E. Yu. Ispolzovanie kompetentnostnoy modeli obrazovatelnoy programmy dlya prinyatiya upravlencheskikh resheniy v obrazovatelnoy organizatsii [Using the competence model of an educational program for making managerial decisions in an educational organization]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2022, no. 2 (58), pp. 27–34.

2. Fedin, M. V. Elektronnaya informatsionno-obrazovatelnaya sreda [Electronic information and educational environment]. *Svidetelstvo o registratsii programmy dlya EHVM RU 2019615133* [Certificate of registration of the computer program RU 2019615133], 2019.

3. Fedin, M. V. Programmnyy modul dlya sistemy anketirovaniya v elektronnoy informatsionnoy-obrazovatelnoy srede [Software module for the questionnaire system in the electronic and information-educational environment]. *Svidetelstvo o registratsii programmy dlya EHVM RU 2019665955* [Certificate of registration of the computer program RU 2019665955], 2019.

4. Fedin, M. V. Programmnyy modul dlya podsistemy testirovaniya elektronnoy informacionnoy-obrazovatelnoy sredy [Software module for the testing subsystem of the electronic and information-educational environment]. *Svidetelstvo o registratsii programmy dlya EHVM RU 2019665806* [Certificate of registration of the computer program RU 2019665806], 2019.

5. Astakhova, I. F. Razrabotka modeley i metodov avtomatizatsii obucheniya i kontrolya znaniy studentov s pomoshchu iskusstvennogo intellekta [Development of models and methods for automating learning and controlling students' knowledge using artificial intelligence]. Fundamentalnye issledovaniya [Fundamental Research], 2011, no. 12–1, pp. 77–80.

6. Rybanov, A. A. Razrabotka web-orientirovannoy informatsionnoy sistemy monitoringa i upravleniya protsessom prokhozhdeniya proizvodstvennoy praktiki [Development of a web-oriented information system for monitoring and managing the process of passing an industrial practice]. *Molodoy uchenyy* [Young Scientist], 2013, no. 7 (54), pp. 34–36.

7. Gradi, B. *Obektno-orientirovannyy analiz i proektirovanie s primerami prilozheniy na S++. Vtoroe izdanie* [Object-oriented analysis and design with examples of applications in C ++. The second edition], 2008. 720 p.

8. Gerberd, Sh. *Polnyy spravochnik po C++* [The Complete C++ Reference], 2006. 800 p.

9. Byuli ,A. *Izuchaem SQL* [Learning SQL], 2007. 311 p.

10. Ruliene, L. N. *Elektronnaya informatsionno-obrazovatelnaya sreda sovremennogo universiteta : monografiya* [Electronic information and educational environment of a modern university : monograph]. Ulan-Ude, Publishing House of the Buryat State University, 2018. 148 p.

Приложение

Фрагмент кода, реализующего защиту информации:

```
class Crypto {
private:
char* Gen_pass() {
srand(time(NULL));
char* pass = new char[17];
```

```
for (int i = 0; i < 16; ++i)
{
switch (rand() % 3) {
case 0:
pass[i] = rand() % 10 + '0';
break;
case 1:
pass[i] = rand() % 26 + 'A';
break;
case 2:
pass[i] = rand() % 26 + 'a';
}
}
pass[16] = '\0';
return pass;
}
public:
void Encrypt() {
Mystr PATH_ENC(PATH);
PATH_ENC += ".enc";
ifstream File;
File.open(PATH, ios::binary);
ofstream File_enc;
File_enc.open(PATH_ENC.Get(), ios::binary | ios::app);
File_enc.seekp(0, ios::beg);
int length;
File.seekg(0, ios::end);
length = File.tellg();
File.seekg(0, ios::beg);
char* szPassword  = Gen_pass();
int dwLength = strlen(szPassword);
File_enc.write((char*)&dwLength, sizeof(dwLength));
File_enc.write((char*)szPassword, dwLength + 1);
HCRYPTPROV hProv;
HCRYPTKEY hKey;
HCRYPTHASH hHash;
if (!CryptAcquireContext(&hProv, NULL, NULL, PROV_RSA_AES, CRYPT_VERIFYCONTEXT))
{
cout << "Error during CryptAcquireContext!";
}
if (!CryptCreateHash(hProv, CALG_MD5, 0, 0, &hHash))
{
cout << "Error during CryptCreateHash!";
}
if (!CryptHashData(hHash, (BYTE*)szPassword, (DWORD)dwLength, 0))
{
cout << "Error during CryptHashData!";
}
if (!CryptDeriveKey(hProv, CALG_RC4, hHash, CRYPT_EXPORTABLE, &hKey))
{
cout << "Error during CryptDeriveKey!";
}
size_t enc_len = 8;
DWORD dwBlockLen = 1000 - 1000 % enc_len;
DWORD dwBufferLen = 0;
if (enc_len > 1)
{
dwBufferLen = dwBlockLen + enc_len;
}
else
{
dwBufferLen = dwBlockLen;
}
int count = 0;
bool final = false;
while (count != length) {
```

```
if (length - count < dwBlockLen) {
dwBlockLen = length - count;
final = true;
}
BYTE* temp = new BYTE[dwBufferLen]();
File.read((char*)temp, dwBlockLen);
if (!CryptEncrypt(hKey, NULL, final, 0, temp, &dwBlockLen, dwBufferLen))
{
cout << "Error during CryptEncrypt. \n";
}
File_enc.write((char*)temp, dwBlockLen);
count = count + dwBlockLen;
}
if (hHash)
{
if (!(CryptDestroyHash(hHash)))
cout << "Error during CryptDestroyHash";
}
if (hKey)
{
if (!(CryptDestroyKey(hKey)))
cout << "Error during CryptDestroyKey";
}
if (hProv)
{
if (!(CryptReleaseContext(hProv, 0)))
cout << "Error during CryptReleaseContext";
}
File.close();
File_enc.close();
if (remove(PATH) != 0) {
cout << "ERROR -- ошибка при удалении файла\n";
}
}
void Decrypt() {
Mystr PATH_ENC(PATH);
PATH_ENC += ".enc";
ofstream File;
File.open(PATH, ios::binary | ios::app);
ifstream File_enc;
File_enc.open(PATH_ENC.Get(), ios::binary);
int length;
File_enc.seekg(0, ios::end);
length = File_enc.tellg();
File_enc.seekg(0, ios::beg);
if (length == -1 || length == 0) {
return;
}
int dwLength;
File_enc.read((char*)&dwLength, sizeof(dwLength));
char* szPassword = new char[dwLength];
File_enc.read((char*)szPassword, dwLength + 1);
HCRYPTPROV hProv;
HCRYPTKEY hKey;
HCRYPTHASH hHash;
if (!CryptAcquireContext(&hProv, NULL, NULL, PROV_RSA_AES, CRYPT_VERIFYCONTEXT))
{
cout << "Error during CryptAcquireContext!";
}
if (!CryptCreateHash(hProv, CALG_MD5, 0, 0, &hHash))
{
cout << "Error during CryptCreateHash!";
}
if (!CryptHashData(hHash, (BYTE*)szPassword, (DWORD)dwLength, 0))
{
cout << "Error during CryptHashData!";
```

```
}
if (!CryptDeriveKey(hProv, CALG_RC4, hHash, CRYPT_EXPORTABLE, &hKey))
{
cout << "Error during CryptDeriveKey!";
}
size_t enc_len = 8;
DWORD dwBlockLen = 1000 - 1000 % enc_len;
DWORD dwBufferLen = 0;
if (enc_len > 1)
{
dwBufferLen = dwBlockLen + enc_len;
}
else
{
dwBufferLen = dwBlockLen;
}
int count = sizeof(dwLength) + strlen(szPassword) + 1;
bool final = false;
while (count != length) {
if (length - count < dwBlockLen) {
dwBlockLen = length - count;
final = true;
}
BYTE* temp = new BYTE[dwBlockLen];
File_enc.read((char*)temp, dwBlockLen);

if (!CryptDecrypt(hKey, 0, final, 0, temp, &dwBlockLen))
{
cout << "Error during CryptEncrypt. \n";
}

File.write((char*)temp, dwBlockLen);
count = count + dwBlockLen;
}
if (hHash)
{
if (!(CryptDestroyHash(hHash)))
cout << "Error during CryptDestroyHash";
}
if (hKey)
{
if (!(CryptDestroyKey(hKey)))
cout << "Error during CryptDestroyKey";
}
if (hProv)
{
if (!(CryptReleaseContext(hProv, 0)))
cout << "Error during CryptReleaseContext";
}
File.close();
File_enc.close();
if (remove(PATH_ENC.Get()) != 0) {
cout << "ERROR -- ошибка при удалении файла\n";
}
}
};
class Menu : Program {
public:
Menu() {
ans = new int;
SetConsoleCP(1251);
SetConsoleOutputCP(1251);
system("cls");
file = new File;
}
~Menu() {
```

```
delete file;
delete ans;
}
bool hub() {
file = new File;
system("cls");
print("Выберите вариант\n");
print("1 - Добавить студента\n");
print("2 - Удалить студента\n");
print("3 - Изменить данные студента\n");
print("4 - Вывести всю базу студентов\n");
print("5 - Вывести всех студентов по заданию: \n");
print("6 - Выйти из программы\n");
print(" >>>> ");
cin >> *ans;
cin_cl();
switch (*ans) {
case 1: {
system("cls");
print("Добавление нового студента(Введите -1, чтобы вернуться назад)\n");
file->Add_student();
Wait();
break;
}
case 2: {
system("cls");
print("Удаление студента\n");
file->Delete_student();
Wait();
break;
}
case 3: {
file->Edit_student();
Wait();
break;
}
case 4: {
system("cls");
print("Вывод всех студентов\n");
print("1 - Вывод всей информации\n");
print("2 - Вывод части информации\n");
print("3 - Назад\n");
print(">>> ");
cin >> *ans;
switch (*ans) {
case 1:
file->Print_students(4, false);
Wait();
break;
case 2:
file->Print_students(2, false);
Wait();
break;
case 3:
break;
}
break;
}
case 5:
system("cls");
print("Условия задания: \n");
print("1 - Вывести список студентов без оценок 5: \n");
print("2 - Назад\n");
print(">>> ");
cin >> *ans;
switch (*ans) {
```

```
        case 1:
        file->Print_students(4, true);
        Wait();
        break;
        case 2:
        break;
        }
        break;
        Wait();
        break;
        case 6:
        return false;
        }
        return true;
        delete file;
        }
        private:
        File* file = nullptr;
        int* ans = nullptr;
        };

        int main() {
        Menu* menu = new Menu();
        while (menu->hub());
        delete menu;
        return 0;
        }
        . . .
        class Mystr {
        private:
        char* data = nullptr;

        public:
        Mystr(const char in[]) {
        data = new char[strlen(in) + 1]();
        for (int i = 0; i < strlen(in); i++) {
        *(data + i) = in[i];
        }
        data[strlen(data)] = '\0';
        }
        ~Mystr() {
        delete[] data;
        }
        void operator += (const char other[]) {
        char* temp = new char[strlen(data) + strlen(other) + 1]();
        int i = 0;
        for (; i < strlen(data); i++) {
        *(temp + i) = *(data + i);
        }
        for (int j = 0; j < strlen(other); j++) {
        *(temp + i + j) = *(other + j);
        }
        temp[strlen(temp)] = '\0';
        delete[] data;
        data = new char[strlen(temp) + 1]();
        for (i = 0; i < strlen(temp); i++) {
        *(data + i) = *(temp + i);
        }
        data[strlen(data)] = '\0';
        }
        char* Get() {
        return data;
        }
};
```

УДК 004.001

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДИК ИССЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Статья поступила в редакцию 29.08.2022, в окончательном варианте – 29.08.2022.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Карманов Михаил Александрович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0003-0953-8125, e-mail: michaelkdev15@gmail.com
Немчинова Валерия Олеговна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
ассистент, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

В настоящей статье представлен сравнительный анализ определенных методик исследования защищенности мобильных приложений. Был выбран ГОСТ Р ИСО/МЭК 18045-2013 – МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ и методика стандарта Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS), использующая в совокупности с техническим руководством тестирования безопасности в аспекте мобильных устройств (OWASP Mobile Security Testing Guide). В контексте работы с мобильными приложениями были отобраны целевые разделы у каждого из стандартов, были определены их сильные и слабые стороны. Был определен набор критериев для оценки методов и подходов к анализу защищенности мобильных приложений, который в будущем может быть расширен или дополнен. Для выбранных методов был выполнен сравнительный анализ по определенному набору критериев для случая, когда все критерии равнозначны и когда выделен некоторый набор более весомых – в случае использования данных стандартов именно при анализе мобильных приложений. В итоге были получены результаты, определяющие применение того или иного стандарта при различных случаях.

Ключевые слова: мобильные приложения, Android, iOS, пользовательская информация, критичная информация, защита данных, кибербезопасность

COMPARATIVE ANALYSIS OF EXISTING RESEARCH METHODS FOR MOBILE APPLICATIONS SECURITY

The article was received by the editorial board on 29.08.2022, in the final version – 29.08.2022.

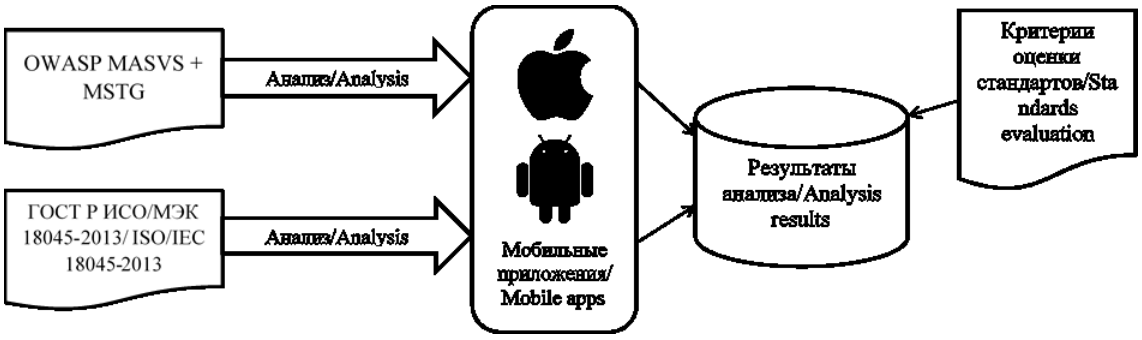
Putyato Mikhail M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: msanya@yandex.ru
Karmanov Mikhail A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
postgraduate student, ORCID: 0000-0003-0953-8125, e-mail: michaelkdev15@gmail.com
Nemchinova Valeriya O., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Assistant, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

This article provides a comparative analysis of certain methods for studying the security of mobile applications. ISO/IEC 18045-2013 (METHODS AND MEANS OF SAFETY. METHODOLOGY FOR ASSESSING THE SECURITY OF INFORMATION TECHNOLOGIES) standard and the methodology of the Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (MASVS) were chosen for, which is used with OWASP Mobile Security Testing Guide (MSTG). During mobile applications security analysis context, target sections

for each of the standards were selected, their pluses and weaknesses were identified. A set of criteria for evaluating methods and approaches to the analysis of the security of mobile applications was determined, which can be expanded or supplemented in the future. For the selected methods, a comparative analysis was carried out according to a certain set of criteria for the case when all criteria are equivalent and when a certain set of more significant ones was selected – in the case of using these standards in the analysis of mobile applications. As a result, results were obtained that determine the application of one or another standard in various cases.

Keywords: mobile apps, Android, iOS, personal data, data protection, critical information, cybersecurity

Graphical annotation (Графическая аннотация)



Введение. В процессе работы перед любым программным обеспечением встает задача обработки информации определенным образом. Алгоритмы работы приложения проектируются и реализуются людьми, что потенциально может привести к тем или иным ошибкам, которые могут стать причиной недочетов и уязвимостей безопасности программного продукта и обрабатываемой информации. Для оперативного устранения подобных недочетов необходимо обращаться к методикам и руководствам исследования защищенности и создания «безопасных» архитектур [1–3].

Описанное выше присуще, в том числе, мобильным приложениям, спроектированным и реализованным для работы на смартфонах, планшетах, умных часах и других мобильных устройствах. На сегодняшний день подобные мобильные устройства могут решить любые задачи благодаря устанавливаемым приложениям. Как следствие, каждое такое приложение оперирует определенным набором данных (пользовательских и данных правообладателя), которые подлежат защите [4].

Развитие информационных технологий способствовало тому, что в настоящее время мобильные устройства берут на себя задачи, для которых раньше требовалось наличие специализированного оборудования. Любой смартфон сегодня содержит множество персональных и корпоративных данных, стоимость которых значительно выше стоимости самого устройства. Поэтому проблема защиты данных мобильных устройств критически важна.

Цель и задачи. Целью данной работы является выделение эффективного подхода к анализу защищенности информации в контексте мобильного приложения.

При постановке цели данной работы были определены следующие задачи:

1) определить перечень существующих методик и подходов, применимых при анализе защищенности мобильных приложений;

2) определить сферы оценки защищенности мобильных приложений для выявленных методик и подходов;

3) определить перечень критериев для оценки методик и подходов и провести сравнительный анализ по данному перечню.

Существующие методы анализа защищенности информации. На момент 3 квартала 2021 года можно выделить различные методики анализа защищенности информации. Первым можно считать оценку профиля защиты по различным аспектам. Полный перечень доступен в стандарте ИСО/МЭК 18045-3-2013 [5]. Касательно анализа защищенности мобильных приложений можно выделить следующие классы:

– разработка архитектуры безопасности (ADV_ARC) [5]. Методы оценки из данного класса отвечают за оценку функциональных возможностей механизмов обеспечения безопасности определенного объекта на предмет невозможности вмешательства в них или обхода;

– разработка политики безопасности (ADV_SPM) [5]. Класс отражает набор требований к процессу проектирования политики безопасности;

– устранение недостатков (ALC_FLR) [5]. Класс, нацеленный, прежде всего, на разработчиков программного обеспечения, содержит инструменты для устранения недостатков объекта в процессе эксплуатация и сопровождения;

– безопасность разработки (ALC_DVS) [5]. Аналогично с классом «ALC_FLR», класс «ALC_DVS» ориентирован на разработчиков, содержит набор требований безопасности для среды разработки, которая должна обеспечивать конфиденциальность разрабатываемого объекта в ней, его целостность и должна обеспечивать возможность его реализации;

– тестирование (ATE) [5]. Данный класс содержит в себе обширный список критериев. В рамках настоящей работы выделены критерии покрытия полноты тестов (ATE_COV), глубины детализации при тестировании (ATE_DPT), а также критерии функционального (ATE_FUN) и независимого (ATE_IND) тестирования;

– оценка уязвимостей (AVA) [5]. Данный класс включает в себя набор методов по идентификации и анализу уязвимостей (подкласс AVA_VAN).

В стандарте предусмотрена градация оценочных уровней доверия (далее – ОУД) от 1 (минимально возможный уровень доверия к системе) до 7 (максимальный уровень), являющийся соотношением получаемого уровня доверия со стоимостью и возможностью достижения этой степени доверия. Так, ОУД1 означает продукт или систему, которая подвергалась базовой оценке, а ОУД7 подразумевает использования полного перечня компонентов доверия из ОУД [5].

Сравнение количества используемых компонентов из представленных выше классов в зависимости от ОУД представлено в таблице 1.

Таблица 1 – Сравнение количества используемых компонентов из представленных выше классов в зависимости от ОУД

Класс доверия	**Семейство доверия**	**Компоненты доверия из оценочного уровня доверия**						
		ОУД1	**ОУД2**	**ОУД3**	**ОУД4**	**ОУД5**	**ОУД6**	**ОУД7**
Разработка	Разработка архитектуры безопасности ADV_ARC	0	1	1	1	1	1	1
	Разработка политики безопасности ADV_SPM	0	0	0	0	0	1	1
Поддержка жизненного цикла	Устранение недостатков ALC_FLR	0	0	0	0	0	0	0
	Безопасность разработки ALC_DVS	0	0	1	1	1	2	2
Тестирование	Тесты покрытия и критерии покрытия полноты тестов ATE_COV	0	1	2	2	2	3	3
	Глубина детализации при тестировании ATE_DPT	0	0	1	2	3	3	4
	Критерии функционального тестирования ATE_FUN	0	1	1	1	1	2	2
	Критерии независимого тестирования ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	Анализ уязвимостей AVA_VAN	1	2	2	3	4	5	5

В контексте мобильных приложений можно добавить, что для ОУД1 достаточно применить независимое тестирование и провести базовый анализ уязвимостей. Тогда как в приложении не будет четкой архитектуры и политики безопасности, не будут соблюдаться требования по безопасности разработки.

Стоит отметить, что, используя подход в данном стандарте, можно в полной мере оценивать лишь информационные системы. Оценивание программного обеспечения частных элементов как в составе подобных систем, так и в самостоятельном виде, является побочным свойством. Другим важным аспектом данного подхода является эфемерность шагов по оцениванию того или иного профиля защиты. «Легко идентифицируемые уязвимости» или оценивающее лицо «должно убедиться» и т.д. – все это примеры эфемерности подхода в угоду абстрагирования стандарта. Но, как итог, включается человеческий фактор, и каждый специалист в силу собственного опыта, знаний и прочих характеристик может получать разные результаты.

Как пример, специалист обладает навыками тестировщика, и данное им заключение по классу тестирования можно расценивать как гарант, но в силу определенных обстоятельств он же производил оценку уязвимостей, где для него «легко идентифицируемые уязвимости» объективно могут не являться таковыми.

Анализ других нормативных и законодательных документов России в области защиты конфиденциальной информации и вопросов защиты информации показал, что в настоящее время методических рекомендаций по защите информации в разрезе мобильных устройств найдено не было.

Другая методика – это неофициальный стандарт проверки защищенности мобильного приложения (OWASP Mobile Application Security Verification Standard) (далее – стандарт OWASP MASVS) [6]. Данный стандарт используется в совокупности с техническим руководством тестирования безопасности в аспекте мобильных устройств (OWASP Mobile Security Testing Guide) (далее – OWASP MSTG) [7], которое помимо технических реализаций требований стандарта содержит информацию по развертыванию тестировочных платформ для операционных систем Android и iOS, и т.н. «чеклистом» безопасности мобильного приложения [8]. По сравнению с приведенным выше стандартом, данное решение имеет четко определенные алгоритмы исследования и критериев оценки защищенности программного обеспечения.

Согласно содержанию стандарта, любой оцениваемый объект рассматривается исходя из целевого уровня защиты, которых представлено 3 вида:

– уровень 1 – минимальный уровень требований к механизмам защиты для любого мобильного приложения. Ориентирован на противодействие легко реализуемым уязвимостям и нарушителю с низким уровнем подготовки;

– уровень 2 – стандартный уровень, который должен применяться к приложениям, которые оперируют критичной информацией. Ориентирован на противодействие подготовленному нарушителю и перечню активно используемого программного обеспечения для поиска уязвимостей в приложениях;

– уровень 3 – продвинутый или высший уровень, применим в военных, медицинских целях, в условиях нахождения в критической инфраструктуре.

В контексте настоящей работы внимание акцентируется на следующих требованиях стандарта:

– требования к архитектуре, дизайну и модели угроз (MSTG-ARCH). Данные требования предписывают в зависимости от выбранного уровня безопасности идентифицировать все компоненты приложения, составить список возможных проверок как завершенного продукта, так и проекта в стадии создания, определить перечень «чувствительных данных». На этапе проектирования должны быть учтены положения по защите данных в приложении в соответствии с регламентирующими положениями, документами и законами стран, в которых приложение будет использоваться;

– требования к конфиденциальности и хранению данных (MSTG-STORAGE). Данные требования предписывают для идентифицированных «чувствительных» данных хранение в защищенных областях устройства и приложения, разграничение доступа к этим данным, особенности отображения в пользовательском интерфейсе при различных состояниях приложения и устройства, минимальные настройки безопасности устройства для работы приложения;

– требования для функций криптографических провайдеров (MSTG-CRYPTO). Здесь можно выделить как явные указания не хранить симметричные ключи шифрования в ходе в каком бы то ни было виде или не использовать устаревшие или непроверенные реализации криптографических алгоритмов, так и оценка целесообразности использования того или иного криптографического алгоритма в определенной функции работы приложения;

– все требования касательно аутентификации (хранение учетных данных, их резервирование, жизненный цикл, верификаторы учетных данных и другие) и управления сессиями (MSTG-AUTH). Требования применимы в случае наличия в мобильном приложении взаимодействия с серверной частью и наличием учетных записей;

– требования для сетевого взаимодействия (MSTG-NETWORK);

– набор условий при взаимодействии с операционной системой устройства (MSTG-PLATFORM). Общими для операционных систем Android и iOS можно выделить минимально необходимый перечень разрешений, минимизация использования *WebView* и применения в нем Javascript;

– требования к сборке приложения (MSTG-CODE) – перечень настроек и рекомендаций при создании релизной версии приложения;

– триггеры устойчивости к атакам на стороне клиента (MSTG-RESILIENCE). Сюда включены проверки на наличие *root/jailbreak*, антиотладочные техники, проверка валидности установочного пакета приложения в качестве мер противодействия динамическому анализу и фальсификациям, а также обфускация исходного кода для противодействия реверс-инжиниринга приложения.

В совокупности с этими абстрактными требованиями можно обратиться уже к техническому руководству: оно включает в себя прикладные сценарии проверки того или иного признака требования, предъявляемого к мобильным приложениям, приведенного в основном стандарте для получения

конкретных действий для соответствия тому или иному требованию стандарта. Так, для представленного выше списка требований можно определить перечень механизмов защиты и необходимых действий. К примеру, одна из подзадач защиты учетных данных в мобильном приложении для различных уровней защиты и платформ операционных систем реализуется по-разному:

– для первого уровня в случае отсутствия в приложении критичных данных допускается хранение учетных данных в открытом виде в конфигурационного xml-файла, т.н. shared preferences, для операционной системы Android, для iOS – в общем хранилище параметров, т.н. User Default, или конфигурационном файле формата Property List (plist);

– для второго уровня в операционной системе Android допускается хранение данных в открытом виде в защищенном хранилище Android KeyStore или с использованием криптографических средств в конфигурационном xml-файле, для iOS – хранение в связке ключей Keychain в открытом виде, а также в конфигурационном файле, но уже в зашифрованном виде;

– для третьего уровня четкие требования отсутствуют – есть лишь замечание, что используемые меры защиты должны быть сопоставимы, как минимум, со вторым уровнем защиты.

В качестве примера полного цикла использования методики можно рассмотреть подзадачу по защите учетных данных. Из «чек-листа», например, взят критерий недопустимости записи в журналы работы приложения критичных данных. Стандарт MASVS будет давать более конкретизированные требования критериев – отсутствие подобных записей только в релизной сборке приложения или вообще во всех. А в MSTG уже можно найти способы решения данной задачи – поиск классов «логгирования», поиск в исходном коде обращений вывода данных в консоль в зависимости от целевой платформы. Графическое представление особенностей работы с данной методикой на примере критерия недопустимости записи в журналы работы приложения критичных данных представлено на рисунке 1.

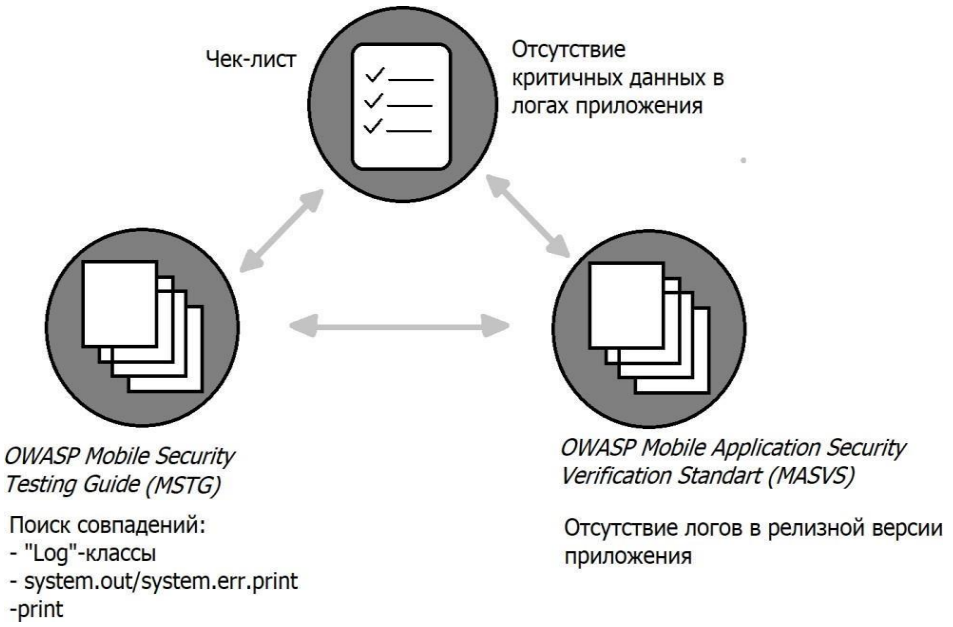


Рисунок 1 – Графическое представление особенностей работы с данной методикой на примере критерия недопустимости записи в журналы работы приложения критичных данных

Стоит отметить, что был приведен пример с неполным перечнем альтернатив, который гораздо больше и может не ограничиваться штатными методами мобильных операционных систем.

Имея требования и способы соответствия им в виде реализаций, оценивающее лицо с помощью всех документов может вынести вердикт касательно защищенности программного продукта.

При использовании подхода данного стандарта стоит учитывать некоторые моменты:

– проведение проверок сопряжено с человеческим фактором, хоть и в меньшей степени;

– стандарт не является государственным, и его возможное использование является добровольным решением;

– несмотря на то, что данный набор документации разработан исключительно для мобильных приложений, требования из них могут применяться и к другим платформам.

Набор критериев для оценки методов и подходов к анализу защищенности мобильных приложений. Для сравнения двух представленных выше методик обеспечения защиты будет использован набор критериев, каждый из которых имеет определенные возможные значения [9]. Набор критериев сравнения методик анализа защищенности приложений приведен в таблице 2.

Таблица 2 – Набор критериев сравнения методик анализа защищенности приложений

Наименование критерия	Возможные значения критериев	Описание значений критериев
Официальность стандарта	Официальный	Документ утвержден в виде стандарта для хотя бы 1 государства и может являться обязательным для соответствия.
	Неофициальный	Не выполняются условия для статуса «официальный».
Доступность стандарта	В открытом доступе	Ознакомиться со стандартом и дополнительной документацией по нему можно на бесплатной основе и любому человеку.
	Предоставляется на платной основе	Получение доступа к стандарту и дополнительной документации по нему происходит на платной основе, причем ограничением здесь может выступать статус лица (физическое или юридическое лицо).
	Закрытый доступ	Получение доступа к стандарту и дополнительной документации по нему ограничено. Для ознакомления с ним необходимо пройти определенные процедуры. Примером могут быть различные виды информации ограниченного распространения (государственная, коммерческая тайна и т.д.).
Применимость стандарта [9, 10]	Узкоспециализированный	Стандарт используется в определенной области применения. Применение в других сферах сопряжено с неактуальностью информации в стандарте в относительном размере более 50 %.
	Условно универсальный	Стандарт предназначен для определенной области и может использоваться для смежных областей. Применение в других сферах сопряжено с неактуальностью информации в стандарте в относительном размере не менее 15 % и не более 50 %.
	Универсальный	Стандарт изначально разрабатывался под применение в различных областях. Применение в разных сферах допускает неактуальность информации в относительном размере не более 15 %.
Покрытие информацией (актуальность)	Низкое	Актуальность сведений менее 50 %. Признак того, что документ является устаревшим или скоро станет таковым.
	Среднее	Актуальность сведений более 50 %. Связана с невозможностью применения неактуальных сведений как ввиду их устаревания, так и по прочим причинам
	Высокое	Актуальность сведений более 90 %. Признак того, что стандарт новый или относительно недавно обновлялся.
Наличие дополнительной документации [8]	Отсутствует	Стандарт представлен в виде единого документа без дополнительной информации по нему.
	Присутствует	Вместе со стандартом идет различная сопутствующая документация, раскрывающая те или иные аспекты в более полной мере. Это может быть справочная информация, примеры применения, техническая документация и т.д.
Подверженность человеческому фактору при использовании	Отсутствует	Человеческого фактора при проведении оценки нет, иначе говоря, процедура работает в автоматическом режиме.
	Низкая	Человек присутствует в процессе как контроллер.
	Средняя	Человеческий фактор заключается в следовании четкой инструкции. Повышенные требования к подготовке в определенной области знаний отсутствуют.
	Высокая	Человеческий фактор заключается в следовании инструкции с абстрактными теоретическими шагами. К человеку предъявляются повышенные требования к подготовке в той или иной области знаний.
Периодичность обновлений	Неопределенная	Стандарт и документация по нему обновляется без привязки к временным промежуткам.
	Раз в 5 лет	Стандарт и документация по нему обновляется примерно раз в 5 лет.
	Ежегодная	Стандарт и документация по нему обновляется примерно ежегодно.
	Ежесезонная	Стандарт и документация по нему обновляется примерно раз в 3 месяца.

Продолжение таблицы 2

Возможность привлечения внешних участников	Отсутствует	Разработку и поддержку стандарта ведут только внутренние участники. Все остальные имеют лишь доступ для ознакомления с дистрибьюторскими версиями.
	Внешние контрибьюторы с урезанными правами, по сравнению с внутренними участниками	Разработку и поддержку стандарта ведут внутренние участники. Внешние участники могут повлиять на нее лишь косвенно: опросы, доступные версии стандартов на этапе разработки и поддержки.
	Внешние участники с полными правами	Разработку и поддержку стандарта ведут внутренние участники совместно с внешними, причем вторые на любое изменение будут проходить премодерацию

Сравнительный анализ методик оценки защищенности. Сравнительный анализ приведенных выше методик оценки защищенности по определенному перечню критериев представлен в таблице 3.

Таблица 3 – Сравнительный анализ методик оценки защищенности

Наименование критерия	**Показатель критерия для стандарта ИСО/МЭК 18045-3-2013**	**Показатель критерия для стандарта OWASP MASVS**	**Примечание**
Официальность стандарта	Официальный	Неофициальный	Стандарт OWASP MASVS опирается на американские государственные стандарты NIST SP 800-57, NIST SP 800-63B, NIST FIPS PUB186, NIST P-384, а также рекомендации NIST [5, 6]
Доступность стандарта	В открытом доступе	В открытом доступе	
Применимость стандарта	Условно-универсальный	Условно-универсальный	
Покрытие информацией (актуальность)	Среднее	Высокое	
Наличие дополнительной документации	Отсутствует	Присутствует	
Подверженность человеческому фактору при использовании	Высокая	Средняя	
Периодичность обновлений	Неопределенная	Ежесезонно	Стандарт OWASP MASVS обновляется по факту чаще и доступен в виде черновых версий стандарта
Возможность привлечения внешних участников	Отсутствует	Внешние участники с полными правами	

Если рассматривать все критерии как равнозначные, то можно сделать вывод, что оба стандарта являются относительно идентичными, со своими плюсами и минусами. Однако, имея вводную задачу в виде анализа защищенности именно мобильных приложений, появления недочетов и уязвимостей в безопасности продуктов при этапах проектирования, реализации и оставшихся без внимания на этапе тестирования и внедрения, можно выделить следующие приоритетные критерии:

– актуальность стандарта, так как мобильные устройства в настоящее время стремительно развиваются и обновляются технологически, что требует частое обновление стандартов;
– покрытие информацией (актуальность);
– наличие дополнительной документации касательно применения стандарта или метода;
– подверженность человеческому фактору при использовании.

Таким образом, относительно универсальный стандарт ИСО/МЭК 18045-3-2013 проигрывает более узкоспециализированному, содержащему дополнительную справочную информацию стандарту OWASP MASVS в случае анализа защищенности мобильных приложений.

Стоит отметить, что для представленных и проанализированных методик качественным скачком вперед было бы добавление алгоритмов анализа защищенности, адаптированных для реализации их в виде программных решений. Таким образом, можно будет нивелировать воздействие человеческого фактора на весь процесс анализа. Кроме того, в программном решении можно реализовать подсистемы обеспечения актуальности контрольных критериев как в виде обращений в общий репозиторий с информацией, так и в виде автономной системы с определенным алгоритмом работы [11]. Также такое решение может работать в совокупности. Как итог, полученное решение может выступать в качестве структурной единицы комплекса решений обеспечения ИБ [12].

Заключение. В работе рассмотрены определенные стандарты и методы, которые могут быть использованы при анализе защищенности мобильных приложений. Для проведения сравнительного анализа был определен набор критериев для оценки. Данный набор в будущем может быть расширен или дополнен. В процессе оценки было установлено, что при равнозначном весе критериев оба рассматриваемых стандарта являются идентичными с точки зрения плюсов и минусов применения. Однако при выделении некоторых критериев для оценки именно мобильных приложений как более приоритетных неофициальный стандарт OWASP MASVS со всеми его дополнениями является более предпочтительным для использования.

Библиографический список

1. Георгиевских, Н. В. Создание безопасных мобильных приложений / Н. В. Георгиевских // Аллея науки. – 2018. – Т. 22, № 6. – С. 985–988.

2. Сафин, Л. Л. Исследование информационной защищенности мобильных приложений / Л. Л. Сафин, А. В. Чернов, Я. А. Александров, К. Н. Трошина // Вопросы кибербезопасности. – 2015. – Т. 12, № 4. – С. 28–37.

3. Путято, М. М. Исследование возможности совершенствования кибербезопасности инфраструктуры интернета вещей на основе интеграции биометрических методов аутентификации / М. М. Путято, А. С. Макарян // Информационные системы и технологии в моделировании и управлении : сборник трудов V Международной научно-практической конференции. – 2020. – С. 267–270.

4. Карондеев, А. М. Исследование защищенности пользовательских данных мобильных приложений на примере мессенджера Whatsapp / А. М. Карондеев, Д. В. Клюев // Современная наука: актуальные проблемы теории и практики. – 2019. – № 7. – С. 88–93.

5. ГОСТ Р ИСО/МЭК 18045-2013 – Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. – Режим доступа: https://docs.cntd.ru/document/1200105309, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.08.2021).

6. Schleier, S. OWASP Mobile Application Security Verification Standard, Mobile application security check guide standard / S. Schleier, J. Willemsen, C. Holguera. – 2020. – 49 p.

7. Mueller, B. OWASP Mobile Security Testing Guide / B. Mueller, S. Schleier, J. Willemsen. – 2020. – 536 p.

8. Releases – OWASP/owasp-mstg – Github: Intermediate update 1.1.3. – Режим доступа: https://github.com/OWASP/owasp-mstg/releases/download/1.1.3-excel/Mobile_App_Security_Checklist-English_1.1.2.xlsx, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 22.08.21).

9. Nagarjun, P. Review of Mobile Security Problems and Defensive Methods / P. Nagarjun, S. S. Ahamad // International Journal of Applied Engineering Research. – 2018 – Vol. 13. – P. 10256–10259.

10. Курносов, К. В. Методика оценки безопасности информационных систем, построенных с использованием технологий виртуализации / К. В. Курносов // Доклады ТУСУР. – 2019. – Т. 22, № 1. – С. 37–44.

11. Симбирцев, Д. В. Разработка автоматизированной системы анализа защищенности веб-ресурсов / Д. В. Симбирцев, В. Г. Жуков // Актуальные проблемы авиации и космонавтики. – 2011. – Т. 1, № 7. – С. 430–431.

12. Макарян, А. С. Анализ практической реализации механизмов выявления кибератак в SIEM-системе SPLUNK / А. С. Макарян, М. М.Путято, А. Р. Очередько // Информационные системы и технологии в моделировании и управлении : сборник трудов V Международной научно-практической конферренции. – 2020. – С. 252–256.

References

1. Georgievskikh, N. V. Sozdanie bezopasnyh mobilnykh prilozheniy [Secure mobile applications development]. *Alleya nauki* [Alley of Science], 2018, no. 6 (22), pp. 985–988.

2. Safin, L. L., Chernov, A. V., Alexandrov, Ya. A., Troshina, K. N. Issledovanie informatsionnoy zashchishchennosti mobilnykh prilozheniy [A study of mobile application security]. *Voprosy kiberbezopasnosti* [Cybersecurity Questions], 2015, no. 4 (12), pp. 28–37.

3. Putyato, M. M., Makaryan, A. S. Issledovanie vozmozhnosti sovershenstvovaniya kiberbezopasnosti infrastruktury interneta veshchey na osnove integratsii biometricheskikh metodov autentifikatsii [Research possibilities for improvement cyber security internet infrastructure of things on basis for integration of biometric methods authentications]. *Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : sbornik trudov V Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Information systems and technologies in modeling and management : Proceedings of the V International Scientific and Practical Conference], 2020, pp. 267–270.

4. Karaondeev, A. M., Kluev, D. V. Issledovanie zashchishchennosti polzovatelskikh dannykh mobilnykh prilozheniy na primere messendzhera Whatsapp [A study of mobile application user data security on the example of Whatsapp messenger]. *Sovremennaya nauka: aktualnye problemy teorii i praktiki* [Modern Science: Actual Problems of Theory and Practice], 2019, no. 7, pp. 88–93.

5. *ISO/IEC 18045-2013 – Metody i sredstva obespecheniya bezopasnosti. Metodologiya otsenki bezopasnosti informatsionnykh tekhnologiy* [Methods and means of safety. Methodology for assessing the security of information technologies]. Available at: https://docs.cntd.ru/document/1200105309 (accessed 19.08.2021).

6. Schleier, S., Willemsen, J., Holguera, C. O*WASP Mobile Application Security Verification Standard, Mobile application security check guide standard*, 2020. 49 p.

7. Mueller, B., Schleier, S., Willemsen, J. *OWASP Mobile Security Testing Guide*, 2020. 536 p.

8. *Releases – OWASP/owasp-mstg – Github: Intermediate update 1.1.3.* Available at: https://github.com/OWASP /owasp-mstg/releases/download/1.1.3-excel/Mobile_App_Security_Checklist-English_1.1.2.xlsx (accessed 22.08.2021).

9. Nagarjun, P., Ahamad, S. S. Review of Mobile Security Problems and Defensive Methods. *International Journal of Applied Engineering Research*, 2018, no. 13, pp. 10256–10259.

10. Kurnosov, K. V. Metodika otsenki bezopasnosti informatsionnykh sistem, postroennykh s ispolzovaniem tekhnologiy virtualizatsii [Methodology for assessing the security of information systems built using virtualization technologies]. *Doklady TUSUR* [Proceedings of TUSUR University], 2019, no. 1 (22), pp. 37–44.

11. Simbirtsev, D. V., Jukov, V. G. Razrabotka avtomatizirovannoy sistemy analiza zashchishchennosti veb-resursov [Web resource automated security analysis system development]. *Aktualnye problemy aviatsii i kosmonavtiki* [Actual Problems of Aviation and Cosmonautics], 2011, no. 7 (1), pp. 430–431.

12. Makaryan, A. S., Putyato, M. M., Ocheredko, A. R. Analiz prakticheskoy realizatsii mekhanizmov vyyavleniya kiberatak v SIEM-sisteme SPLUNK [Analysis of the practical implementation of mechanisms for detecting cyber attacks in the SPLUNK SIEM system]. *Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : sbornik trudov V Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Information systems and technologies in modeling and management], 2020, pp. 252–256.

DOI 10.54398/20741707_2022_4_98
УДК 004.001

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АНАЛИЗА СИСТЕМНЫХ ЖУРНАЛОВ ОПЕРАЦИОННОЙ СИСТЕМЫ MICROSOFT WINDOWS[1]

Статья поступила в редакцию 25.10.2022, в окончательном варианте – 26.10.2022.

Павлычев Алексей Викторович, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
директор Центра информационной безопасности, ORCID: 0000-0002-1588-5468, e-mail: pavlychev.av@dvfu.ru
Стародубов Максим Игоревич, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
аспирант, ORCID: 0000-0002-3799-8375, e-mail: starodubov.mi@dvfu.ru
Галимов Александр Дмитриевич, Дальневосточный федеральный университет, 690922, Российская Федерация, г. Владивосток, о. Русский, п. Аякс, 10,
аспирант, ORCID: 0000-0002-5671-1368, e-mail: galimov.ad@dvfu.ru

В статье предлагается способ выявления компьютерных инцидентов, основанный на анализе записей в системных журналах операционной системы Microsoft Windows. Рассматриваются различные технологии обнаружения вредоносного программного обеспечения: технологии сигнатурного обнаружения, технологии эвристического анализа, технологии проактивной защиты и технологии обнаружения системных аномалий. Несмотря на наличие большого разнообразия видов вредоносных программ, все они оставляют следы своей работы в системных журналах различных информационных систем, в том числе операционной системы рабочей станции, подвергшейся несанкционированному воздействию. В работе проведен анализ структуры журналов операционной системы Microsoft Windows с точки зрения выявления событий информационной безопасности. Функционирование любой компьютерной программы, в том числе вредоносной, можно представить в виде уникального набора признаков, которые формируются на основе анализа записей в системных журналах операционной системы. Следовательно, данный набор признаков можно использовать для построения модели функционирования и дальнейшего выявления вредоносного программного обеспечения, в том числе ранее не известного.

Ключевые слова: вредоносное программное обеспечение, компьютерный инцидент, системные журналы Microsoft Windows, набор признаков

FUNCTIONING MODEL OF MALICIOUS SOFTWARE BASED ON ANALYSIS OF SYSTEM LOGS MICROSOFT WINDOWS OPERATING SYSTEM

The article was received by the editorial board on 25.10.2022, in the final version – 26.10.2022.

Pavlychev Aleksey V., Far Eastern Federal University, 10 Ajax, isl. Russkiy, Vladivostok, 690922, Russian Federation,
Director of Cybersecurity Center, ORCID: 0000-0002-1588-5468, e-mail: pavlychev.av@dvfu.ru
Starodubov Maksim I., Far Eastern Federal University, 10 Ajax, isl. Russkiy, Vladivostok, 690922, Russian Federation,
postgraduate student, ORCID: 0000-0002-3799-8375, e-mail: starodubov.mi@dvfu.ru
Galimov Alexander D., Far Eastern Federal University, 10 Ajax, isl. Russkiy, Vladivostok, 690922, Russian Federation,
postgraduate student, ORCID: 0000-0002-5671-1368, e-mail: galimov.ad@dvfu.ru

This article suggests a method for identifying computer incidents is proposed, based on the analysis of entries in the system logs of the Microsoft Windows operating system. Various technologies for detecting malicious software are considered: signature detection technologies, heuristic analysis technologies, proactive protection technologies and system anomaly detection technologies. Despite the presence of a wide variety of types of malware, they all leave traces of their work in the system logs of various information systems, including the operating system of the workstation,

[1]Исследование проведено при финансовой поддержке Минобрнауки России («Грант ИБ МТУСИ») № 40469-23-2021-К.

which has been exposed to unauthorized influence. The paper analyzes the structure of the logs of the Microsoft Windows operating system from the point of view of identifying information security events. The functioning of any computer program, including malware, can be represented as a unique set of features that are formed on the basis of the analysis of entries in the system logs of the operating system. Therefore, this set of features can be used to build a model of functioning and further identify malicious software, including previously unknown ones.

Keywords: malicious software, computer incident, Microsoft Windows system logs, a set of features

Введение. Современные геополитические вызовы диктуют новые требования к киберустойчивости цифровых сервисов, предназначенных для полноценного обеспечения интересов личности, общества и государства.

Складывающаяся политическая обстановка говорит о дальнейшем росте хакерских атак на российскую информационную инфраструктуру с использованием новых видов кибероружия [1, 2].

Указанные обстоятельства свидетельствуют о высокой актуальности исследований, направленных на выявление компьютерных инцидентов с использованием вредоносного программного обеспечения.

В целях поиска нового эффективного способа выявления компьютерных инцидентов в рамках работы авторами поставлен ряд задач:

1. Обзор существующих технологий обнаружения вредоносного ПО.
2. Исследование структуры и содержания системных журналов операционной системы с точки зрения информационной безопасности.
3. Построение модели функционирования вредоносного программного обеспечения, основанной на результатах проведенного эксперимента.
4. Применение разработанной модели для выявления признаков компьютерных инцидентов.

Технологии обнаружения вредоносного программного обеспечения. Вредоносное программное обеспечение – широкое понятие, обозначающее часть программного кода, программного средства или специальный модуль, сознательно созданную в целях нанесения ущерба компьютерной системе, перехвата информации, проникновения в систему получения полного или частичного контроля над системой.

Согласно статье 273 Уголовного кодекса Российской Федерации, вредоносным программным обеспечением считается программное обеспечение, заведомо предназначенное для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Существует большое количество технологий обнаружения вредоносного ПО: технологии сигнатурного обнаружения, технологии эвристического анализа, технологии проактивной защиты и технологии обнаружения системных аномалий. Чем сложнее технология обнаружения, тем больше вероятность обнаружения ранее неизвестных вредоносных объектов [3, 4].

В настоящее время исследователями вредоносного ПО выделяются следующие основные технологии обнаружения:

1. Технология обнаружения по сигнатурам.

Одной из первых технологий обнаружения вредоносного программного кода стал сигнатурный метод – метод распознавания участков кода, позволяющих однозначно установить вредоносную программу. В данном случае антивирусная программа во время сканирования файла обращается к уже известному словарю антивирусных программ [5].

Данный метод имеет ряд важных преимуществ: точность обнаружения вредоносного кода достаточно высока; незначительное количество ложных срабатываний в доле общих срабатываний. Однако он имеет и ряд очень важных недостатков: отсутствует возможность выявления нового вредоносного ПО; невозможность борьбы с полиморфизмом, мутациями кода и другими технологиями сокрытия вредоносного кода; необходимость регулярного обновления антивирусных баз; необходимость ручного наполнения словаря сигнатур.

2. Технология эвристического анализа.

Технология эвристического анализа также является одной из ранних. В своей первой итерации она представляла собой расширение для сигнатурной технологии обнаружения вредоносных объектов. Однако на данный момент она является самостоятельной и более эффективной. Данная технология подразумевает аналитический компонент, работающий на основе принципа нечеткого поиска решения и описываемый событийным языком программирования. Методы эвристического анализа используют в качестве источника информации не только программы, как массивы байт, но и сведения об эмуляции, отчеты «песочниц», сведения, полученные из мониторинга за системой [5].

Данная технология имеет ряд преимуществ: известна уже давно, на практике доказана её эффективность; отсутствует необходимость частых обновлений. Также у неё есть ряд недостатков: требуются значительные вычислительные мощности; недостаточно высокий уровень обнаружения; высокий уровень ложных срабатываний. Указанная технология может применяться на широком

списке устройств: от рабочих станций до интернет-шлюзов. На сегодняшний день данная технология является единственной, которая применяется во всех антивирусных продуктах всех компаний.

3. Системы проактивной защиты.

Технологии проактивной защиты – совокупность технологий, основной целью которых является предотвращение заражения пользовательской системы, а не поиск уже известных вредоносных программ. Продукты, построенные на таких технологиях, можно поделить на системы предотвращения вторжений и системы блокирования по поведению [6].

Системы предотвращения вторжения являются важной компонентой любой системы защиты, они предусматривают возможность обнаружения и блокирования уязвимостей, используемых вредоносными программами. Данная технология эффективно борется с путями распространения сетевых червей, вирусов, а также достаточно эффективно работает против целенаправленных и широких атак пользователей, но имеет крайне низкую эффективность против классических троянских программ, а также требует обновления баз сигнатур атак.

Системы блокирования по поведению существуют на рынке уже более 10 лет. Основная задача таких систем – анализ поведения программ и блокировка выполнения любого возможного опасного действия. Теоретически такие системы могут предотвратить не только распространение известных вредоносных программ, но и неизвестных. Именно в этом направлении и движется развитие практически всех антивирусных продуктов.

Существует три поколения систем блокирования по поведению. В первом поколении таких систем при обнаружении подозрительного действия система блокируется до получения разрешения на выполнение действия от пользователя. Однако такие действия могут выполнять и легальное ПО. Из этого вытекает главный недостаток – необходимость достаточной квалификации пользователя. Системы блокирования по поведению второго поколения имеют лишь одно, но очень весомое отличие от подобных систем первого поколения. Системы этого поколения исследуют события не по отдельности, а исследуются цепочки событий. В результате этого количество запросов к пользователю сильно сокращается, а надежность обнаружения повышается. В системах третьего поколения запросы к пользователю отсутствуют, система обрабатывает все действия автоматически.

Достоинства данной технологии очевидны: высокий уровень обнаружения вредоносного ПО; технология известна достаточно давно и показала свою эффективность; отсутствует необходимость в частых обновлениях; отсутствует привязка к конкретному типу вредоносного программного обеспечения; отсутствует необходимость в большом количестве компьютерных ресурсов. Однако нельзя не отметить и ряд недостатков: высокий процент ложных срабатываний; требуется возможность восстановления системы после частичного исполнения вредоносного кода; повышенный риск безопасности для пользовательской системы, так как используется мониторинг действия с реальной рабочей системы.

Системы блокирования по поведению могут использоваться только в тех случаях, когда возможен запуск и исполнение вредоносного программного кода. В иных случаях вредоносные объекты остаются незамеченными.

4. Системы исследования системных аномалий.

Еще одной важной технологией обнаружения является технология исследования системных аномалий – самый абстрактный метод анализа вредоносного ПО [7]. Она основана на следующих предположениях:

- операционная система является интегральной системой;
- система имеет некоторое «здоровое» (нормальное) состояние;
- после запуска вредоносного кода система переходит в «нездоровое» состояние.

Сравнивая различные состояния системы, можно установить наличие вредоносного кода.

Несмотря на наличие большого разнообразия видов вредоносных программ, все они оставляют следы своей работы в системных журналах различных информационных систем, в том числе операционной системы рабочей станции, подвергшейся несанкционированному воздействию.

Анализ системных журналов операционной системы. Одним из способов выявления компьютерных инцидентов является исследование файлов журналов различных информационных систем, в том числе системных журналов операционной системы на предмет выявления скрытых закономерностей и различных аномалий.

Несмотря на курс России на импортозамещение, в настоящее время операционная система Microsoft Windows установлена на подавляющем большинстве рабочих мест как обычных пользователей, так и в органах власти, предприятиях промышленности, транспорта, обороны, организациях финансового сектора и иных объектах критической информационной инфраструктуры. В операционной системе Microsoft Windows ведутся журналы, которые регистрируют пользовательские события и работу системных и прикладных программ на компьютере.

Для ликвидации последствий компьютерного инцидента специалистам по информационной безопасности или компьютерным криминалистам необходимо отслеживать не только текущее состояние операционной системы, но и состояния, которые предшествовали атаке. Необходимо видеть всю динамику происходящих в операционной системе процессов. Журналы событий Windows хранят в себе информацию обо всех произошедших событиях в операционной системе.

Большинство программного обеспечения, созданного для операционных систем семейства Windows, как и сама операционная система, регистрируют собственные ошибки, сбои, события в собственные журналы событий, и все они имеют отличный друг от друга формат. Ведение же централизованного журнала событий, в который записываются события работы той или иной программы, значительно облегчает работу с журналами, так как не требуется работать одновременно с различными типами регистрации событий. Абсолютно все программные продукты для операционной системы Windows записывают как минимум информацию о запуске программы в журналы событий Windows, а некоторое программное обеспечение записывает также и выход из него.

Журнал системных событий – это механизм, позволяющий фиксировать все события, происходящие в операционной системе, чтобы в случае необходимости специалист по защите информации или администратор мог их просмотреть, проанализировать и выявить причины нештатных ситуаций, возникающих в системе. Журналы событий облегчают отслеживание текущего состояния системы, позволяют проанализировать производительность системы и историю изменений. Они могут предоставить информацию об ошибках и сбоях, произошедших в системе, и определить потенциально опасную деятельность пользователя. Анализ журналов помогает не только определить нештатное поведение программного обеспечения, но и сделать выводы о времени и причинах такого поведения. События операционной системы Windows могут содержать в себе множество различных типов событий, от которых будет зависеть запись в тот или иной журнал событий.

Журнал событий представляет собой бинарный файл специального формата (с расширением EVTX), схожий с файлом базы данных.

Журналы событий Windows содержат ряд дескрипторов, позволяющих объединять события в такие категории, как «информационные» и «критические». Отдельные идентификаторы указывают на конкретные типы событий, а последние версии Windows имеют отдельные файлы журналов событий для различных приложений и служб [8].

Каждый журнал событий содержит заголовок, представленный структурой ELF_LOGFILE_HEADER, используемый в начале журнала событий для определения информации о журнале, имеющий фиксированный размер.

Служба регистрации событий должна добавить ELF_LOGFILE_HEADER в журнал событий.

Структура ELF_LOGFILE_HEADER:

```
EVENTLOGHEADER {
    ULONG HeaderSize;
    ULONG Signature;
    ULONG  MajorVersion;
    ULONG MinorVersion;
    ULONG StartOffset;
    ULONG EndOffset;
    ULONG CurrentRecordNumber;
    ULONG OldestRecordNumber;
    ULONG MaxSize;
    ULONG Flags;
    ULONG Retention;
    ULONG EndHeaderSize;
}
```

где:

HeaderSize – размер структуры заголовка. Размер всегда 0x30.

Signature – подпись всегда 0x654c664c, что является ASCII для журнала событий.

MajorVersion – основной номер версии журнала событий, всегда установлен на 1.

MinorVersion – дополнительный номер версии журнала событий, всегда установлен на 1.

StartOffset – смещение к самой старой записи в журнале событий.

EndOffset – смещение к ELF_EOF_RECORD в журнале событий.

CurrentRecordNumber – номер следующей записи, которая будет добавлена в журнал событий.

OldestRecordNumber – номер самой старой записи в журнале событий. Для пустого файла самый старый номер записи установлен 0.

MaxSize – максимальный размер в байтах журнала событий. Максимальный размер определяется при создании журнала событий. Служба регистрации событий обычно не обновляет это значение, она опирается на конфигурацию реестра. Считыватель журнала событий может использовать обычные файловые API для определения размера файла.

Flags – статус журнала событий.

Retention – значение хранения файла при его создании. Служба регистрации событий обычно не обновляет это значение, она опирается на конфигурацию реестра.

EndHeaderSize – конечный размер структуры заголовка. Размер всегда 0x30.

За заголовком следует переменное число записей событий, представленных структурой EVENTLOGRECORD, содержащей информацию о записи события.

Структура EVENTLOGRECORD:

```
EVENTLOGRECORD {
    DWORD Length;
    DWORD Reserved;
    DWORD RecordNumber;
    DWORD TimeGenerated;
    DWORD TimeWritten;
    DWORD EventID;
    WORD EventType;
    WORD NumStrings;
    WORD EventCategory;
    WORD  ReservedFlags;
    DWORD ClosingRecordNumber;
    DWORD StringOffset;
    DWORD UserSidLength;
    DWORD UserSidOffset;
    DWORD DataLength;
    DWORD DataOffset;
}
```

где:

Length – размер этой записи события в байтах.

Reserved – значение DWORD, которое всегда установлено в ELF_LOG_SIGNATURE.

RecordNumber – номер записи. Это значение можно использовать с флагом EVENTLOG_SEEK_READ в функции ReadEventLog, чтобы начать чтение с указанной записи.

TimeGenerated – время, когда эта запись была представлена. Это время измеряется в количестве секунд, прошедших с 00:00:00 1 января 1970 года, всемирное координированное время.

TimeWritten – время, когда эта запись была получена службой для записи в журнал. Это время измеряется в количестве секунд, прошедших с 00:00:00 1 января 1970 года, всемирное координированное время.

EventID – идентификатор события. Это значение зависит от источника события и используется с именем источника, чтобы найти строку описания в файле сообщений для источника события.

EventType – тип события.

NumStrings – количество строк, присутствующих в журнале. Эти строки объединяются в сообщение перед его отображением для пользователя.

EventCategory – категория для этого события. Значение этого значения зависит от источника события.

UserSidOffset – смещение идентификатора безопасности (SID) в этой записи журнала событий. Чтобы получить имя пользователя для этого SID, используется функция LookupAccountSid.

DataLength – размер специфичных для события данных в байтах.

DataOffset – смещение специфичной для события информации в этой записи журнала событий в байтах.

Заключительной структурой является ELF_EOF_RECORD, содержащая информацию, которая включается после последней записи в журнале событий и используется в журнале событий, чтобы позволить службе регистрации событий реконструировать ELF_LOGFILE_HEADER.

Структура ELF_EOF_HEADER:

```
EVENTLOGEOF {
    ULONG RecordSizeBeginning;
    ULONG One;
    ULONG Two;
    ULONG Three;
```

```
        ULONG Four;
        ULONG BeginRecord;
        ULONG EndRecord;
        ULONG CurrentRecordNumber;
        ULONG OldestRecordNumber;
        ULONG RecordSizeEnd;
    }
```

где:

1. RecordSizeBeginning – начальный размер ELF_EOF_RECORD. Начальный размер всегда 0x28.

2. One – идентификатор, который помогает отличить эту запись от других записей в журнале событий. Значение всегда установлено в 0x11111111.

3. Two – идентификатор, который помогает отличить эту запись от других записей в журнале событий. Значение всегда установлено в 0x22222222.

4. Three – идентификатор, который помогает отличить эту запись от других записей в журнале событий. Значение всегда установлено в 0x33333333.

5. Four – идентификатор, который помогает отличить эту запись от других записей в журнале событий. Значение всегда установлено на 0x44444444.

6. BeginRecord – смещение к самой старой записи. Если журнал событий пуст, это устанавливается в начало этой структуры.

7. EndRecord – смещение к началу этой структуры.

8. CurrentRecordNumber – номер записи следующего события, которое будет записано в журнал событий.

9. OldestRecordNumber – номер самой старой записи в журнале событий. Номер записи будет 0, если журнал событий пуст.

10. RecordSizeEnd – конечный размер ELF_EOF_RECORD всегда 0x28.

11. Если журнал событий пуст, ELF_EOF_RECORD записывается сразу после ELF_LOGFILE_HEADER.

Структура ELF_LOGFILE_HEADER и структура ELF_EOF_RECORD записываются в журнал событий при создании журнала и обновляются каждый раз, когда событие записывается в журнал.

Запись в журнал осуществляется с помощью функции ReportEvent, которая делает запись в конец указанного журнала событий, которая передает параметры службе регистрации событий. Служба регистрации событий использует эту информацию для записи структуры EVENTLOGRECORD в журнал событий.

Синтаксис:

```
BOOL ReportEvent (
    HANDLE hEventLog,
    WORD wType,
    WORD wCategory,
    DWORD dwEventID,
    PSID lpUserSid,
    WORD wNumStrings,
    DWORD dwDataSize,
    LPCSTR lpStrings,
    LPVOID lpRawData
);
```

где:

1. hEventLog – дескриптор журнала событий. Функция RegisterEventSource возвращает этот дескриптор.

2. wType – тип события для регистрации.

3. wCategory – категория события. Это информация об источнике, категория может иметь любое значение.

4. dwEventID – идентификатор события. Идентификатор события указывает запись в файле сообщений, связанную с источником события.

5. lpUserSid – указатель на идентификатор безопасности текущего пользователя. Этот параметр может быть недействителен, если идентификатор безопасности не требуется.

6. wNumStrings – количество строк вставки в массиве, на которое указывает параметр lpStrings. Нулевое значение указывает на отсутствие строк.

7. dwDataSize – количество байтов необработанных (двоичных) данных, специфичных для события, для записи в журнал. Если этот параметр равен нулю, данные для конкретного события отсутствуют.

8. lpStrings – указатель на буфер, содержащий массив строк с нулевым символом в конце, которые объединяются в сообщение до того, как средство просмотра событий отобразит эту строку для пользователя. Этот параметр должен быть допустимым указателем (или NULL), даже если wNumStrings равен нулю. Каждая строка ограничена 31 839 символами.

9. lpRawData – указатель на буфер, содержащий двоичные данные. Этот параметр должен быть допустимым указателем (или NULL), даже если параметр dwDataSize равен нулю.

Запись событий в журналы организована одним из следующих способов:

Non-wrapping. Самая старая запись находится сразу после заголовка журнала событий, а новые записи добавляются после последней добавленной записи (до ELF_EOF_RECORD). Журнал событий не переносится, пока не будет достигнут предел размера журнала событий. Размер журнала событий ограничен либо значением конфигурации MaxSize, либо объемом системных ресурсов.

Wrapping. Записи организованы в виде кольцевого буфера. Самые старые записи заменяются новыми по мере их добавления. Расположение самых старых и новых записей будет различаться. Между ELF_EOF_RECORD и самой старой записью есть некоторое пространство, потому что система сотрет целое число записей, чтобы освободить место для самой новой записи. Например, если самая новая запись имеет длину 100 байт, а две самые старые записи имеют длину 75 байт, система удалит две самые старые записи. Дополнительные 50 байтов будут использованы позже при записи новых значений.

Файл журнала событий имеет фиксированный размер, и когда для записи новых событий в файле не хватает места, то запись разделяется на две записи. Например, если позиция для следующей записи составляет 100 байтов от конца файла, а размер записи составляет 300 байтов, первые 100 байтов будут записаны в конце файла, а следующие 200 байтов будут записаны в начале файла сразу после ELF_LOGFILE_HEADER.

Наибольший интерес для исследователей информационной безопасности представляют следующие журналы операционной системы Windows: Security (Безопасность), System (Система) и Application (Приложение) [9].

Модель функционирования вредоносного программного обеспечения. В работе используется подход, основанный на исследовании изменений, оставляемых вредоносным программным обеспечением в журналах Security, System и Application операционной системы Microsoft Windows.

В связи с этим изучение вредоносных программ ограничивается исполняемыми для представленной операционной системы файлами.

Рассмотрим множество U – множество всех возможных программ:

$$U = \{M_1, \dots, M_k, T_1, \dots, T_m\}, \quad (1)$$

$$n = k + m, \quad (2)$$

где n – количество всех возможных программ; k – количество всех возможных программ, являющихся вредоносным ПО; m – количество всех возможных программ, не являющихся вредоносным ПО.

Пусть множество $Sec = \{Sec_1, \dots, Sec_p\}$, множество булевых функций, где p – количество всех возможных событий, отображаемых в журнале Security.

Каждый элемент множества Sec имеет следующий смысл: функция Sec_i имеет значение 1, тогда и только тогда, когда за время выполнения программы происходило i-е событие из множества Sys, множества всех возможных событий журнала Security.

Пусть множество $Sys = \{Sys_1, \dots, Sys_t\}$, множество булевых функций, где t – количество всех возможных событий, отображаемых в журнале System.

Каждый элемент множества Sys имеет следующий смысл: функция Sys_i имеет значение 1, тогда и только тогда, когда за время выполнения программы происходило i-е событие из множества Sys, множества всех возможных событий журнала System.

Пусть множество $App = \{App_1, \dots, App_s\}$, множество булевых функций, где s – количество всех возможных событий, отображаемых в журнале Application.

Каждый элемент множества App имеет следующий смысл: функция App_i имеет значение 1, тогда и только тогда, когда за время выполнения программы происходило i-е событие из множества App, множества всех возможных событий журнала Application.

Определим любой элемент множества U, множества всех возможных программ как набор следующих векторов.

Каждый элемент U_i из множества U имеет вид:

$$U_i = \{\begin{bmatrix} Sec_{1,i} & Sys_{1,i} & App_{1,i} \\ \cdots & \cdots & \cdots \\ Sec_{p,i} & Sys_{t,i} & App_{s,i} \end{bmatrix}\}, i = \overline{1,n}. \quad (3)$$

Пусть $\varphi(U_i)$: $U_i \to \{0,1\}$ – функционал, обозначающий выполнение программы U_i и приводящий либо к безопасному состоянию системы (0), либо к небезопасному состоянию (1). Определим область вероятностей вредоносного поведения ПО как $V = \{U_i: U_i \in U, P(\varphi(U_i) = 1)\}$.

Исходя из вышеперечисленного, существует множество G (множество всех полезных программ) и множество M (множество всех вредоносных программ).

Определим множества $G = \{T_1, \dots, T_m\}$ и $M = \{M_1, \dots, M_k\}$.

Элемент $U_i \in U$ является элементом множества M тогда и только тогда, когда $U_i \in V$.

Элемент $U_i \in U$является элементом множества G тогда и только тогда, когда $U_i \notin V$ не является элементом области V.

Таким образом, на основе проведенного анализа системных журналов операционной системы Windows функционирование любой программы, как вредоносной, так и легитимной, можно представить в виде следующего набора признаков, соответствующих наступлению определенного события в журналах Security, System и Application.

В рамках проведенного эксперимента установлено, что набор признаков уникален для каждого исследуемого приложения. Таким образом, специалистам по расследованию компьютерных инцидентов необходимо выявлять наборы значений в системных журналах, характерные для работы вредоносного программного обеспечения.

Применение разработанной модели. На специально подготовленной инфраструктуре проведена эксплуатация ряда популярных в хакерской среде уязвимостей операционной системы Microsoft Windows [10]. После успешного применения вредоносного программного обеспечения осуществлен сбор и анализ записей журналов Security (рис. 1), System (рис. 2) и Application (рис. 3) скомпрометированных рабочих станций.

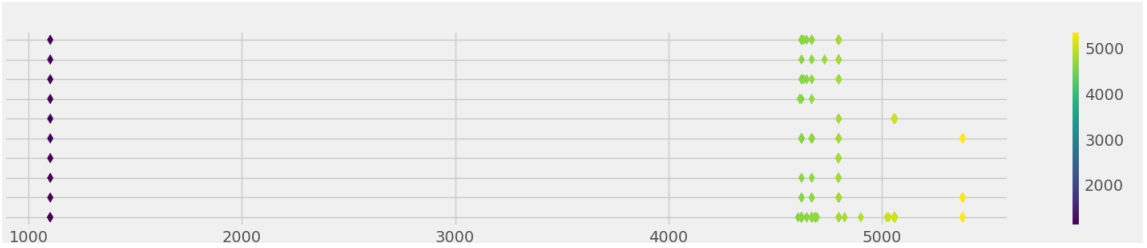


Рисунок 1 – Сравнительный анализ наборов записей в журналах Security

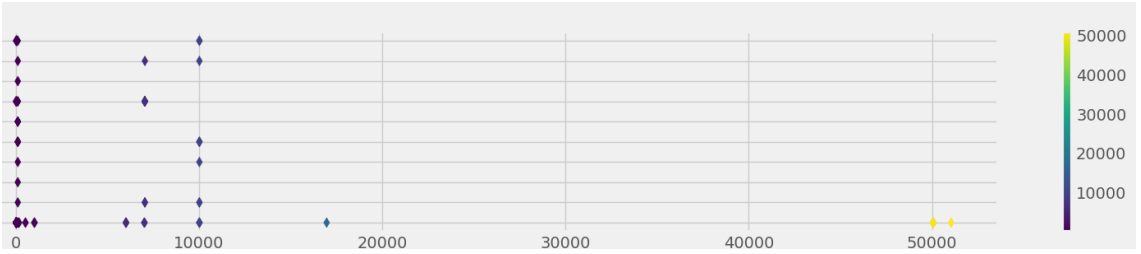


Рисунок 2 – Сравнительный анализ наборов записей в журналах System

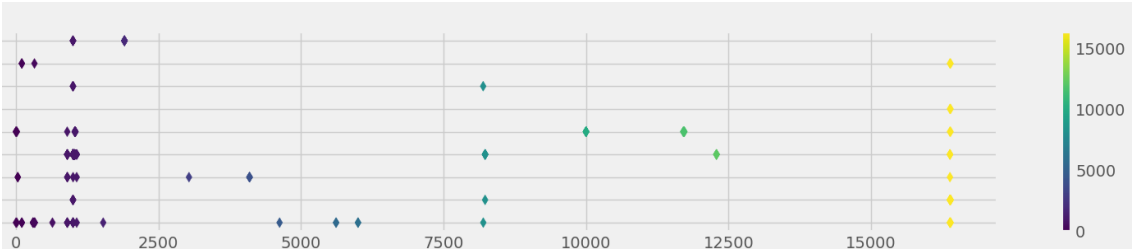


Рисунок 3 – Сравнительный анализ наборов записей в журналах Application

Установлено, что каждый эксплойт оставил уникальный набор записей в системных журналах, что имеет важное значение с точки зрения выявления компьютерных инцидентов.

Заключение. В рамках исследования авторами проведен обзор существующих технологий обнаружения вредоносного программного обеспечения, исследована структура и содержание системных журналов операционной системы с точки зрения информационной безопасности, построена модель функционирования вредоносного программного обеспечения. С использованием Банка данных угроз ФСТЭК России выбраны наиболее распространенные уязвимости для операционной системы Windows и проведена их эксплуатация. По результатам эксперимента проведен анализ на предмет оставления следов эксплойтов в системных журналах информационной системы, подвергшейся несанкционированному воздействию. Доказано, что каждый рассмотренный вид вредоносного программного обеспечения формирует уникальный набор записей в журналах.

Все задачи, поставленные в рамках работы, достигнуты. Предложенный способ выявления компьютерных инцидентов, основанный на анализе записей системных журналов операционной системы, может быть положен в основу дальнейших исследований с целью выявления набора признаков, характерных для различного вида вредоносных программ.

Библиографический список

1. Атаки на российские компании во 2-м квартале 2022 года. – Режим доступа: https://rt-solar.ru /analytics/reports/2880/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 02.09.2022).

2. Dutta, N. Cyber Security: Issues and Current Trends / N. Dutta, N. Jadav, S. Tanwar. – Springer, 2021. – P. 129–141.

3. Badhwar, R. The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms / R. Badhwar. – Springer, 2021. – P. 279–285.

4. Rabaiotti, J. Counter Intrusion Software: Malware Detection using Process Behaviour Classification and Machine Learning / J. Rabaiotti. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.2417&rep=rep1&type=pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 10.09.2022).

5. Campion, M. Learning metamorphic malware signatures from samples / M. Campion // Journal of Computer Virology and Hacking Techniques. – 2021. – Vol. 17. – P. 1–17.

6. Li, N. A Survey on Feature Extraction Methods of Heuristic Malware Detection / N. Li, Z. Zhang, X. Che // Journal of Physics Conference Series. – 2021 – P. 1757–1765.

7. Albanese, M. Industrial Control Systems Security and Resiliency / M. Albanese, S. Jajodia. – Springer, 2019. – P. 169–202.

8. Павлычев, А. В. Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения / А. В. Павлычев, К. С. Солдатов, В. А. Сказин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24, № 4. – С. 27–32.

9. Windows Events. – Режим доступа: https://docs.microsoft.com/en-us/windows/win32/events/windows-events, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 02.08.2022).

10. Банк данных угроз безопасности информации. – Режим доступа: https://bdu.fstec.ru/vul, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.09.2022).

References

1. *Ataki na rossiyskuyu kompaniyu vo 2-m kvartale 2022 goda* [Attacks on Russian companies in the 2nd quarter of 2022]. Available at: https://rt-solar.ru/analytics/reports/2880/ (accessed 02.09.2022).

2. Dutta, N., Jadav, N., Tanwar, S. *Cyber Security: Issues and Current Trends*. Springer, 2021, pp. 129–141.

3. Badhwar, R. *The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms*. Springer, 2021, pp. 279–285.

4. Rabaiotti, J. *Counter Intrusion Software: Malware Detection using Process Behaviour Classification and Machine Learning*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.2417&rep=rep1&type=pdf, (accessed 10.09.2022).

5. Campion, M. Learning metamorphic malware signatures from samples. *Journal of Computer Virology and Hacking Techniques*, 2021, vol. 17, pp. 1–17.

6. Li, N., Zhang, Z., Che, X. A Survey on Feature Extraction Methods of Heuristic Malware Detection. *Journal of Physics Conference Series*, 2021, pp. 1757–1765.

7. Albanese, M., Jajodia, S. *Industrial Control Systems Security and Resiliency*. Springer, 2019, pp. 169–202.

8. Pavlychev, A. V., Soldatov, K. S., Skazin, V. A. Vyyavleniye setevykh anomaliy v sistemnykh zhurnalakh operatsionnoy sistemy Microsoft Windows s ispolzovaniyem metodov mashinnogo obucheniya [Detection of network anomalies in the system logs of the Microsoft Windows operating system using machine learning methods]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [(Reports of the Tomsk State University of Control Systems and Radioelectronics], 2021, vol. 4 (24), pp. 27–32.

9. *Windows Events*. Available at: https://docs.microsoft.com/en-us/windows/win32/events/windows-events (accessed 08.02.2022).

10. *Bank dannykh ugroz bezopasnosti informatsii* [Data bank of information security threats]. Available at: https://bdu.fstec.ru/vul (accessed 20.09.2022).

DOI 10.54398/20741707_2022_4_107
УДК 004.056

МОДЕЛЬ И АЛГОРИТМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ С УЧЕТОМ ТРЕБОВАНИЙ УПРАВЛЕНИЯ НА ОСНОВЕ ДАННЫХ[1]

Статья поступила в редакцию 26.10.2022, в окончательном варианте – 26.10.2022.

Золотарев Вячеслав Владимирович, Сибирский государственный университет науки и технологий, 660037, Российская Федерация, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31,

кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

Лапина Мария Анатольевна, Северо-Кавказский федеральный университет, 355017, г. Ставрополь, ул. Пушкина, 1,

кандидат физико-математических наук, доцент, заместитель директора по международной деятельности, заведующий базовой кафедры комплексного обеспечения информационной безопасности автоматизированных систем Института цифрового развития, ORCID: 0000-0001-8117-9142, e-mail: mlapina@ncfu.ru

В современных подходах к управлению информационной безопасностью внимание разработчиков акцентировано на инфраструктурных и организационных элементах. Особенно это характерно для организаций, формирующих основное содержание управленческих процессов не через технические и программно-аппаратные возможности, например, автоматизацию, а через организационные элементы: регламенты, политики, требования. Вместе с тем для управления информационной безопасностью существенно учитывать и другие элементы, которые могут быть объектами воздействия мер защиты: базы данных и базы знаний, процессы, контролирующие их жизненный цикл, а также персонал, задействованный этими процессами. В работе описаны модель и алгоритм управления информационной безопасностью с учетом требований информационной безопасности, относящихся к собираемым и используемым данным. Схема, предложенная в работе, может быть использована как для имитационных моделей, так и для реализации в виде набора процессов управления информационной безопасностью в практических задачах.

Ключевые слова: управление информационной безопасностью, процессный подход, алгоритм управления безопасностью, образовательный процесс, информационная инфраструктура, управление на основе данных

THE INFORMATION SECURITY MANAGEMENT MODEL AND ALGORITHM WITH REQUIREMENTS OF DATA MANAGEMENT FOR EDUCATIONAL ORGANIZATION OF HIGHER EDUCATION

The article was received by the editorial board on 26.10.2022, in the final version – 26.10.2020.

Zolotarev Vyacheslav V., Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, Head of Information Technologies Security Department, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

Lapina Maria A., North Caucasus Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

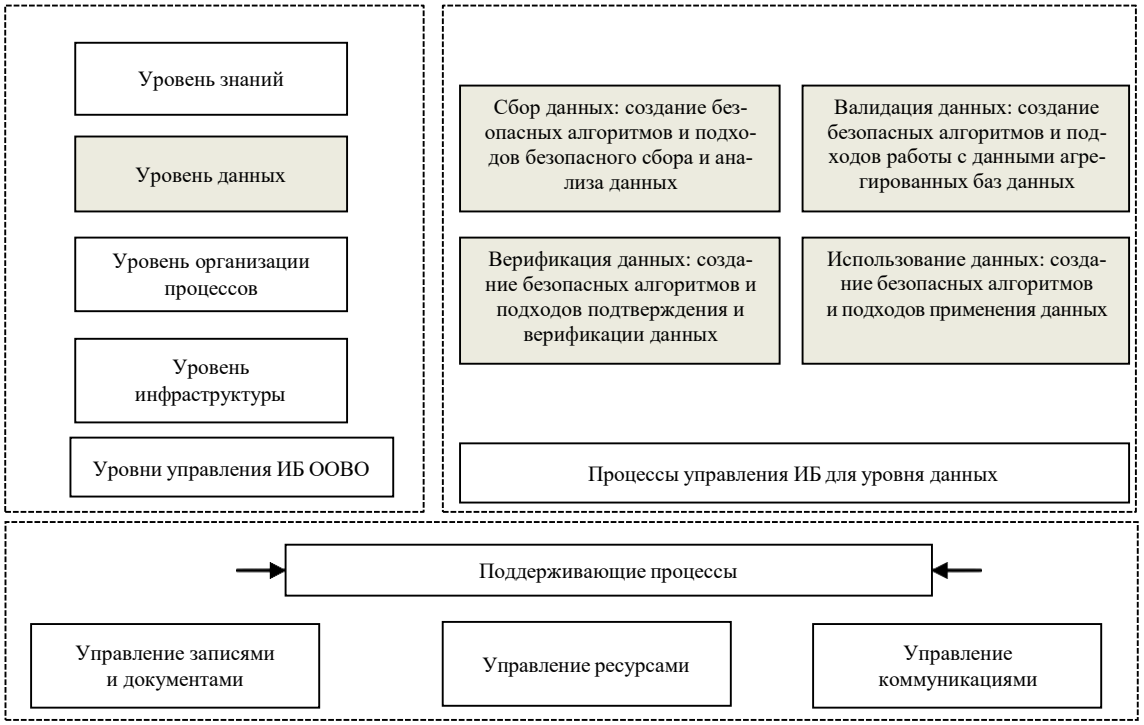
Cand. Sci. (Physics and Mathematics), Associate Professor, Deputy Director for International Activities, Head of the Basic Department of Integrated Information Security of Automated Systems of the Institute for Digital Development, ORCID: 0000-0001-8117-9142, e-mail: mlapina@ncfu.ru

In modern approaches to information security management, the attention of developers is focused on infrastructure and organizational elements. This is especially true for organizations that form the main content of management processes not through technical and hardware-software capabilities, for example, automation, but through organizational elements: regulations, policies, requirements. At the same time, for information security management, it is essential to take into account other elements that may be affected by security measures: databases and knowledge bases, processes that control their life cycle, as well as personnel involved in these processes. The paper describes the model and algorithm of information security management, taking into account the requirements of information security related to the collected and used data. The scheme proposed in the paper can be used both for simulation models and for implementation as a set of information security management processes in practical tasks.

Keywords: information security management, process approach, security management algorithm, educational process, information infrastructure, data-based management

[1]Исследование выполнено при финансовой поддержке Минцифры РФ (Грант ИБ). Проект № 40469-01/2022-д.

Graphical annotation (Графическая аннотация)



Введение. Управление информационной безопасностью в образовательных учреждениях высшего образования – сложный многоуровневый процесс, часто недооцениваемый в рамках практической деятельности. Его использование как составляющей принятия управленческих решений требует как глубокого понимания внутренних процессов (бизнес-процессов или, если такой термин представляется университету более приемлемым, технологических процессов), так и сопоставления текущей практической ситуации с развитием теории в области управления информационной безопасностью. К примеру, авторы работы [1] справедливо указывают, что «принятие управленческих решений в университетах становится невозможным без опоры на агрегированные данные, собираемые из ключевых учетных информационных систем вуза. Каким бы ни был уровень автоматизации университета, его базовые процессы взаимодействия «преподаватель – студент», по требованиям федеральных государственных образовательных стандартов, должны происходить в электронной информационно-образовательной среде (ЭИОС)» [1].

Но при этом, очевидно, должны происходить трансформационные изменения как в составе средств защиты информации, так и в лежащей в основе обеспечения информационной безопасности университета модели их применения. Как минимум необходимо отметить следующие моменты:

1. Агрегирование данных предполагает не только создание и использование баз данных, содержащих такие агрегированные данные, но и управление на основе данных как отдельный существенный слой бизнес-процессов, включающих, например, такие критичные для принятия решений, как верификация и валидация данных.

2. Появление слоя управления данными, в свою очередь, должно порождать в том или ином виде (часто вырожденном, редуцированном, но тем не менее) отдельный слой управления знаниями.

Далее будет показано, что на современном уровне развития методической поддержки процесса управления информационной безопасностью ни управлению данными, ни тем более управлению знаниями не уделяется достаточного внимания на уровне управления безопасностью.

Здесь же можно упомянуть проблему управления информационной безопасностью цифровых двойников [2]. Интеграционные процессы в образовании на уровне их создания и использования приводят к тому, что меняются порядок и схема применения результатов их применения, формируются новые устойчивые связи, поддерживающие процессы управления информационной безопасности на уровне как самого цифрового двойника, так и определяющих его функционирование информационных и социально-экономических систем.

Даже задача изменения ландшафта атак с учетом применения цифровых двойников в образовании имеет множество интересных измерений, не говоря уже о ее приложениях к упомянутым выше, но мало рассматриваемым в литературе слоям управления данными и управления знаниями.

Целью исследования, результаты которого приведены ниже, является решение следующей проблемы: возможно ли с учетом установленных ограничений сформулировать и решить в заданное время задачу управления информационной безопасностью с учетом требований к новому слою бизнес-процессов управления данными? Отдельным вопросом является решение указанной задачи в переходных состояниях цифровой трансформации. Пример такого переходного состояния может быть выбран из следующего запроса: «возможно ли развернуть центр ситуационного мониторинга инженерных систем образовательного учреждения, включая в число таких систем как систему контроля управления доступом, так и контрольно-измерительные устройства инженерных систем, с агрегированием данных в единую базу данных университета? Существенным условием является следующее: если развертывание системы защиты информации информационных систем персональных данных университета не завершено?». Даже первое приближение к задаче управления информационной безопасностью при такой постановке сгенерирует множество вопросов для обсуждения, от защиты (и классификации) биометрических данных до управления доступом к единой базе лиц, ответственных за валидацию данных инженерных систем.

Новыми результатами исследования, представленными ниже, стали:

1) формирование четырехуровневой модели управления информационной безопасностью, включающей слой управления данными и слой управления знаниями, для описания процессов управления информационной безопасностью, затрагивающих несколько уровней этой модели;

2) формирование новых устойчивых связей поддерживающих процессов управления информационной безопасностью на уровне отдельных задач с учетом четырехуровневой модели с акцентом на уровень данных.

Процесс управления информационной безопасностью образовательного процесса. В данном исследовании предлагается использовать измеряемые количественные признаки, пригодные для оценки устойчивых связей поддерживающих процессов управления информационной безопасностью. Уровень управления данными будет рассмотрен с использованием требований программ цифровой трансформации, разработанных в университетах в 2021 году.

Каждая из таких моделей, к примеру, должна включать уровень управления данными, что может создать основу для решаемых в настоящем исследовании задач управления информационной безопасностью, и при этом генерирует множественные вариации этой задачи в переходных состояниях, некоторые примеры которых будут рассмотрены ниже.

В целом, для дальнейшего рассмотрения можно учесть следующее. Согласно программе цифровой трансформации, «целевой моделью университета, с позиций цифровой трансформации, является формирование единого цифрового образовательного и научного пространства. При этом глобально университет должен представлять комплекс цифровых возможностей, транслирующих идею цифровой трансформации всем участникам образовательного процесса и заинтересованным сторонам через цифровые сервисы, элементы цифровой среды, инфраструктуру и исследовательские задачи» [3]. Но это, как видно из формулировки, требует пересборки как поддерживающих процессов на уровне самого университета, так и на уровне заинтересованных в участии в таком взаимодействии сторон.

Управление информационной безопасностью, безусловно, часть указанного процесса трансформации. В основе своей это является следствием продолжающейся цифровой трансформации образовательного процесса. Управление информационной безопасностью в целом должно генерировать базовые процессы, применимые в задаче, такие как [2]:

- управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа;
- реализация процедур и сценариев обеспечения непрерывности образовательного контента, включая сценарии нарушения работоспособности при развертывании виртуальных стендов и контроля целостности цифровых двойников рабочих программ дисциплин;
- обучающие сценарии и сценарии оповещения при администрировании организационной и технической части образовательного процесса, в том числе и обучение действиям на основе стресс-тестов;
- управление уязвимостями используемого программного обеспечения для виртуальных лабораторий и виртуальной инфраструктуры в целом;
- управление рисками, включая правовые и юридические моменты, при формировании и использовании цифровых двойников дисциплин, рабочих программ, лабораторий и программных (программно-аппаратных) средств защиты информации (в рамках рассматриваемой проблематики); для иных областей образования – программных (программно-аппаратных) средств, используемых для формирования образовательного контента цифрового двойника дисциплины;
- управление инцидентами;

– целостное и непрерывное управление изменениями образовательного контента и цифровых двойников, включая процедуры синхронизации.

Далее будет показан план развертывания поддерживающих процессов в различных моделях управления информационной безопасностью.

К примеру, авторы работы [4], акцентируя внимание на управляющих системах индустриального типа, изучают отличия подхода к построению систем управления информационной безопасностью промышленных систем от стандартного подхода как на уровне свойств безопасности, так и на уровне стандартных требований. Интересным в плане настоящего исследования в упомянутой работе является отслеживание типового информационного потока и сопоставление различных требований безопасности по областям их применения.

В исследовании [5] проводится анализ стандартов безопасности для улучшения их управления информационной безопасностью. Дедуктивный метод был применен для обзора и анализа соответствующих стандартов для государственных учреждений. В результате была получена информация о различных политиках безопасности, стандартах и руководствах, которые применяются национальными и международными общественными организациями. Приведена схема мероприятий по принятию стандартов для организаций, модель управления информационной безопасностью, основанная на стандартах и матрица управления информационной безопасностью, на основе которой был рассчитан процент снижения риска. Получены результаты, что поддержание высокого уровня безопасности в организациях требует принятия стандартов контроля в разных сферах и взаимодействия различных организационно-иерархических уровней организаций.

Авторы работы [6], формируя модель управления информационной безопасностью, сосредоточились на оптимизационной задаче, отталкиваясь от ограниченности ресурсов. Подход авторов статьи заключается в возможности многоуровневой (отличающейся по сложности и ресурсоемкости) системы защиты и риск-ориентированном порядке действий.

В статье [7] изучаются требования к сервис-ориентированным платформам с позиций управления безопасностью. Для информационных систем образовательных учреждений это имеет значение с позиций изучения управляющих механизмов безопасности центрального ядра электронно-информационной образовательной среды и развернутой в ней цифровых сервисов.

В диссертационной работе [8] показано, каким образом возможно учесть для управляющих механизмов безопасности информационной среды дестабилизирующие факторы в условиях неопределенности, что может быть применено и для переходных состояний различного типа, и для ситуаций (сценариев) с неполной информацией. Авторы [9] же сосредоточились на задачах оценки зрелости организаций (и организационных структур).

Даже краткие обзоры работ показывают, что, к примеру, нормой при развертывании системы управления информационной безопасностью является конфликт интересов, дублирование задач, снижение эффективности использования ресурсов [10], а учет движения данных и задач работы с ними, не говоря уже о более абстрактных уровнях приложения управляющих воздействий, остается в тени инфраструктурных и организационных задач.

Следовательно, такие модели управления информационной безопасностью, которые могут учитывать и требования к работе с данными, и более высокие уровни абстракции, могут быть востребованы на практике при дальнейшем росте уровня зрелости организаций в области информационной безопасности. Далее авторами и показаны особенности работы с процессами управления информационной безопасности с учетом нового слоя процессов управления данными.

Уровни модели управления информационной безопасностью. Начнем рассмотрение с общей схемы, учитывающей особенности цифровой трансформации ООВО, представленной на рисунке 1. Принципиальные изменения, декларируемые в ней, следующие:

1. Появляется отдельный класс систем управления на основе данных, которые необходимо использовать в работе.

2. Появляются множественные информационные потоки, ранее не представленные (или представленные фрагментарно) в системах управления ООВО.

Управления знаниями здесь нет, но создаются предпосылки для массового использования одной или нескольких агрегированных баз данных, что генерирует задачи управления информационной безопасностью как самих этих баз, так и доступом к ним. Вернемся к этим задачам позже.

Рисунок 1 – Схема функционирования университета по завершению цифровой трансформации (КЦЭ – компетенции цифровой экономики; ОП – образовательный процесс)

Если же рассмотреть схему управления ООВО на примере отдельных процессов, то можно выделить 6–8 процессов, наиболее интересных с позиции выстраивания новой схемы управления информационной безопасностью (рис. 2).

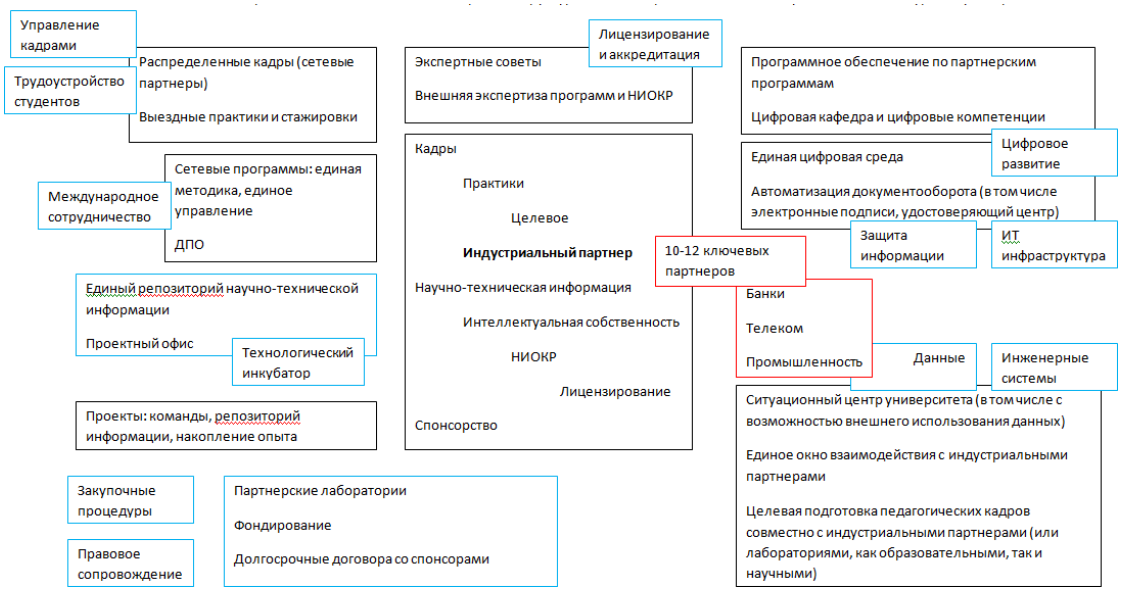


Рисунок 2 – Схема управления ООВО на примере отдельных процессов

Такими процессами, интересными с позиции управления информационной безопасностью на уровне управления данными, с учетом приведенной схемы могут быть:

1. Работа с данными образовательного процесса и исследовательских задач.
2. Сбор и анализ данных инженерных систем.
3. Сбор и анализ данных закупочных процедур (с учетом возможности внешнего доступа к ним).

4. Сбор и анализ данных правового сопровождения базовых процессов ООВО (с учетом возможности внешнего доступа к ним).

5. Работа с агрегированными базами данных студентов, выпускников и сотрудников.

6. Функционирование ситуационного центра (ситуационных центров) и центров поддержки принятия решений.

Даже на приведенной схеме видно несколько моментов, возникающих на уровне управления информационной безопасностью агрегированных баз данных, а именно:

1. Можно ли гарантировать, что управление доступом к различным элементам баз данных со стороны взаимодействующих сторон не приведет к нарушению требований информационной безопасности, (хотя бы) определенных законодательно?

2. Можно ли гарантировать, что агрегирование, верификация и валидация данных не приведет, прямо или косвенно, к возможности нарушения их конфиденциальности и/или целостности, что, в свою очередь, нарушит процессы управления ООВО или ее партнеров?

3. Можно ли сформировать единые требования к управлению информационной безопасностью с учетом элементов, указанных выше на схеме, не нарушая требований, определенных нормативно, но при этом не нарушая работоспособности управленческих процессов?

Рассмотрим общую модель управления информационной безопасностью образовательной организации высшего образования с учетом требований управления данными на схеме ниже (рис. 3).

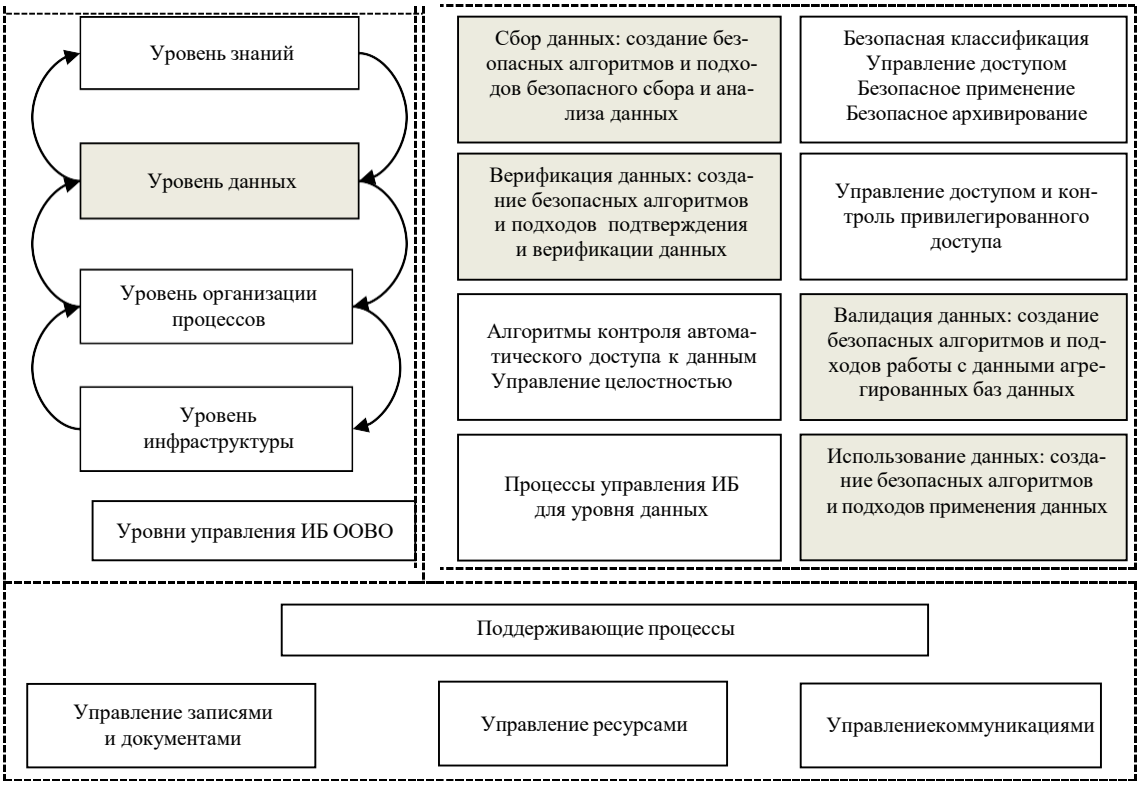


Рисунок 3 – Модель управления информационной безопасностью образовательной организации высшего образования с учетом требований управления данными

Итак, в данном случае требования к управлению данными должны быть дополнены требованиями управления информационной безопасностью для агрегированных баз, используемых для принятия решений. Далее на основе современного стандарта [11], регламентирующего практические правила управления информационной безопасностью, показаны применимые (и недостающие) процессы управления ИБ (табл. 1).

Акцентирование внимание на четырех основных процессах – сбора, валидации, верификации и использования данных позволяет как использование принципа, который можно сформулировать так: все данные, собираемые внутри систем и процессов ООВО, должны быть доступны для использования в любых процессах, в которых они могут понадобиться (принцип максимальной полезности), так и особенность самой деятельности по сбору, анализу и использованию данных, которая

предполагает агрегирование, но не обязательно требует централизации (синхронизированные децентрализованные базы данных и некоторые другие решения также применимы). Таким образом, далее описано управление ИБ универсальных процессов уровня управления данными.

Таблица 1 – Применимые (и недостающие) процессы управления ИБ для уровня данных

Процесс	**Назначение**	**Требования**	**Примечание**
Сбор данных	– Назначение ролей и обязанностей по контролю, анализу и технологии безопасного сбора данных – Разделение обязанностей в области безопасного сбора и анализа данных – Минимизация полномочий – Обеспечение информационной безопасности при управлении проектами	– Ограничение доступа к данным (не все данные должны подлежать автоматическому или автоматизированному сбору), ограничение по ролям и обязанностям – Срок хранения и место хранения, а также условия хранения должны быть определены	ГОСТ Р ИСО/МЭК 27002-2021, п. 6.1.1, 6.1.2, 6.1.5 (применимо)
Верификация данных	– Назначение ролей и обязанностей по контролю, анализу и технологии безопасной верификации данных – Разделение обязанностей в области безопасной верификации данных – Минимизация полномочий – Обеспечение информационной безопасности при взаимодействии с органами власти и профессиональными сообществами	– Ограничение доступа к источникам вспомогательных данных для верификации (записям, документам, регистрационным данным) – Ограничение доступа к данным для случая запроса внешних заинтересованных лиц – Ограничение доступа к данным для случая запроса внутренних заинтересованных лиц	ГОСТ Р ИСО/МЭК 27002-2021, п. 6.1.1, 6.1.3, 6.1.4 (применимо)
Валидация данных	– Назначение ролей и обязанностей по контролю, анализу и технологии безопасной валидации данных – Разделение обязанностей в области безопасного анализа данных – Минимизация полномочий	– Ограничение доступа к тестовым и имитационным моделям управления качеством – Ограничение доступа к источникам вспомогательных данных для валидации (записям, документам, регистрационным данным)	ГОСТ Р ИСО/МЭК 27002-2021, п. 6.1.1 (применимо)
Использование данных	– Разделение обязанностей в области безопасного использования данных – Минимизация полномочий – Обеспечение информационной безопасности при взаимодействии с органами власти и профессиональными сообществами	Управление доступом к данным на всех этапах жизненного цикла	ГОСТ Р ИСО/МЭК 27002-2021, п. 6.1.1, 6.1.3, 6.1.4 (применимо)
Общие процессы	– Моделирование бизнес-процессов в области управления ИБ для уровня данных – Реализация политики управления данными в части ИБ – Оценка и контроль защищенности уровня данных модели управления ИБ ООВО – Обеспечение безопасности дистанционной работы с данными – Управление активами, связанными с данными – Управление доступом к данным – Резервное копирование – Управление коммуникациями – Управление тестовыми данными	– Ограничение доступа к данным, используемым для формирования моделей чувствительных бизнес-процессов ООВО – Учет требований при формировании руководящих указаний в части информационной безопасности	ГОСТ Р ИСО/МЭК 27002-2021, п. 5.1, п. 6.2, п.8, п.9, п. 12.3, п. 13, п.14.3, п. 18 (применимо)

Если же рассматривать указанный уровень более подробно, то основными процессами управления информационной безопасностью в данном случае должны быть:

– управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа, основанное на непрерывном мониторинге цифровой среды, в которой развернут образовательный контент. Ценность данных в этом случае будет выше, если помимо непосредственных процедур обращения к данным будут проанализированы с позиций управления информационной безопасностью и регламентированы вспомогательные процедуры, такие как маркировка данных и управление жизненным циклом данных;

– реализация процедур и сценариев обеспечения непрерывности управления на основе данных. Анализ таких процедур и сценариев должен быть непрерывным и базироваться на моделировании бизнес-процессов организации в реальном времени (что требует отдельных усилий по модернизации системы управления организацией и системы менеджмента качества);

– реализация политики управления данными в части информационной безопасности, включая удаление, использование и передачу заинтересованным сторонам различных данных, применимых в процессах и процедурах управления образовательной организации.

Для поддерживающих процессов (рис. 3) в данном случае необходимо реализовать:

– управление записями и регламентами работы с данными в части обеспечения, мониторинга и анализа информационной безопасности;

– управление ресурсами в плане выделения процессорного времени, резервирования каналов передачи данных и оперативной памяти, резервирования времени использования инфраструктуры общего пользования для задач управления на основе данных, управления данными;

– управление коммуникациями в плане формирования протоколов обмена данными цифрового следа, включая их безопасность;

– управления резервированием агрегированных баз данных;

– управления безопасным обменом данными, в том числе в рамках внутренних и внешних процедур взаимодействия;

– управление доступом к источникам вспомогательных данных для задач валидации и верификации, а также различных служебных задач (таких как сбор телеметрии инженерных систем);

– управление активами, связанными с данными.

При этом необходимо учитывать, что работа на уровне управления данными предполагает набор задач по защите информации для агрегированных баз данных организации, а работа на уровне управления на основе данных – задач коммуникации, верификации, валидации данных и принятия решений заинтересованными сторонами.

К примеру, информационные потоки задачи управления данными (табл. 2) для автоматизированных процедур может выглядеть следующим образом

Таблица 2 – Пример информационных потоков

Наименование информационной системы	**Вид данных**	**Экспортируемые данные**	**Импортируемые данные**	**Вид управления данными**
Система дистанционного обучения	Учетные записи пользователей (ФИО, логин, пароль, электронная почта, дополнительные данные, цифровой след)	Количество посещений пользователями сервера в сутки Количество электронных образовательных курсов (ЭОК) по подразделениям Количество студентов и преподавателей	Резервные копии ЭОК Учетные записи сторонних пользователей (участники олимпиад, слушатели курсов)	Автоматизированный

При этом задача управления на основе данных будет предполагать, к примеру, предиктивный анализ образовательного контента на основе известных данных о пользовательской активности и внешних требованиях к составу ЭОК.

Кроме того, надо учитывать, что одной из стратегических задач в рамках цифровой трансформации любой организации, и ООВО в том числе, является максимальное раскрытие данных с целью повышения как осведомленности (прозрачности) относительно принимаемых решений, так и качества принимаемых решений. При этом задача обеспечения раскрытия данных и задача управления

информационной безопасности данных и процедур принятия решения на основе данных не должны вступать в противоречие, что также является одним из аспектов решения поставленной в настоящем исследовании задачи.

Далее рассмотрим обобщенный алгоритм управления информационной безопасностью для образовательной организации высшего образования на уровне данных.

Алгоритм управления информационной безопасностью ООВО на уровне данных и примеры задач в переходных состояниях. Для управления информационной безопасностью ООВО на уровне данных, как указано выше, критично учитывать процедуры сбора, обработки, хранения и использования данных с позиций информационной безопасности. Таким образом, алгоритм может выглядеть следующим образом:

1. Оценка снимаемых параметров различных информационных систем, действий, процессов и процедур, их формата и способа считывания для анализа возможности применения мер защиты информации. На этом уровне интересен формат, способ сбора данных и возможность автоматизированной либо автоматической процедуры работы с ними на любом из этапов.

2. Анализ протоколов обмена данными для получения информации о способе передачи, формате данных и заголовков, служебной информации, промежуточных коммуникационных устройствах. При этом передача данных может быть и неавтоматизированной, что подразумевает также учет диаграммы потоков данных организации, заинтересованных сторон и персонала, задействованного в жизненном цикле данных.

3. Анализ системы управления хранением данных и их обработкой. В большинстве случаев речь будет идти либо о работе с файлами, в том числе большого размера, либо о системе управления базами данных. Соответственно меры по защите информации будут сосредоточены либо на безопасности штатных средств обработки данных, либо на защите учетных записей, привязанных к их обработке. Также допустимо сквозное шифрование. Данные, полученные от пользователей в формате анкетирования и опросов, также должны быть предварительно обработаны для загрузки в базы данных, следовательно, процедуры предобработки также должны быть проанализированы.

4. Анализ порядка доступа к данным (в том числе для процессов валидации, верификации, создания и уничтожения данных). Это может быть значимо как для управления принятием решения с позиций управления информационной безопасностью этого процесса, так и для извлечения и обработки данных. Имеет значение используемая операционная среда, а также возможности штатных средств доступа, такие как резервное копирование и защита информации резервных копий, идентификация и аутентификация, шифрование данных.

Ниже (рис. 4) показана общая схема работы с информационными потоками на основе указанного обобщенного алгоритма.

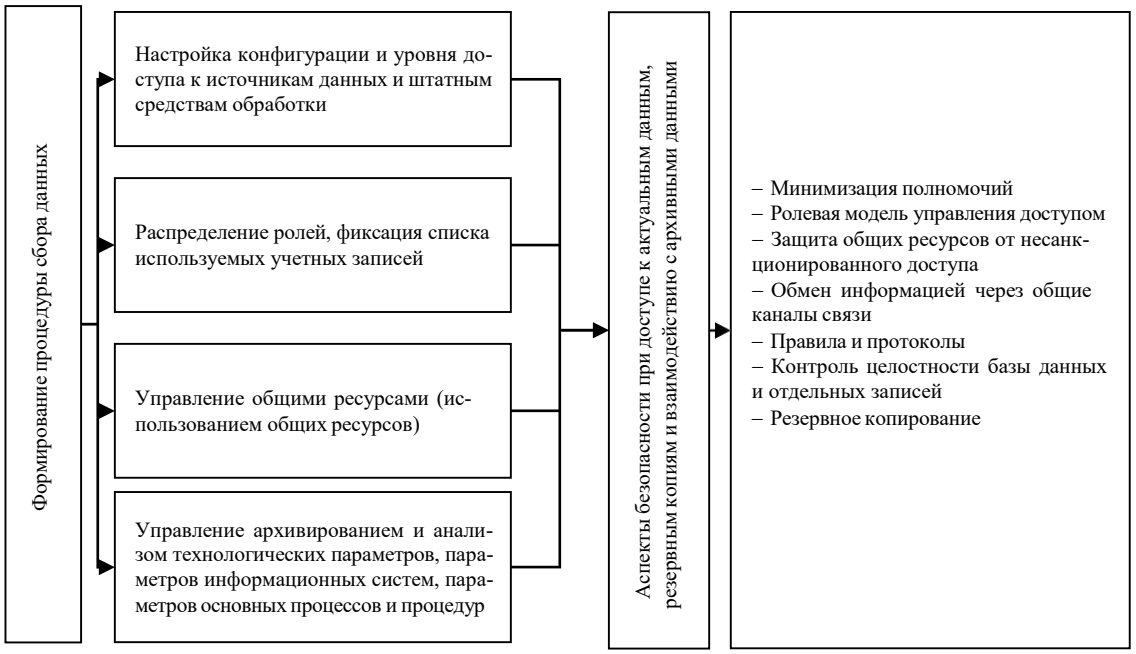


Рисунок 4 – Общая схема работы с информационными потоками

Информационные потоки внутри системы стимулируют внедрение и конкретных мер управления информационной безопасностью на уровне управления на основе данных. Системы управления на основе данных как генерируют собственный контекст мер безопасности (такие как разделение потоков, управление конфиденциальностью выдачи данных или работа с целостностью сообщений источников данных), так и учитывают существующий контекст информационной системы.

Если учитывать показанный выше алгоритм действий и замечание относительно контекста уровня работы с данными, то формируется следующая схема применения конкретных мер защиты данных (рис. 5).

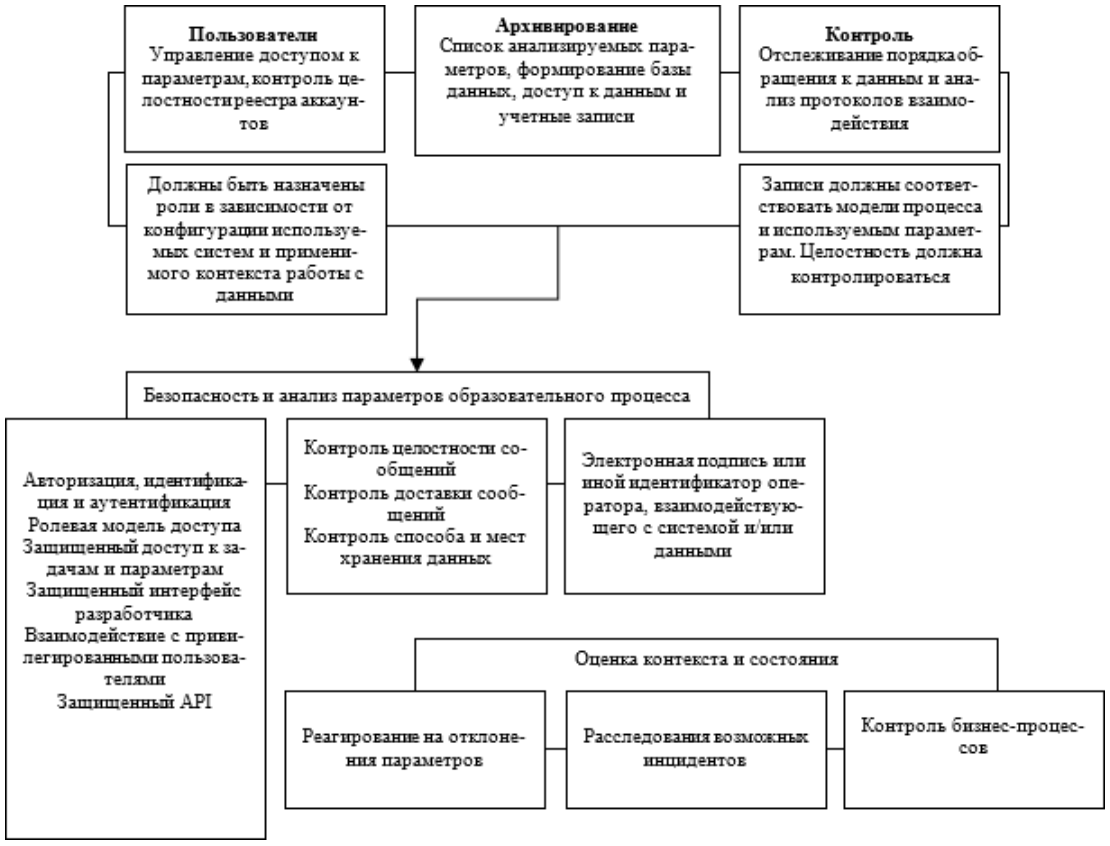


Рисунок 5 – Управление информационной безопасностью при работе с уровнем данных (меры защиты)

При этом нет гарантий, что изменения информационной инфраструктуры и/или организационных процессов не приведут к изменениям в слое данных. На самом деле при функционировании любой информационной системы, и информационные системы рассматриваемого в исследовании типа не исключение, требуется на постоянной основе отслеживать динамику изменений как базовой основы системы, так и контекста ее применения.

Ниже (табл. 3) приводится пример такого переходного состояния, возникающего в процессе изменений системы. Для построения модели перед расчетом переходных состояний целесообразно учитывать контрольные испытания или опыт реализации процессов с учетом времени выполнения; обеспечивать автономность выполнения задач. В частности, возможно заранее предусмотреть дублирование или параллельное выполнение отдельных задач, резервирование ресурсов.

Переходные состояния различного типа, а также уровень знаний как уровень модели информационной безопасности, а также обобщающие требования для различных уровней должны быть рассмотрены отдельно. Тем не менее, исходя из поставленной задачи, для уровня управления данными (и в целом слоя данных) возможно построение такой процессной модели, которая будет учитывать основные требования управления безопасности и вместе с тем расширять понимание изучаемого объекта. Отдельным вопросом является наличие стабильных состояний такой модели (с учетом слоев инфраструктуры, данных и организационных процессов), а также стабильных состояний расширенной, четырехуровневой модели, с учетом дополнительного слоя управления знаниями.

Таблица 3 – Примеры задач управления информационной безопасностью в переходных состояниях системы

Задача	Возможность моделирования времени перехода	Возможность формализации процесса перехода	Возможность привязки к смежным задачам
Внедрение аналитической системы мониторинга и анализа цифровых следов обучающегося, сотрудника, ученого	Подзадачи (пример): расчет времени верификации данных	Подзадачи (пример): моделирование процессов управления требованиями	Подзадачи (пример): управление ИБ при создании цифровых двойников [2]

Заключение. Исследование сосредоточено на формировании пригодных в практике рекомендаций по построению процессной модели управления информационной безопасности, учитывающей как традиционные рассматриваемые уровни управления инфраструктурой информационной системы и управления организационными процессами, так и новые, расширяющие модель уровень-данных, рассмотренный в настоящей работе, и уровень знаний.

Подобное расширение может быть полезно при развертывании разных типов экспертных и советующих систем, систем поддержки принятия решений, ситуационных центров и особенно интересно для задач переходных состояний, которые возможно рассмотреть в отдельных исследованиях.

Библиографический список

1. Кунц, Е. Ю. Использование компетентностной модели образовательной программы для принятия управленческих решений в образовательной организации / Е. Ю. Кунц, П. С. Ложников // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 2. – С. 27–34.

2. Попов, А. М. Проблема управления информационной безопасностью при создании цифрового двойника дисциплины / А. М. Попов, В. В. Золотарев, Е. Ю. Кунц // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 2. – С. 109–118.

3. Стратегия цифровой трансформации Сибирского государственного университета науки и технологий. – Красноярск, 2021. – 117 с.

4. Sanghyun, Park. Advanced Approach to Information Security Management System Model for Industrial Control System / Sanghyun Park and Kyungho Lee // The Scientific World Journal. – 2014. – Vol. 2014, article ID 348305. – 13 p. – http://dx.doi.org/10.1155/2014/348305.

5. Toapanta, Segundo Moisés Toapantaa. Analysis for the adoption of security standards to improve the management of securities in public organizations / Toapanta Segundo Moisés Toapantaa, Ronquillo Madeleine Lilibeth Alvaradob, Gallegos Luis Enrique Maflab, Zezzatti Alberto Ochoac // 2020 International Conference on Machine Learning and Intelligent Systems, MLIS-2020. Frontiers in Artificial Intelligence and Applications. – 2020. – Vol. 332. – P. 310–321. – https://doi.org/10.3233/FAIA200796 MLIS-2020.

6. Фомченкова, Л. В. Модель управления информационной безопасностью / Л. В. Фомченкова, А. В. Леонов // Journal of Economy and Business. – 2019. – Vol. 12–3 (58). – https://doi.org/10.24411/2411-0450-2019-11489.

7. Wilk, J. Information security management model for integration platforms / J. Wilk // 2015 Forth International Conference on e-Technologies and Networks for Development (ICeND). – 2015. – P. 1–6. – https://doi.org /10.1109/ICeND.2015.7328532.

8. Зырянова, Т. Ю. Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов : автореф. дис. … канд. техн. наук по специальности: 05.13.19 – Методы и системы защиты информации / Т. Ю. Зырянова. – Томск, 2008.

9. Osamah, M. M. Al-Matari. Adopting security maturity model to the organizations' capability model / Osamah M. M. Al-Matari, Iman M. A. Helal, Sherif A. Mazen, Sherif Elhennawy // Egyptian Informatics Journal. – 2021. – Vol. 22, issue 2. – P. 193–199. – https://doi.org/10.1016/j.eij.2020.08.001.

10. Офицеров, А. И. Концептуальные основы обеспечения комплексной безопасности критически важных объектов / А. И. Офицеров, О. О. Басов, С. С. Бачурин // Экономика. Информатика. – 2020. – Т. 47, № 1.

11. ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. Information technology. Security techniques. Code of practice for information security controls ОКС 35.030. Дата введения 2021-11-30.

References

1. Kunts, E. Yu., Lozhnikov, P. S. Ispolzovaniye kompetentnostnoy modeli obrazovatelnoy programmy dlya prinyatiya upravlencheskikh resheniy v obrazovatelnoy organizatsii [Using the competence model of an educational program for making managerial decisions in an educational organization]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2022, no. 2, pp. 27–34.

2. Popov, A. M., Zolotarev, V. V., Kunts, E. Yu. Problema upravleniya informatsionnoy bezopasnostyu pri sozdanii tsifrovogo dvoynika distsipliny [The problem of information security management when creating a digital

twin of the discipline]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2022, no. 2, pp. 109–118.

3. *Strategiya tsifrovoy transformatsii Sibirskogo gosudarstvennogo universiteta nauki i tekhnologiy* [Digital Transformation Strategy of the Siberian State University of Science and Technology]. Krasnoyarsk, 2021. 117 p.

4. Sanghyun, Park and Kyungho, Lee. Advanced Approach to Information Security Management System Model for Industrial Control System. *The Scientific World Journal*, 2014, vol. 2014, article ID 348305, 13 p. http://dx.doi.org/10.1155/2014/348305.

5. Toapanta, Segundo Moisés Toapantaa, Ronquillo, Madeleine Lilibeth Alvaradob, Gallegos, Luis Enrique Maflab, Zezzatti, Alberto Ochoac. Analysis for the adoption of security standards to improve the management of securities in public organizations. *2020 International Conference on Machine Learning and Intelligent Systems, MLIS-2020. Frontiers in Artificial Intelligence and Applications*, 2020, vol. 332, pp. 310–321. https://doi.org/10.3233/FAIA200796.

6. Fomchenkova, L. V., Leonov, A. V. Model upravleniya informatsionnoy bezopasnostyu [Information security management model]. *Journal of Economy and Business*, 2019, vol. 12–3 (58). https://doi.org/10.24411/2411-0450-2019-11489.

7. Wilk, J. Information security management model for integration platforms. *2015 Forth International Conference on e-Technologies and Networks for Development (ICeND)*, 2015, pp. 1–6. https://doi.org/10.1109 /ICeND.2015.7328532.

8. Zyryanova, T. Yu. *Model sistemy upravleniya informatsionnoy bezopasnostyu v usloviyakh neopredelennosti vozdeystviya destabiliziruyushchikh faktorov : avtoreferat dissertatsii … kandidata tekhnicheskikh nauk po spetsialnosti: 05.13.19 – Metody i sistemy zashchity informatsii* [Model of the information security management system in conditions of uncertainty of the impact of destabilizing factors : abstract of the dissertation for the degree of Candidate of Technical Sciences in the specialty: 05.13.19 – Methods and systems of information protection]. Tomsk, 2008.

9. Osamah, M. M. Al-Matari, Iman, M.A. Helal, Sherif, A. Mazen, Sherif, Elhennawy. Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal*, 2021, vol. 22, issue 2, pp. 193–199. https://doi.org/10.1016/j.eij.2020.08.001.

10. Ofitserov, A. I., Basov, O. O., Bachurin, S. S. Kontseptualnyye osnovy obespecheniya kompleksnoy bezopasnosti kriticheski vazhnykh obyektov [Conceptual foundations of complex security of critical facilities]. *Ekonomika. Informatika* [Economy. Computer Science], 2020, vol. 47, no. 1.

11. *GOST R ISO/MEK 27002-2021. Natsionalnyy standart Rossiyskoy Federatsii. Informatsionnyye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil primeneniya mer obespecheniya informatsionnoy bezopasnosti* [GOST R ISO/IEC 27002-2021. National Standard of the Russian Federation. Information technology. Methods and means of ensuring security. A set of rules and regulations for the application of information security measures Information technology. Security techniques. Code of practice for information security controls ACS 35.030], date of introduction 2021-11-30.

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

УДК 621.396.93:681.518.3

ИССЛЕДОВАНИЕ МЕТОДОВ СИНХРОНИЗАЦИИ ГЕНЕРАТОРОВ В СПУТНИКОВЫХ СИСТЕМАХ

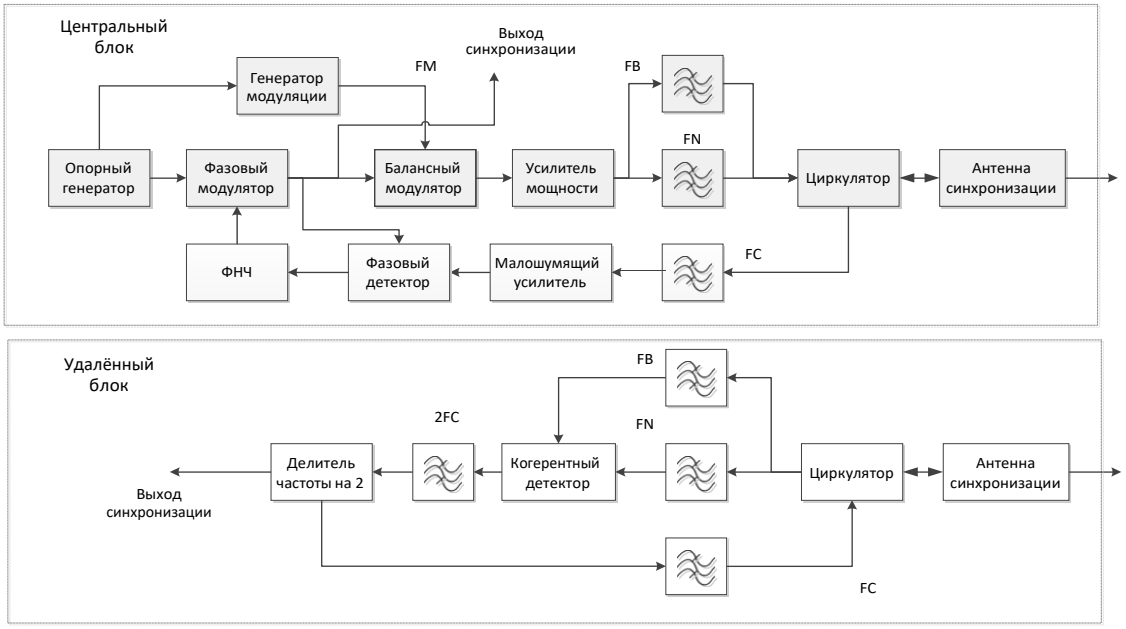
Статья поступила в редакцию 12.09.2022, в окончательном варианте – 20.09.2022.

Нгуен Суан Чыонг, Тульский государственный университет, 300012, Российская Федерация, г. Тула, проспект Ленина, 92,
аспирант, ORCID: 0000-0001-7880-2351, e-mail: xuantruong19@hotmail.com.vn

В данной работе приводятся результаты исследований методов синхронизации генераторов спутниковых систем радиолокационного мониторинга Земли, которые работают в бистатическом режиме. Автором рассмотрены условия для обеспечения работоспособности системы синхронизации разнесенных генераторов, а также оценено влияние дополнительных факторов на точность измерения фазы, разработана структурная схема фазовой синхронизации с амплитудно-модулированным сигналом. В исследовании автор делает вывод о том, что эффективность работы системы синхронизации будет больше, если использовать трёхчастотную схему, преимущества которой заключаются в повышении развязки сигналов, передаваемых в противоположных направлениях, и обеспечении высокого уровня синхронизации в разнесённых системах при простых алгоритмах обработки сигналов. Отмечается, что существенным недостатком предложенной схемы с сигналами балансной амплитудной модуляции является работа фазового детектора на высокой частоте. В настоящий момент проводятся работы по поиску возможных вариантов устранения данного недостатка.

Ключевые слова: фазовая синхронизация, система мониторинга Земли, методы синхронизации

Графическая аннотация (Graphical annotation)



RESEARCH OF SYNCHRONIZATION METHODS FOR GENERATORS IN SATELLITE SYSTEMS

The article was received by the editorial board on 12.09.2022, in the final version – 20.09.2022.

Nguyen Xuan Truong, Tula State University, 92 Lenin Ave., Tula, 300012, Russian Federation, post-graduate student, ORCID: 0000-0001-7880-2351, e-mail: xuantruong19@hotmail.com.vn

This paper presents the results of the research on the synchronization method of satellite systems for Earth radar monitoring operating in the bistatic mode. The conditions for ensuring the operability of a synchronization system for spaced generators are considered, the influence of additional factors on the accuracy of phase measurement is estimated, a block diagram of phase synchronization with amplitude modulated signals has been developed. In the study, the author concludes that the efficiency of the synchronization system will be greater if a three-frequency scheme is used, the advantages of which are to increase the isolation of signals transmitted in opposite directions and provide a high level of synchronization in diversity systems with simple signal processing algorithms. It is noted that a significant drawback of the proposed scheme with the BAM signal is the operation of the phase detector at a high frequency. Currently, work is underway to find possible ways to eliminate this shortcoming.

Keywords: phase synchronization, Earth monitoring system, synchronization methods

Введение. Особенностью модуля синхронизации космических аппаратов (КА) информационно-измерительных и управляющих систем космического мониторинга земной поверхности являются большие расстояния между ними и непрерывное измерение положения в пространстве, что обусловливает необходимость использования широких (сферических) диаграмм направленности антенн, приводящих к значительному ослаблению сигналов при распространении. Эта особенность систем синхронизации недостаточно исследована учеными [7–10].

В статье приведены результаты оценки фазовых ошибок в системе синхронизации с учётом изменения уровня сигнала от расстояния между космическими аппаратами, что позволяет оценить характеристики выбранного метода синхронизации и выбрать оптимальные параметры системы.

Анализ характеристик существующих методов синхронизации. При использовании одночастотной синхронизации (схема которой показана на рисунке 1) центральный космический аппарат (ЦКА) непрерывно передаёт гармонический сигнал несущей частоты:

$$U_0(t) = U_{0m}\cos(\omega_0 t + \varphi_0). \quad (1)$$

Удалённый космический аппарат (УКА) принимает сигнал и с помощью системы фазовой автоподстройки частоты подстраивает свой опорный генератор на частоту и фазу ЦКА, а затем передаёт его на центральный КА [5].

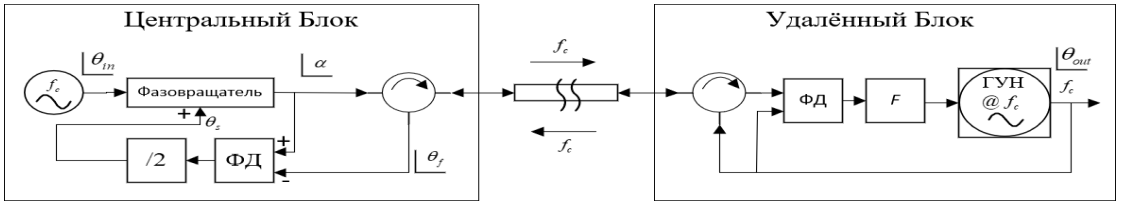


Рисунок 1 – Схема одночастотной фазовой синхронизации: ФД – фазовый детектор; F – фильтр; ГУН – генератор, управляемый напряжением

За время вышеописанного цикла «приём-передача» возможны изменения частоты и фазы опорного генератора ЦКА и изменение фазы при распространении излучения, поэтому на вход приёмника центрального КА поступает сигнал от УКА, а также сигнал, проходящий на вход приёмника через неидеальный ферритовый циркулятор:

$$U_{вх}(t) = U_0 K_c \cos(\omega_0 t + \varphi_0) + U_0 K(R)\cos(\omega_0 t + \varphi_0 + \varphi_y), \quad (2)$$

где K_c – коэффициент передачи опорного сигнала через циркулятор; $K(R)$ – уменьшение амплитуды сигнала при распространении в пространстве на расстоянии R, которое приближённо может быть рассчитано по уравнению идеальной радиопередачи:

$$K(R) = \sqrt{\frac{D_1 D_2 \lambda^2}{16\pi^2 R^2}} e^{-j\beta R}, \quad (3)$$

где D_1, D_2 – коэффициенты направленного действия антенн системы синхронизации ЦКА и УКА; λ – длина волны излучения; β – фазовая постоянная распространения волны; φ_y – фаза опорного сигнала УКА.

Фазовый множитель $e^{-j\beta R}$ зависит от расстояния между ЦКА и УКА и рассчитывается на основе точного определения расстояния между КА, что позволяет в дальнейшем этот фазовый сдвиг не учитывать. Так, например, в системе дистанционного зондирования Земли TerraSar используется прецизионная оптическая система измерения расстояния между КА и дополнительное оптическое измерение расстояния до опорного геостационарного КА с точностью до 1 мм [4].

Сигнал после фазового детектирования в ЦКА определяется следующим выражением:

$$U_{д}(t) = 0{,}5U_0 K_c \sin(2\omega_0 t) + 0{,}5U_0 \sqrt{\frac{D_1 D_2 \lambda^2}{16\pi^2 R^2}} \left[\sin(2\omega_0 t + \varphi_y) - \sin\varphi_y\right]. \quad (4)$$

После фильтрации второй гармоники формируется полезный сигнал:

$$U_{д}(t) = U_0 \sqrt{\frac{D_1 D_2 \lambda^2}{32\pi^2 R^2}} \sin\varphi_y \ . \quad (5)$$

Поскольку при распространении сигнала его амплитуда значительно снижается, необходимо оценить отношение сигнал – шум на выходе детектора.

С учётом тепловых шумов:

$$U_n = \sqrt{\sigma_n^2} = \sqrt{4kT\Delta F}\,, \quad (6)$$

где k – постоянная Больцмана; T – абсолютная температура; ΔF – ширина полосы, отношение сигнал – шум на выходе фазового детектора составит:

$$S/N = \left\lfloor \frac{U_0^2 D_1 D_2 \lambda^2}{128\pi^2 R^2 kT\Delta F} \sin\varphi_y \right\rfloor. \quad (7)$$

На рисунке 2 приведены результаты расчёта зависимости отношения сигнал – шум от расстояния между КА в дБ на выходе фазового детектора одночастотной системы синхронизации гармоническим сигналом.

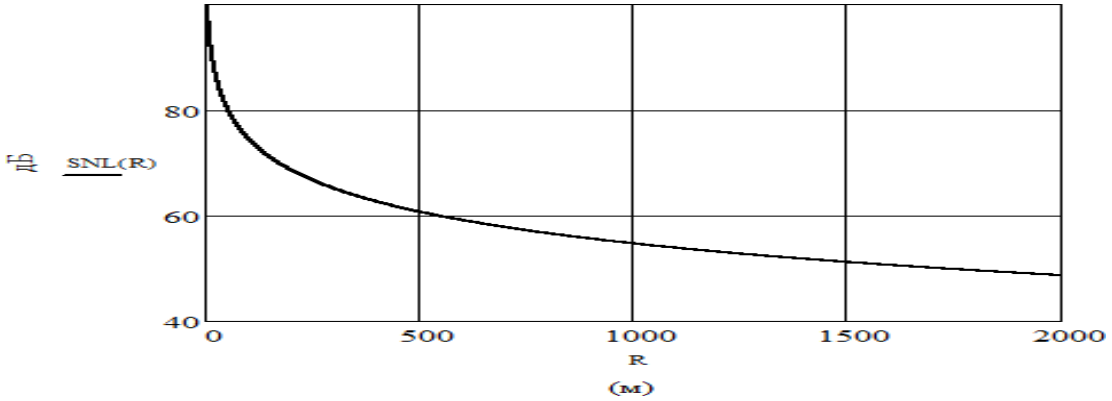


Рисунок 2 – Зависимость отношения сигнал – шум в дБ на выходе фазового детектора одночастотной системы синхронизации от расстояния между КА

Результаты показывают, что из-за необходимости обеспечения широкой диаграммы направленности и сильного уменьшения амплитуды волны при распространении передаваемый сигнал сильно затухает, однако отношение сигнал-шум для внутренних шумов остаётся достаточным для обеспечения малых значений предельной погрешности измерения фазы [1]:

$$\sigma_\varphi^2 = 1/(S/N). \quad (8)$$

Однако на максимальной дальности предельная дисперсия измерения фазы приблизительно равна $\sigma_\varphi^2 = 10^{-5}$, что для среднего квадратичного отклонения (СКО) фазы составляет порядка 0,2 градуса, и максимальная фазовая ошибка может составлять более 0,5 градуса.

Вторым негативным фактором является прохождение на вход приёмника через циркулятор опорного сигнала, который по амплитуде существенно превышает сигнал УКА, причём фазы сигналов в фазовом детекторе и на входе могут отличаться. Это приводит к дополнительной фазовой ошибке, которая может быть оценена из выражения:

$$\Delta\varphi(R) = \varphi - \arctan\left[\frac{K(R)\sin(\varphi)}{K_c\left(1+\frac{K(R)\cos(\varphi)}{K_c}\right)}\right], \quad (9)$$

где φ – фаза сигнала удалённого КА.

На рисунке 3 приведены результаты расчёта данной фазовой ошибки.

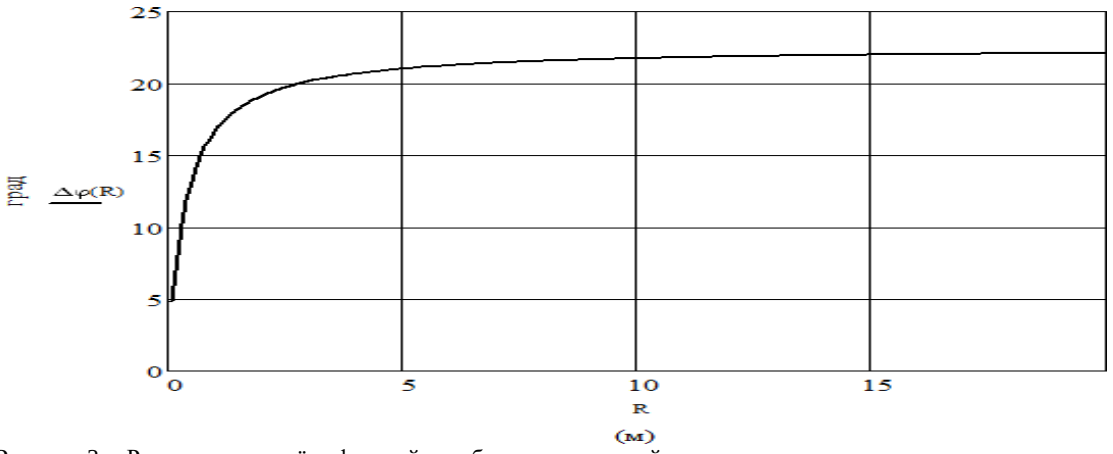


Рисунок 3 – Результаты расчёта фазовой ошибки, возникающей из-за прохождения опорного сигнала через циркулятор

Как видно из рисунка 3, уже на малых расстояниях ошибка становится недопустимой. Всё это показывает непригодность одночастотных систем для синхронизации космических аппаратов.

Если сигнал гармонической помехи имеет случайную фазу, распределённую по равновероятному закону φ_n, то при вычислениях по методике, предложенной в работе В.Б. Пестрякова [5] плотность вероятности отклонения результирующей фазы φ_p от измеряемой будет определяться следующими выражениями:

$$p(\varphi_p) = \frac{\cos(\varphi_p)}{\pi\sqrt{\frac{n}{U_0} - \sin^2(\varphi_p)}}; \quad \frac{U_n}{U_0} < 1; \quad (10)$$

$$p(\varphi_p) = \frac{1}{2\pi} + \frac{\cos(\varphi_p)}{2\pi\sqrt{\frac{n}{U_0} - \sin^2(\varphi_p)}}; \quad \frac{U_n}{U_0} > 1; \quad (11)$$

где U_n – амплитуда помехи; U_0 – амплитуда измеряемого сигнала.

Полученные выражения позволяют рассчитать дисперсию и СКО измерения фазы в этом случае:

$$\sigma_p^2 = \int_{-\pi}^{\pi} \varphi_p^2 p(\varphi_p) d\varphi_p. \quad (12)$$

На рисунке 4 приведены результаты расчёта влияния гармонической помехи со случайной фазой на СКО отклонения фазы при измерениях.

Результаты расчёта показывают, что для получения СКО отклонения фазы при измерениях не более десятых долей градуса относительный уровень сигнала помехи не должен превышать $5 \cdot 10^{-3}$, т.е. соотношение сигнал – помеха (по мощности) требуется более 46 дБ. При сравнимых уровнях сигнала (и тем более, при превышении помехи над сигналом) измерения невозможны.

Проведённое исследование показало, что для обеспечения работоспособности системы синхронизации необходимо обеспечить ортогональность сигналов ЦКА и УКА. Обеспечение ортогональности прямого и обратного сигналов в системе возможно аппаратным методом (используя циркулятор), частотным (при разделении частот прямого и обратного каналов), временным (сигналы передаются в несовпадающие моменты времени), а также поляризационными методами. Поляризационный метод в данном случае неприменим, поскольку ЦКА и УКА перемещаются в пространстве и меняют ориентацию.

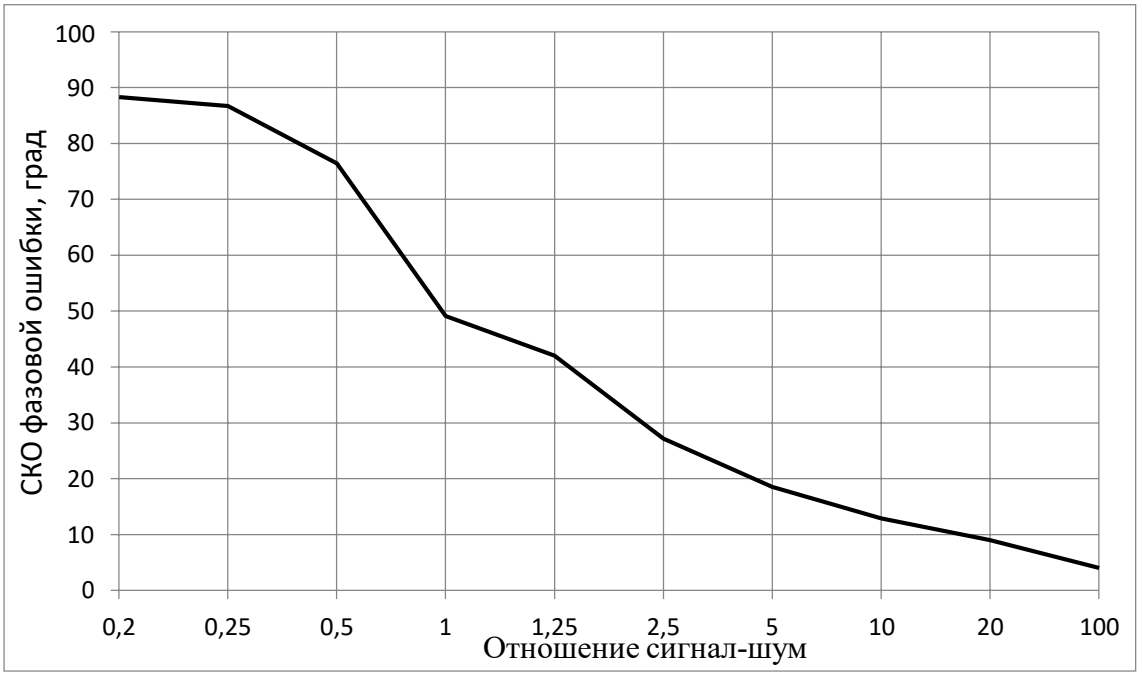


Рисунок 4 – Результаты расчёта влияния гармонической помехи со случайной фазой на СКО отклонения фазы при измерениях

Модернизация двухчастотного метода синхронизации. Простейшим вариантом решения проблемы является использование частотной ортогональности, которая может быть реализована через двухчастотную схему [6, 7]. При использовании двухчастотной схемы используются две различные частоты: одна – для передачи от ЦКА к УКА, вторая – для передачи от УКА к ЦКА. Необходимая развязка каналов обеспечивается линейными частотными фильтрами.

Оценить уровень вносимой фазовой ошибки из-за прохождения опорного сигнала можно по ранее полученному выражению, в котором коэффициент $K_ф$ учитывает дополнительное подавление сигнала частотным фильтром

$$\Delta\varphi(R) = \varphi - \arctan\left[\frac{K(R)\sin(\varphi)}{K_c K_\phi\left(1+\frac{K(R)\cos(\varphi)}{K_c K_\phi}\right)}\right]. \quad (13)$$

При реализации двухчастотных систем возникают проблемы с созданием двухчастотных каналов (прямого и обратного), работающих на различных частотах, но связанных по фазе (когерентных).

Для решения указанной проблемы предлагается модернизация двухчастотного метода, заключающаяся в формировании двух частот для прямого и обратного каналов методом балансной амплитудной модуляции (БАМ):

$$U_{БАМ}(t) = U_0\cos(\omega_0 t + \theta_0)\cos(\omega_m t + \theta_m) = \\ = \frac{U_0}{2}\cos\left[(\omega_0 + \omega_m)t + \theta_0 + \theta_m\right] + \frac{U_0}{2}\cos\left[(\omega_0 - \omega_m)t + \theta_0 - \theta_m\right], \quad (14)$$

где ω_0 – несущая частота; ω_m – частота модуляции; θ_0 ,θ_m – фазы соответственно несущей и модулирующей частот.

Предлагаемый метод уже подробно описан автором настоящей статьи в работе, посвященной схеме синхронизации с амплитудно-модулированным сигналом для распределенных генераторов в спутниковых системах [2, 3], и отличается простотой реализации и контролируемостью сдвига их фаз. Частота модуляции определяется возможностью получения требуемого подавления второго канала и может выбираться (в зависимости от несущей) от единиц до десятков мегагерц.

Разработка структурной схемы системы синхронизации с БАМ-сигналом. На рисунке 5 представлена структурная схема системы фазовой синхронизации с БАМ-сигналом.

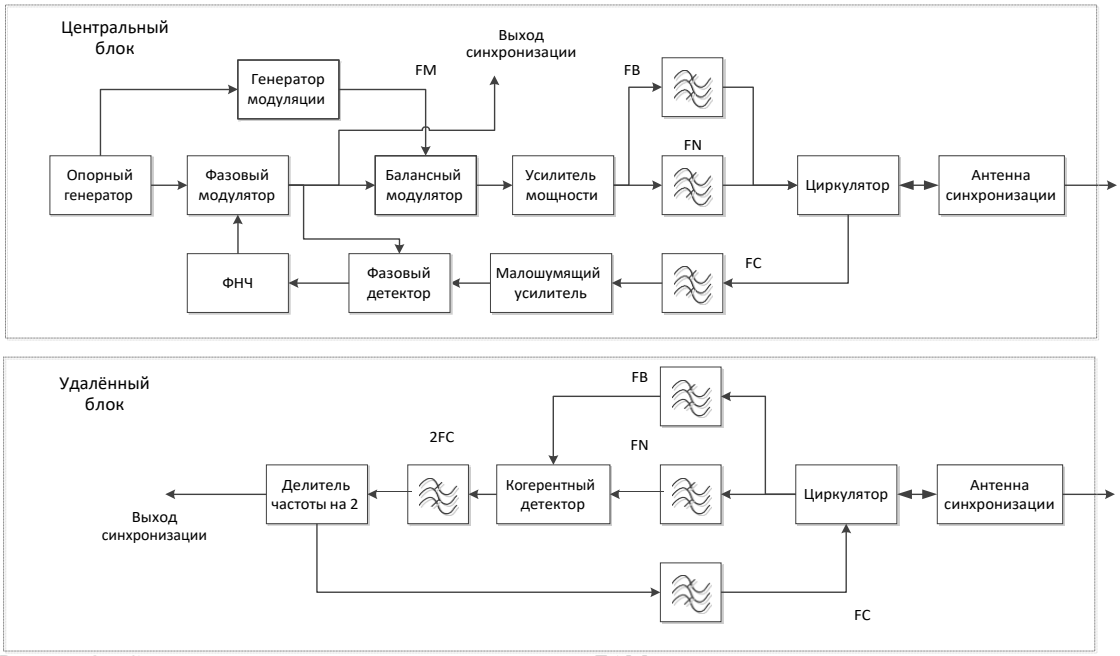


Рисунок 3 – Структурная схема системы синхронизации с БАМ-сигналом

Предлагаемая автором система синхронизации с БАМ-сигналом работает следующим образом.

1. Опорная частота синхронизации FC задаётся опорным генератором. Фаза этого сигнала может регулироваться фазовым модулятором. Для формирования двух связанных частот опорная частота модулируется в балансном модуляторе частотой FM, в результате чего формируются верхняя FB и нижняя FN боковые частоты. После усиления этот сигнал передаётся на удалённый блок. Набор фильтров на частоты FC, FB и FN обеспечивает частотное мультиплексирование – демультиплексирование сигналов.

2. Сигнал, принятый удалённым блоком, содержит верхнюю и нижнюю боковые частоты FB и FN. В когерентном детекторе после преобразования формируется суммарная частота 2FC и разностная частота FM. После фильтрации частота сигнала делится на два, и при этом формируется частота синхронизации удалённого блока. Кроме того, эта частота передаётся в центральный блок.

3. Сигнальная частота FC в центральном блоке усиливается и поступает на фазовый детектор, где сравнивается с текущей частотой центрального блока. Сигнал рассогласования управляет фазовым модулятором, который устраняет фазовое различие фаз центрального и удалённого блоков.

Предлагаемая схема является трёхчастотной, что позволяет повысить развязку сигналов, передаваемых в противоположных направлениях, обеспечить высокий уровень синхронизации в разнесённых системах при простых алгоритмах обработки сигналов.

Заключение. Эффективность работы системы синхронизации будет больше, если использовать трёхчастотную схему. Преимущества такой схемы заключаются в повышении развязки сигналов, передаваемых в противоположных направлениях и обеспечении высокого уровня синхронизации в разнесённых системах при простых алгоритмах обработки сигналов.

Недостатком предложенной схемы с БАМ-сигналом является работа фазового детектора на высокой частоте, что затрудняет обеспечение высокой точности измерения фазы и ограничивает рабочую частоту системы синхронизации.

В настоящий момент проводятся работы по поиску возможных вариантов устранения данного недостатка. Одним из возможных путей является использование специального частотного канала синхронизации со специализированными антенными системами.

Библиографический список

1. Бакулев, П. А. Радиолокационные системы : учебник для вузов / П. А. Бакулев. – Изд. 3-е, перераб. и доп. – Москва : Радиотехника, 2015. – 440 с.

2. Нгуен, С. Ч. Схема синхронизации с амплитудно-модулированным сигналом для распределенных генераторов в спутниковых системах / С. Ч. Нгуен // Техника XXI века глазами молодых ученых и специалистов : сборник конференции ТулГУ. – 2021. – С. 107–113.

3. Нгуен, С. Ч. Двухчастотная схема синхронизации распределенных генераторов в спутниковых си мах / С. Ч. Нгуен // Известия ТулГУ. Технические науки. – 2020. – № 11. – С. 108–113.

4. Описание Террастар. – Режим доступа: https://сельхозпортал.рф/pesticidy_i_agrohimikaty/herbicides /?c_name=terrastar_vdg, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.06.2022).

5. Пестряков, В. Б. Фазовые радиотехнические системы / В. Б. Пестряков. – Москва : Советское радио, 1968. – 469 с.

6. Чернов, Д. А. Синхронизация времени в пространственно разнесенной аппаратуре с помощью сигналов глобальной навигационной спутниковой системы (ГНСС) / Д. А. Чернов // Радиотехнические и телекоммуникационные системы. – 2016. – № 3. – С. 62–67.

7. Juan, Carlos Merlano Duncan. Phase Synchronization Scheme for Very Long Baseline Coherent Arrays / Juan Carlos Merlano Duncan. – 2012. – 197 с.

8. Pinheiro, M. Reconstruction methods of missing SAR data: Analysis in the frame of TanDEM-X synchronization link / M. Pinheiro, M. Rodriguezcassola // Proceedings of the European Conference on Synthetic Aperture Radar, Nuremberg, Germany, 23–26 April 2012.

9. Wang, W.-O. Measurement of Baseline and Orientation between Distributed Aerospace Platforms / W.-O. Wang // The ScientificWorld Journal. – 2013. – Vol. 2013

10. Younis, M. Performance Prediction and Verification for Bistatic SAR Synchronization Link / M. Younis et al. – 2006. – 4 p.

References

1. Bakulev, P. A. *Radiolokatsionnye sistemy : uchebnik dlya vuzov* [Radar systems: a textbook for universities]. Moscow, Radiotekhnika Publ., 2015. 440 p.

2. Nguen, S. Ch. Skhema sinkhronizatsii s amplitudno-modulirovannym signalom dlya raspredelennykh generatorov v sputnikovykh sistemakh [Synchronization circuit with an amplitude-modulated signal for distributed generators in satellite systems]. *Tekhnika XXI veka glazami molodykh uchenykh i specialistov : sbornik konferentsii Tulskogo gosudarstvennogo universiteta* [Technology of the XXI century through the eyes of young scientists and specialists : collection of the conference of Tula State University], 2021, pp. 107–113.

3. Nguyen, S. Ch. Dvukhchastotnaya skhema sinkhronizatsii raspredelennykh generatorov v sputnikovykh sistemakh [Dual Frequency Synchronization Scheme for Distributed Generators in Satellite Systems]. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskiye nauki* [News of Tula State University. Technical Science], 2020, no. 11. pp. 108–113.

4. *Opisanie Terrastar [*Description Terrastar]. Available at: https://сельхозпортал.рф/pesticidy_i_agrohimikaty/herbicides/?c_name=terrastar_vdg (accessed 25.06.2022).

5. Pestryakov, V. B. *Phase radio engineering systems* [Phase radio engineering systems]. Moscow, Sovetskoe radio Publ., 1968. 469 p.

6. Chernov, D. A. Sinkhronizatsiya vremeni v prostranstvenno raznesennoy apparature s pomoshchyu signalov globalnoy navigatsionnoy sputnikovoy sistemy (GNSS) [Time Synchronization in Spatially Diversified Equipment Using Global Navigation Satellite System (GNSS) Signals]. *Radiotekhnicheskiye i telekommunikatsionnyye sistemy* [Radio Engineering and Telecommunication Systems], 2016, no. 3, pp. 62–67.

7. Juan, Carlos Merlano Duncan. *Phase Synchronization Scheme for Very Long Baseline Coherent Arrays*, 2012, 197 p.

8. Pinheiro, M., Rodriguezcassola, M. Reconstruction methods of missing SAR data: Analysis in the frame of TanDEM-X synchronization link. *Proceedings of the European Conference on Synthetic Aperture Radar, Nuremberg, Germany*, 2012, 23–26 April.

9. Wang, W.-O. Measurement of Baseline and Orientation between Distributed Aerospace Platforms [Measurement of Baseline and Orientation between Distributed Aerospace Platforms]. *The Scientific World Journal* [The Scientific World Journal], 2013.

10. Younis, M. et al. *Performance Prediction and Verification for Bistatic SAR Synchronization Link*, 2006. 4 p.

ПРАВИЛА ДЛЯ АВТОРОВ

1. В журнале публикуются материалы на английском и русском языках по тематике, соответствующей утвержденным для журнала отраслям наук, группам специальностей.

2. В список соавторов работ включаются только те лица, которые внесли творческий вклад в подготовку представленных материалов. Лицам, оказавшим только техническую помощь, можно выразить благодарность в конце статьи. Один человек может быть автором (соавтором) не более чем двух статей в одном номере журнала, причем единственным автором он может быть только в одной статье.

3. Объем публикаций для научных статей должен быть не менее 8 страниц, а количество источников в библиографическом списке (списке литературы) – не менее 10 позиций.

4. Содержание каждой статьи должно включать следующие элементы: УДК; название статьи; сведения об авторах, включая их место работы, должность, адрес электронной почты; аннотацию объемом от 100 до 250 слов, ключевые слова (от 9 до 13); графическую аннотацию, отражающую содержание статьи; название статьи, сведения об авторах, аннотацию и ключевые слова на английском языке (для англоязычных статей – на русском языке); введение – оно должно заканчиваться формулировкой цели работы в явной форме; собственно текст статьи – очень желательна его сегментация на разделы, имеющие содержательные заголовки; выводы или заключение (должны соответствовать формулировке цели статьи).

5. Для русскоязычных статей приводится два библиографических списка: на языке оригинала статьи; список с транслитерацией русскоязычных источников на латиницу и (дополнительно) приведением в квадратных скобках переводов названий статей и названий источников на английский язык.

В «русскоязычном» библиографическом списке (списке литературы) порядок следования источников – по алфавиту фамилий авторов (сначала русскоязычные источники, потом иноязычные). На все источники, включенные в библиографический список, должны быть даны ссылки в тексте статьи в квадратных скобках. При необходимости авторы могут указывать номера страниц в источниках, на которые даются ссылки. Приветствуются ссылки на иноязычные источники, а также на материалы, опубликованные ранее в журнале «Прикаспийский журнал: управление и высокие технологии». Однако в последнем случае количество таких ссылок не должно превышать 20 % от общего количества источников, включенных в библиографический список. Для источников, имеющих DOI, целесообразно его указывать. При ссылках на статьи, опубликованные в журнале «Прикаспийский журнал: управление и высокие технологии», целесообразно в конце библиографического описания источника в круглых скобках указывать гиперссылку, указывающую на место размещения статьи на страничке сайта Астраханского государственного университета.

Ссылки в библиографическом списке на материалы, размещенные в интернете, допускаются при соблюдении следующих условий: если у материала, на который дается ссылка, имеется автор и/или название, то они должны быть указаны для этого источника; должен быть приведен полный маршрут доступа к источнику в интернете; должна быть указана дата обращения (доступа) к источнику.

Ограничения по списку литературы: доля самоцитирований для любого из авторов статьи, а также по совокупности всех авторов статьи, не должна превышать 25 %; доля ссылок на статьи с участием одного автора, не являющегося автором (соавтором) статьи, не должна превышать 25 %.

6. Суммарная доля таблиц и иллюстраций в общем объеме представляемой статьи не должна превышать 40 %. Под иллюстрациями понимаются следующие объекты: диаграммы; графики; рисунки; эскизы; фотографии; карты и т.п.

7. Доля оригинального текста в статьях (оцениваемого через систему «Антиплагиат» на сайте www.antiplagiat.ru) должна быть не менее 80 %.

8. Указание на то, что работа финансируется по какому-либо гранту, в рамках Федеральной целевой программы, государственного заказа и пр. дается в виде постраничной сноски после заголовка (названия) работы.

9. В сведения об авторах работ помимо места работы и должности целесообразно включать ORCID автора и гиперссылку на страничку с его личными наукометрическими показателями на сайте www.elibrary.ru. По желанию можно привести также ссылки на странички с наукометрическими показателями на Scopus, в ResearchGate; на личную страничку, размещенную на сайте организации.

10. Основные технические требования к оформлению статей (материалов):

10.1. Текст должен быть расположен по ширине страницы формата А4 с учётом полей (все поля по 2,5 см), набран шрифтом Times New Roman, кегль 10, межстрочный интервал 1,0. В таблицах, подрисуночных надписях допускается уменьшенный шрифт – вплоть до 8 кегля. Альбомная ориентация страниц допускается только в порядке исключения для следующих случаев: широкоформатные таблицы с большим количеством колонок; иллюстрации большого размера, которые не умещаются на странице с книжной ориентацией.

Абзацные отступы одинаковы по всему тексту – 0,75 см. Кавычки («»), скобки ([ ], ( )), маркеры и другие знаки должны быть аналогичными на протяжении всего предоставляемого для публикации материала.

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 4 (60)

Свидетельство о регистрации средства массовой информации
Федеральной службы по надзору в сфере массовых коммуникаций,
связи и охраны культурного наследия
ПИ № ФС77-31932 от 16 мая 2008 г.

Учредитель
Астраханский государственный университет имени В.Н. Татищева
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Адрес редакции:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20

Адрес издателя:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Издание включено в Интернет-каталог
ООО «Агентство «Книга-Сервис» 2022/1

Главный редактор И.М. Ажмухамедов

Редактирование,
компьютерная правка, верстка *Н.Н. Сахно*

Дата выхода в свет 28.12.2022 г.

Цена свободная
Уч.-изд. 12,7. Усл. печ. л. 17,7.
Заказ № 4481. Тираж 500 экз. (первый завод – 25 экз.)

Астраханский государственный университет имени В. Н. Татищева
414056, г. Астрахань, ул. Татищева, 20а Тел. (8512) 24-64-95, тел./факс (8512) 24-68-37
E-mail: asupress@yandex.ru