ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

4
2023

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

1.1.6. Computational Mathematics

2.3.6. Information security methods and systems, information security

2.3.8. Informatics and information processes

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047

e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

1.1.6. Вычислительная математика

2.3.6. Методы и системы защиты информации, информационная безопасность

2.3.8. Информатика и информационные процессы

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика» публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

электронный адрес: grnat@rambler.ru

CONTENTS

СОДЕРЖАНИЕ

УДК 004.65
DOI: 10.28995/2686-679X-2023-4-8-25

Сравнение методов решения задачи выбора плана запроса в реляционной базе данных PostgreSQL

Ирина В. Козлова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, irinakozlovakiv@yandex.ru

Михаил В. Филиппов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, filippov.mike@mail.ru

Аннотация. В данной работе представлен обзор методов построения плана запроса в системе управления базами данных PostgreSQL. План выполнения SQL-запроса – конкретный ряд операций, которые системе управления базами данных необходимо выполнить для получения результата запроса. Задача выбора наименьшего по стоимости плана запроса является задачей поиска оптимального решения, а именно поиска наименьшего по стоимости пути в графе. План запроса можно представить в виде дерева узлов. Такое дерево можно получить из графа всевозможных операций данного запроса, где каждая вершина графа определяет некоторую инструкцию для PostgreSQL и ее стоимость в зависимости от того, в какой последовательности ранее выполнялись операции. Приведенный обзор и представленная классификация позволяют объективно оценить возможности уже существующего метода (генетического алгоритма), а также описать алгоритм применения новых методов в данной области. Предметная область включает в себя описание спецификации реализации построения и выбора плана запроса. Построение плана будет рассматриваться для select-запроса, который направлен на выборку данных. Предложена классификация методов построения плана запроса в реляционной базе данных PostgreSQL.

Ключевые слова: план запроса, PostgreSQL, базы данных, система управления базами данных, СУБД, SQL, динамическое программирование, выборка данных, алгоритм соединения строк, доступ к данным

Для цитирования: Козлова И.В., Филиппов М.В. Сравнение методов решения задачи выбора плана запроса в реляционной базе данных PostgreSQL // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 8–25. DOI: 10.28995/2686-679X-2023-4-8-25

Comparison of methods for the query plan selection problem in a PostgreSQL relational database

Irina V. Kozlova
Bauman Moscow State Technical University, Moscow, Russia,
irinakozlovakiv@yandex.ru

Mikhail M. Filippov
Bauman Moscow State Technical University, Moscow, Russia,
filippov.mike@mail.ru

Abstract. The article is an overview of the methods of building a query plan in PostgreSQL database management system. A SQL query execution plan is a specific set of operations that a database management system needs to perform in order to obtain the query result. The problem of choosing the least costly query plan is the problem of finding the optimal solution, namely finding the least costly path in the graph. The query plan can be represented as a tree of nodes. Such a tree can be obtained from the graph of all possible operations of the query, where each node of the graph defines some instruction for PostgreSQL and its cost depending on the sequence in which the operations were previously executed. The review and the presented classification allow objective evaluating the capabilities of an already existing method (genetic algorithm), as well as describing the algorithm for applying new methods in that area. The subject area includes the description of the specification of the implementation specification of the construction and selection of the query plan. Plan construction will be considered for select-query, which is aimed at data sampling. Classification of methods of query plan construction in PostgreSQL relational database is proposed.

Keywords: query plan, PostgreSQL, databases, database management system, DBMS, SQL, dynamic programming, data sampling, row concatenation algorithm, data access

For citations: Kozlova, I.V. and Filippov, M.B. (2023), "Comparison of methods for the query plan selection problem in a PostgreSQL relational database", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 8–25, DOI: 10.28995/2686-679X-2023-4-8-25

Введение

Каждый запрос, который приходит на вход реляционной базы данных (РБД), обрабатывается в пять этапов [Домбровская 2022].

1. Перевод запроса в промежуточный формат, известный как дерево синтаксического анализа.
2. Трансформация запроса, то есть перезаписывается сгенерированное на втором этапе дерево таким образом, чтобы планировщик/оптимизатор мог с ним работать.
3. Оценка плана запроса с помощью стоимостной модели.
4. Выбор плана запроса с минимальной стоимостью.
5. Выполнение запроса и возврат результата.

Для начала выполнения запроса необходимо извлечь сохраненные данные. Операция доступа к данным определяет алгоритм просмотра таблиц и извлечения только тех строк, которые соответствуют заданному критерию. Поскольку таблицы и индексы хранятся на диске, для работы с ними эти объекты считываются в память, где они представлены в виде отдельных фрагментов (страниц). Эти страницы имеют специальную структуру, и размер страницы по умолчанию составляет 8 килобайт. Существует несколько различных алгоритмов доступа [Домбровская 2022; Моргунов 2017].

1. Последовательный просмотр.
2. Просмотр по индексу.
3. Просмотр исключительно на основе индекса.
4. Просмотр на основе битовой карты.

Второй не менее важной операцией при выполнении запроса является операция соединения наборов строк, это механизм непосредственного выполнения соединения наборов строк. Набор строк может быть получен не только из одной таблицы, а может быть результатом соединения других наборов. Принципиально важным моментом является то, что за один раз соединяются только два набора строк [Тимофеева, Дмитриева, Сагаева 2018].

Существуют три основных алгоритма соединения [Домбровская 2022; Моргунов 2017].

1. Вложенный цикл.
2. Хеширование.
3. Слияние.

Описанные выше операции доступа к данным и соединения строк являются основными в построении плана запроса.

План выполнения SQL-запроса – конкретный ряд операций, которые системе управления базами данных необходимо выполнить для получения результата запроса. Такой план можно представить в виде дерева, где ребра дерева – это движение данных, а узлы –

операции над данными. На примере PostgreSQL будут разобраны шаги получения плана запроса и структуры, которые создаются для этого в памяти [Тимофеева, Дмитриева, Сагаева 2018].

Планировщик SQL-запросов – часть системы управления базами данных (СУБД), которая отвечает за создание итогового плана выполнения запроса. В подавляющем большинстве современных реляционных СУБД используется стоимостный планировщик запросов.

Стоимостная модель оценки плана запроса

Процесс поиска оптимального плана можно разделить на две части: оценку стоимости любого плана (то есть количества ресурсов, необходимых для его выполнения) и выбор плана с минимальной стоимостью [Домбровская 2022].

На сегодняшний день в распространенных СУБД, таких как PostgreSQL, MySQL, Oracle MSSQL, используется планировщик запросов, основанный на стоимостной модели. Его суть заключается в том, что для каждого плана возможно оценить стоимость его выполнения, и на основании этого критерия из всего множества планов СУБД оценит и выберет тот, который будет исполняться быстрее всего.

Стоимость плана рассчитывается с помощью определенных переменных, которые задаются на определенной шкале. По умолчанию эти переменные определяются относительно стоимости чтения последовательной страницы. Например, переменная чтения страницы с диска может быть задана равной 1.0, а остальные переменные стоимости могут быть определены относительно нее [Shetty 2020]. Пример некоторых таких переменных стоимости указаны в табл. 1.

Таблица 1

Название	Описание	Стоимость
seq_page_cost	Чтение одной страницы с диска	1
random_page_cost	Чтение одной произвольной страницы с диска	4
cpu_tuple_cost	Обработка каждой строки при выполнении запроса	0,01
cpu_index_tuple_cost	Обработка каждой записи индекса при сканировании индекса	0,005
cpu_operator_cost	Обработка оператора или функции при выполнении запроса	0,0025

Основными операциями, отображаемыми в планах выполнения запросов СУБД PostgreSQL, являются доступ к данным и соединение наборов строк.

При решении задачи поиска минимального плана запроса его можно представить в виде дерева узлов, где каждый конкретный узел обозначает определенную операцию в PostgreSQL. В данном случае необходимо рассмотреть математическую формализацию задачи, основанную на поиске минимального пути в графе.

В первую очередь необходимо обозначить основные величины:

* *query* – анализируемый запрос;
* $cost_i$ – стоимость вершины графа (у. е.), где $i = 1, \overline{N_{\{Cost\}}}$;
* *CP* – стоимость плана запроса;
* *arr_CP* – массив стоимости всех построенных планов;
* *res_CP* – итоговый план запроса;
* *res_nodes_CP* – множество вершин, входящих в итоговый план запроса;
* *time_plan* – время поиска плана запроса;
* *time_exp_plan* – время выполнения самого дорогого плана (в качестве дорогого плана берется простое соединение всех таблиц без оптимизации).

Стоимость одного плана можно посчитать по следующей формуле:

$$CP = \sum_{i}^{k} cost_i, \tag{1}$$

где k – количество вершин графа, из которых состоит результирующий план запроса.

Выбранный план запроса можно считать решением в случае, если подсчитанная стоимость данного плана является минимальной из всех возможных.

В случае, если время такого плана превышает время выполнения самого «дорогого» плана, то в качестве результата выбирается «дорогой» план. В общем случае условие можно записать следующим образом:

$$res\_CP = \begin{cases} \min(arr\_CP), & \text{если } time\_exp\_plan < time\_plan, \\ time\_exp\_plan, & \text{иначе.} \end{cases} \tag{2}$$

SQL-запрос на выборку данных, для которого происходит выбор плана, должен содержать команду JOIN (INNER JOIN) в операторе FROM:

$$query = '\%INNER\ JOIN\%'. \quad (3)$$

Критерием оптимизации является минимизация стоимости плана. Как было отмечено выше, стоимость плана – это объем ресурсов, необходимых для выполнения плана, то есть для получения всех кортежей результата. Целевая функция принимает следующий вид:

$$L = \sum_i cost_i \to min, \qquad i = (res\_nodes\_CP). \quad (4)$$

Все вышеописанные формулы необходимо привести в математическую модель рассматриваемой задачи выбора плана SQL-запроса:

$$\begin{cases} CP = \sum_i^k cost_i, \\ query =' \%INNER\ JOIN\%', \\ L = \sum_i cost_i \to min, i = (res\_nodes\_CP), \\ res\_CP = \begin{cases} \min(arr\_CP), & \text{если } time\_\text{exp}\_plan < time\_plan, \\ time\_exp\_plan, & \text{иначе.} \end{cases} \end{cases} \quad (5)$$

Таким образом, чем ниже стоимость, тем лучше план [Домбровская 2022].

Жизненный цикл запроса в СУБД PostgreSQL

Каждый запрос, который приходит на вход PostgreSQL обрабатывается в пять этапов [Баканов, Романова, Крюкова 2010].

1. Перевод запроса в промежуточный формат, известный как дерево синтаксического анализа.
2. Трансформация запроса, то есть перезаписывается сгенерированное на втором этапе дерево таким образом, чтобы планировщик/оптимизатор мог с ним работать.
3. Оценка плана запроса с помощью стоимостной модели.
4. Выбор плана запроса с минимальной стоимостью.
5. Выполнение запроса и возврат результата.

На рис. 1 представлена IDEF0 диаграмма жизненного цикла запроса в PostgreSQL [Хайдарова 2020].

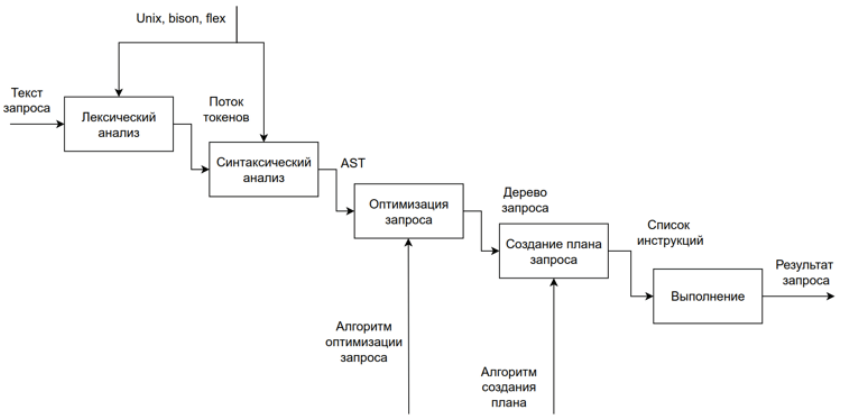

Рис. 1. IDEF0 диаграмма жизненного цикла запроса в PostgreSQL

На рис. 2 представлена IDEF0 диаграмма второго уровня шага «Оптимизация запроса» [Хайдарова 2020]. На этапе «Создание порядка соединений отношений» для ускорения работы можно применить различные методы:

– динамического программирования;
– имитации отжига;
– итеративного улучшения;
– двухфазной оптимизации.

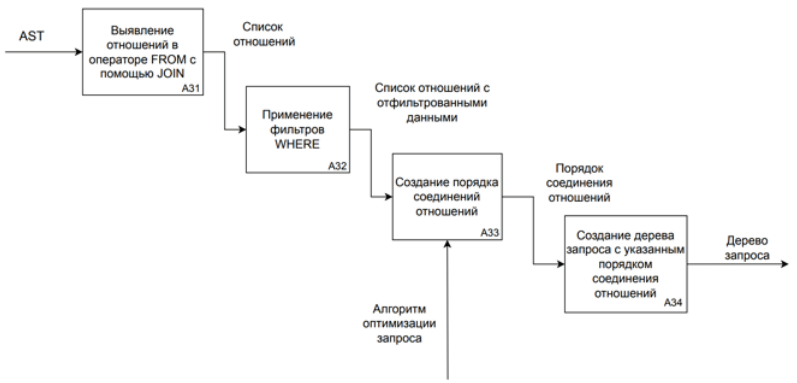

Рис. 2. IDEF0 диаграмма второго уровня шага «Оптимизация запроса»

Методы выбора оптимального плана запроса

Задача построения плана запроса включает в себя задачу поиска оптимального плана. Данная задача относится к классу задач дискретного математического программирования. В связи с большим размером пространства эквивалентных планов поиск оптимального является наиболее ресурсоемким этапом выполнения задачи построения плана запроса.

С одной стороны, найденный план должен быть как можно более эффективным, с другой – на построение не может быть затрачено слишком много времени. Поэтому в зависимости от сложности запроса применяют точные или приближенные методы, результатом которых является некоторый субоптимальный план.

Задачу поиска оптимального плана запроса условно можно разделить на два шага [Хайдарова 2020].

1. Оценка стоимости плана (количество ресурсов, необходимых для его выполнения).
2. Выбор плана с минимальной стоимостью.

Метод динамического программирования

Метод динамического программирования для решения задач оптимизации был предложен американским математиком Р. Беллманом в середине прошлого века [Гришкина 2019]. Динамическое программирование – метод решения задачи путем ее разбиения на несколько одинаковых подзадач, рекуррентно связанных между собой, которые имеют такую же структуру. Для того чтобы метод динамического программирования мог быть применен, задача должна обладать оптимальной подструктурой, то есть оптимальное решение задачи может быть составлено из оптимальных решений ее подзадач. Кроме того, должны быть пересекающиеся подзадачи, то есть одна и та же подзадача нужна для решения большого количества других подзадач.

Основная идея метода заключается в сведении сложной задачи к последовательности более простых задач. Например, рассматривалась задача управления движением динамической системы, где состояние системы описывается параметрами. Внешние воздействия, осуществляемые в определенные моменты времени, переводят систему из одного состояния в другое. Последовательность таких переходов образует траекторию движения системы.

Задача динамического программирования заключается в поиске такого набора внешних воздействий, который переведет систему из начального состояния в конечное с минимальными затратами [Гришкина 2019].

Метод динамического программирования является эффективным способом решения задач оптимизации. Он основан на принципе оптимальности Р. Беллмана, который гласит, что оптимальное решение задачи может быть составлено из оптимальных решений ее подзадач. Для применения метода динамического программирования необходимо, чтобы задача обладала оптимальной подструктурой, пересекающимися подзадачами и возможностью сохранять вычисленные значения для повторного использования [Чернов, Куров 2022].

Динамическое программирование обычно придерживается двух подходов к решению задач: нисходящего и восходящего. В нисходящем подходе задача разбивается на более простые подзадачи меньшего размера, которые решаются отдельно и затем комбинируются для получения оптимального решения исходной задачи. В восходящем подходе все подзадачи основной задачи вычисляются заранее и сохраняются для дальнейшего использования при построении решения исходной задачи.

Нисходящее динамическое программирование решает только подзадачи по мере необходимости, что позволяет сократить количество вычислений [Окулов 2015]. Восходящее динамическое программирование, напротив, вычисляет все подзадачи заранее, что позволяет избежать повторных вычислений, но требует больше памяти для сохранения всех вычисленных значений.

Оба подхода имеют свои преимущества и недостатки, и выбор между ними зависит от конкретной задачи и ее требований. Однако в обоих случаях метод динамического программирования позволяет эффективно решать сложные оптимизационные задачи, разбивая их на более простые подзадачи и используя полученные значения для выбора оптимального решения [Гришкина 2019].

Основная идея использования данного метода при решении задачи построения плана запроса заключается в пошаговом наращивании частичного плана, производя частичный перебор с последующим отсевом заведомо неоптимальных вариантов на каждом шаге.

Другими словами, имея набор различных планов извлечения данных для участвующих в запросе отношений, можно выделить следующие шаги.

1. Рассмотрение всех планов попарного соединения отношений и удаление заведомо неоптимальных.

2. Рассмотрение всевозможных попарных соединений оставшихся планов из первоначального набора с планами, полученными в результате предыдущего шага, удаление заведомо неоптимальных планов из дальнейшего рассмотрения.

Данные шаги повторяются до тех пор, пока не будет получено соединение всех участвующих отношений.

Алгоритм динамического программирования дает точное решение оптимизационной задачи, однако имеет высокую вычислительную сложность в наихудшем случае [Гришкина 2019; Окулов 2015]. Он является эффективным подходом к решению оптимизационных задач, основанным на разбиении исходной задачи на подзадачи и использовании результатов решения этих подзадач для нахождения оптимального решения всей задачи.

Оценка сложности динамического программирования может быть выражена с помощью следующей формулы:

$$T(n) = O(k \cdot n^m), \quad (6)$$

где $T(n)$ – время выполнения алгоритма в зависимости от размера входных данных n, k – константа, которая зависит от конкретной задачи и используемых операций, m – количество подзадач, на которые задача разбивается. Время выполнения алгоритма растет экспоненциально с увеличением размера входных данных.

В задаче выбора плана запроса данный метод может использоваться для оптимизации порядка соединения таблиц в операторе FROM. Выбор между нисходящим и восходящим подходами зависит от конкретной задачи и ее требований. Если задача имеет большой размер и требует оптимального использования памяти, то нисходящий подход может быть предпочтительным. Если задача маленькая или требует предварительного вычисления всех подзадач, то восходящий подход может быть более эффективным [Хайдарова 2020].

Методы случайного «блуждания» на графах

Для выбора из более сложных вариантов запроса можно использовать методы случайного «блуждания» на графах (метод случайного выбора).

В качестве возможных методов случайного «блуждания» можно упомянуть методы имитации отжига (метод имитации спуска), итеративного улучшения и двухфазной оптимизации. Следует отметить, что эти методы являются общими и могут быть

применены к различным аспектам оптимизации, включая оптимизацию запросов. В таких методах оптимальный план находится путем случайных перемещений по графу. Планы пространства поиска рассматриваются как узлы графа.

Узлы соединены дугами, если один план может быть преобразован в другой с помощью некоторого элементарного преобразования. Узлы, которые могут быть достигнуты из другого узла за один шаг (то есть соединены дугой), называются соседними узлами. Каждому узлу присваивается его стоимость.

Цель таких методов – найти узел с минимальной стоимостью среди всех узлов графа. Шаги могут быть как вверх, если стоимость узла, в который он приведет, будет выше стоимости текущего узла, так и вниз, если стоимость будет ниже.

Узел называется глобальным минимумом, если его стоимость минимальна среди всех узлов графа. Если стоимость узла минимальна среди всех его соседей и он не является глобальным минимумом, то такой узел называется локальным минимумом.

Метод имитации отжига

Метод имитации отжига (Simulated Annealing, SA) [Окулов 2015; Giri, Kumar 2013] – это метод решения различных оптимизационных задач, основанный на моделировании физического процесса кристаллизации вещества из жидкого состояния в твердое, включая отжиг металлов.

Цель метода заключается в минимизации определенной функции. В процессе работы алгоритма сохраняется текущее решение, которое является промежуточным результатом и становится ответом после выполнения алгоритма.

Для описания алгоритма следует ввести следующие понятия.

1. Температура – действительное число (изначально равно единице), которое будет изменяться в течение оптимизации и влиять на вероятность перейти в соседнее состояние.

2. Энергия – вещественного число, которое характеризует оптимальность предлагаемого решения, является оценкой начального решения.

Основные этапы данного метода.

1. Выбор начального решения.

Начальное решение обычно выбирается случайным образом, но также можно использовать решение, полученное другими методами «блуждания» на графах. Это дает методу базу, на основе которой он будет строить более оптимальное решение.

2. Оценка начального решения.

3. Возможная замена текущего решения измененным.

Для определенности будем считать, что оптимизация заключается в минимизации энергии. На данном этапе происходит проверка и возможная замена текущего решения измененным. Если измененное решение имеет меньшую энергию, то оно принимается за текущее. Если же измененное решение имеет большую энергию, то оно принимается с вероятностью по формуле Больцмана:

$$P = \exp\left(\frac{E_{current} - E_{new}}{t}\right), \quad (7)$$

где P – вероятность принять измененное решения, E_{new} – энергия измененного решения, $E_{current}$ – энергия текущего решения, t – текущая температура.

4. Уменьшение температуры.

При большой температуре высока вероятность выбора менее оптимального решения. Это позволяет искать оптимальное решение, когда температура становится достаточно низкой. Однако если температура снижается слишком быстро, то алгоритм может найти локальный минимум. Поэтому важно подобрать правильную стратегию уменьшения температуры, чтобы достичь баланса между исследованием пространства решений и поиском оптимального решения.

В случае применения этого метода к задаче построения плана запроса алгоритм начинает работу в определенной точке графа и продолжает перемещаться, всегда допуская случайные шаги вниз и с некоторой вероятностью шаги вверх, чтобы избежать попадания в дорогой локальный минимум.

В процессе работы алгоритма вероятность сделать шаг вверх постепенно уменьшается до нуля, и алгоритм завершает работу, достигнув некоторого локального минимума. Метод имитации отжига является стохастическим методом оптимизации, который позволяет искать глобальный минимум путем принятия случайных решений и прогрессивного уменьшения вероятности принятия худших решений по мере улучшения текущего решения.

Оценку сложности метода имитации отжига сложно выразить с помощью конкретной формулы, так как она зависит от различных факторов, таких как размер пространства поиска, начальное состояние системы, параметры алгоритма и т. д.

Однако в общем случае сложность метода имитации отжига может быть оценена по формуле

$$T(n) = O(k \bullet n), \quad (8)$$

где $T(n)$ – время выполнения алгоритма в зависимости от размера входных данных n, k – константа, которая зависит от конкретной задачи и используемых операций, n – количество итераций алгоритма или размер пространства поиска. Время выполнения метода имитации отжига растет линейно с увеличением количества итераций или размера пространства поиска.

Метод итеративного улучшения

Концепция метода итеративного улучшения (Iterative Improvement, II) основана на использовании двух циклов [Giri, Kumar 2013]. Внутренний цикл в основном применяется для процесса локальной оптимизации. Во время локальной оптимизации алгоритм сначала выбирает случайное состояние из огромного пространства поиска, а затем последовательно улучшает решение до достижения состояния локального минимума. Этот процесс итеративного улучшения решения продолжается до достижения условия остановки.

По достижении условия остановки алгоритм возвращает минимальную стоимость, достигнутую данным распределением состояний [Giri, Kumar 2013]. Если есть вероятность бесконечного времени, то алгоритм может достичь глобального минимума, который зависит от параметров задачи, которую решает.

При решении задачи построения плана запроса метод итеративного улучшения выполняет множество локальных оптимизаций, каждая из которых начинается в случайном узле графа. Локальная оптимизация заключается в последовательном выполнении случайных шагов вниз до достижения локального минимума или выполнения условия завершения, которое может быть связано с ограничением плана запроса или временем.

В результате возвращается наименьший из найденных локальных минимумов, полученных таким образом. Использование метода итеративного улучшения может привести к выигрышу во времени в задаче выбора плана запроса. Это связано с тем, что метод позволяет быстро и эффективно находить локальные оптимумы, что может сократить время, затраченное на поиск глобального минимума.

В задаче выбора плана запроса метод итеративного улучшения может использоваться для оптимизации параметров плана запроса, таких как порядок выполнения операций или выбор индексов.

Внутренний цикл метода будет итеративно улучшать план запроса, выбирая случайные состояния и находя локальные минимумы.

Оценка сложности метода итеративного улучшения может быть выражена с помощью следующей формулы:

$$T(n) = O(k \bullet n), \quad (9)$$

где $T(n)$ – время выполнения алгоритма в зависимости от размера входных данных n, k – константа, которая зависит от конкретной задачи и используемых операций, n – количество итераций алгоритма или размер пространства поиска. Время выполнения метода имитации отжига растет линейно с увеличением количества итераций или размера пространства поиска. Однако эффективность метода может сильно варьироваться в зависимости от выбора параметров и начального состояния системы.

Метод двухфазной оптимизации

Метод двухфазной оптимизации (Two-Phase Optimization, 2PO) в задаче построения плана запроса представляет собой комбинацию различных методов, например метода итеративного улучшения и имитации отжига.

На первой фазе производится несколько итераций, где ищется локальный минимум. Полученный локальный минимум становится стартовым узлом на второй фазе, где происходит «блуждание» по графу, например, при помощи SA с низкой вероятностью шагов вверх, тем самым позволяя обходить небольшие локальные минимумы, но не допуская слишком длинные пути вверх.

Выигрыш во времени при использовании метода двухфазной оптимизации в задаче выбора плана запроса заключается в более быстрой сходимости к оптимальному решению. Поскольку на первой фазе происходит поиск локального минимума, а на второй фазе используются методы «блуждания» по графу, поэтому ускоряется процесс оптимизации и снижается вероятность застревания в небольших локальных минимумах.

Оценка сложности метода двухфазной оптимизации может быть выражена с помощью следующей формулы:

$$T(n) = O(k \bullet n1 + m \bullet n2), \quad (10)$$

где $T(n)$ – время выполнения алгоритма в зависимости от размера входных данных n, k – константа, которая зависит от конкретной задачи и используемых операций в первой фазе, $n1$ – количество

итераций алгоритма или размер пространства поиска в первой фазе, *m* – константа, которая зависит от конкретной задачи и используемых операций, *n2* – количество итераций алгоритма или размер пространства поиска в первой фазе.

Если рассматривать select-запросы на выборку данных с использованием INNER JOIN, то вышеперечисленные методы можно применить на шаге «Создание порядка соединений отношений», так как время выполнения и планирования запроса, содержащего оператор JOIN, зависит именно от того, в каком порядке таблицы будут соединяться.

По вышеописанным оценкам сложности можно ожидать выигрыш во времени планирования запроса, представленный в табл. 2.

Таблица 2

Метод	Ожидаемый выигрыш во времени
динамического программирования	0,9 – 1,0 раза
имитации отжига	1,2 – 1,5 раза
итеративного улучшения	1,2 – 1,5 раза
двухфазной оптимизации	0,5 – 0,8 раза

Также стоит отметить, что ожидается лучший выигрыш во времени при большем количестве соединений. На основе сравнения описанных методов, представленного в табл. 3, можно предположить, что если использовать методы «блуждания» по графам для запроса с небольшим набором таблиц в операторе FROM, то можно уменьшить время планирования запроса.

Заключение

Метод имитации отжига может быть полезен для задачи выбора плана запроса, когда пространство состояний большое и сложно исследовать его полностью. Итеративное улучшение – когда целевая функция сложна или неформализуема. Двухфазная оптимизация – когда требуется быстрое приближенное решение и дополнительные ресурсы могут быть выделены для точного решения. Динамическое программирование – когда задача имеет определенную структуру и можно использовать рекурсивный подход для ее решения.

В зависимости от особенностей запроса, план которого нужно выбрать, можно определить наиболее подходящий метод для достижения оптимального плана запроса.

Таблица 3

Разновидность	Наличие фактора случайности в выборе следующего шага	Нахождение минимума	Допустимый размер запроса
Метод имитации отжига	Вероятностный	Локальный	Небольшие запросы (до 20 соединений)
Метод итеративного улучшения	Нет	Локальный	Небольшие запросы (до 20 соединений)
Метод двухфазной оптимизации	Зависит от алгоритма	Локальный	Большие запросы (от 20 соединений)
Нисходящее динамическое программирование	Нет	Глобальный	Небольшие запросы (до 20 соединений)
Восходящее динамическое программирование	Нет	Глобальный	Большие запросы (от 20 соединений)

Литература

Баканов, Романова, Крюкова 2010 – *Баканов М.В., Романова В.В., Крюкова Т.П.* Базы данных. Системы управления базами данных: Учеб. пособие. Кемерово: Кемеровский технологический институт пищевой промышленности, 2010. 166 с.

Гришкина 2019 – *Гришкина Т.Е.* Динамическое программирование: Учеб.-метод. пособие. М.: АмГУ, 2019. 38 с.

Домбровская 2022 – *Домбровская Г.* Оптимизация запросов в PostgreSQL. М.: ДМК Пресс, 2022. 279 с.

Моргунов 2017 – *Моргунов Е.П.* Основы языка SQL. СПб.: БХВ-Петербург, 2017. 257 с.

Окулов 2015 – *Окулов С.М.* Динамическое программирование. М.: Бином, 2015. 20 с.

Тимофеева, Дмитриева, Сагаева 2018 – *Тимофеева Н.Е., Дмитриева К.А., Сагаева И.Д.* Анализ современных технологий хранения сверхбольших объемов информации // Программные продукты, системы и алгоритмы. 2018. № 1. С. 3.

Хайдарова 2020 – *Хайдарова С.* Создание SQL-запросов в реляционных базах данных // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 3. С. 8–19. DOI: 10.28995/2686-679X-2020-3-8-19.

Чернов, Куров 2022 – *Чернов И.Е., Куров А.В.* Применение генетических алгоритмов в криптографии // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 63–82. DOI: 10.28995/2686-679X-2022-1-63-82.

Giri, Kumar 2013 – *Giri A.K., Kumar R.* Distributed query processing plan generation using iterative improvement and simulated annealing // 3rd IEEE International Advance Computing Conference (IACC). New York, NY: IEEE, 2013. P. 757–762.

Shetty 2020 – *Shetty S.* Mastering PostgreSQL 13. Birmingham: Packt, 2020. 363 c.

References

Bakanov, M.V., Romanova, V.V. and Kryukova, T.P. (2010), *Bazy dannykh. Sistemy upravleniya bazami dannykh. Ucheb. posob.* [Databases. Systems of database management. Study guide], Kemerovo Technological Institute of Food Industry, Kemerovo, Russia, 166 p.

Grishkina, T.E. (2019), *Dinamicheskoe programmirovanie. Ucheb.-metod. posobie* [Dynamic programming. Study guide], Amur State University, Moscow, Russia, 38 p.

Dombrovskaya, G. (2022), *Optimizatsiya zaprosov v PostgreSQL* [Query Optimization in PostgreSQL], DMK Press, Moscow, Russia, 279 p.

Morgunov, E.P. (2017), *Osnovy yazyka SQL* [SQL Basics], BHV-Petersburg, Saint Petersburg, Russia, 257 p.

Okulov, S.M. (2015), *Dinamicheskoe programmirovanie* [Dynamic programming], Binom, Moscow, Russia, 20 p.

Timofeeva, N.E., Dmitrieva, K.A. and Sagaeva, I.D. (2018), "Analysis of modern technologies for storing ultra-large amounts of information", Software products, systems and algorithms, no. 3, p. 3.

Khaidarova, S. (2020), "Creation of SQL-queries in relational databases", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 3, pp. 8–19. DOI: 10.28995/2686-679X-2020-3-8-19.

Chernov, I.E., and Kurov, A.V. (2022), "Using of genetic algorithms in cryptography", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 1, pp. 63–82. DOI: 10.28995/2686-679X-2022-1-63-82.

Giri, A.K. and Kumar, R. (2013), "Distributed query processing plan generation using iterative improvement and simulated annealing", 3rd IEEE International Advance Computing Conference (IACC), IEEE, New York, NY, USA, pp. 757–762.

Shetty, S. (2020), Mastering PostgreSQL 13. Packt, Birmingham, England, 363 p.

Информация об авторах

Ирина В. Козлова, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; irinakozlovakiv@yandex.ru

Михаил В. Филиппов, кандидат технических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; filippov.mike@mail.ru

Information about the authors

Irina V. Kozlova, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; irinakozlovakiv@yandex.ru

Mikhail M. Filippov, Cand. Of Sci. (Computer Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; filippov.mike@mail.ru

УДК 004:343.1
DOI: 10.28995/2686-679X-2023-4-26-46

Цифровое уголовное дело: перспективы и проблемы

Дмитрий А. Митюшин
Российский государственный гуманитарный университет, Москва, Россия, dalexx@inbox.ru

Андрей С. Моляков
Российский государственный гуманитарный университет, Москва, Россия, andrei_molyakov@mail.ru

Аннотация. Цифровизация в той или иной степени проникает во все сферы жизни современного общества. Связано это как со вступлением большого количества государств в постиндустриальную эпоху развития, так и с введением отдельных законодательных актов для цифровизации различных сфер деятельности общества.

Вопросы цифровизации не оставили в стороне и такие сферы, как уголовный процесс и уголовное судопроизводство. По данной теме ведутся дискуссии как на различных тематических конференциях, так и в научных публикациях специалистами различных научных направлений, большей частью юристами.

В данной статье рассмотрены вопросы трансформации «традиционной» (бумажной) процедуры формирования уголовного дела в цифровую форму на этапах его жизненного цикла, начиная с момента возбуждения уголовного дела и заканчивая сдачей его в архив. Показаны перспективы такой трансформации и возникающие при этом проблемы, требующие решения.

В первую очередь рассмотрены технические вопросы цифровизации уголовного делопроизводства.

Информация, представленная в статье, будет полезна не только специалистам в области информационных технологий и защиты информации, но и специалистам в области уголовного права и уголовного процесса.

Ключевые слова: цифровизация, уголовное дело, цифровое уголовное дело, следствие, следственные органы

Для цитирования: Митюшин Д.А., Моляков А.С. Цифровое уголовное дело: перспективы и проблемы // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 26–46. DOI: 10.28995/2686-679X-2023-4-26-46

Digital criminal case. Prospects and issues

Dmitrii A. Mityushin
Russian State University for the Humanities, Moscow, Russia,
dalexx@inbox.ru

Andrei S. Molyakov
Russian State University for the Humanities, Moscow, Russia,
andrei_molyakov@mail.ru

Abstract. In a sense digitalization penetrates into all spheres of life of modern society. It is due both to the entry of a large number of states into the post-industrial era of development, and to the introduction of separate legislative acts for the digitalization of various spheres of society.

The issues of digitalization have not left aside such areas as criminal process and criminal proceedings. There are heated discussions on the issue, both at various thematic conferences and in scientific publications by specialists of various scientific fields, mostly lawyers.

Without going too much into legal subtleties, the article discusses the transformation of the "traditional" (paper) procedure of the criminal case formation into a digital form at the stages of its life cycle, starting from the initiation of a criminal case to its archiving. The prospects for such a transformation and issues that arise therefrom that need to be solved are shown.

First of all, the technical issues in such digitalization of criminal proceedings are considered.

The information presented in the article will be useful not only for specialists in the field of information technology and information protection, but also for those in the field of criminal law and criminal procedure.

Keywords: digitalization, criminal case, digital criminal case, investigation, investigative authorities

For citation: Mityushin, D.A. and Molyakov, A.S. (2023), "Digital criminal case. Prospects and issues", *RSUH/RGGU Bulletin. "Informatics. Information security. Mathematics"* Series, no. 4, pp. 26–46, DOI: 10.28995/2686-679X-2023-4-26-46

Введение

Процесс цифровизации в той или иной степени проникает во все сферы жизни современного общества. Затронул он также и различные аспекты деятельности правоохранительных органов. Большей частью это касается облегчения подготовки документов, ускорения документооборота за счет внедрения различных систем

электронного документооборота (например, сервис СЭД системы ИСОД МВД России[1]).

Несколько лет назад в сети Интернет и научных публикациях обсуждалась проблема перевода уголовного судопроизводства в цифровой формат и отказ от «бумажного» вида уголовных дел. На проходившей 10 и 11 мая 2023 г. в Санкт-Петербургском университете МВД России Международной конференции эта тема снова была затронута.

В данной статье рассмотрим вопросы цифровизации уголовного дела (далее – УД) главным образом с точки зрения технической реализации и некоторых аспектов информационной безопасности.

Понятие цифрового уголовного дела

Для начала определим, что будем понимать под цифровым уголовным делом. Для этого определимся с термином «уголовное дело». Специалисты в области уголовного процесса (далее – УП) по-разному определяют данное понятие.

Как указывают в своей работе В.В. Конин, А.В. Кудрявцева и А.В. Петров [Конин, Кудрявцева, Петров 2022], уголовно-процессуальное законодательство нашей страны не содержит ответа на вопрос, что следует понимать под термином «уголовное дело». В то же время, как отмечают указанные авторы, Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ или УПК) использует термин «уголовное дело» 1598 раз, но не содержит каких-либо разъяснений и толкований, что следует понимать под этим термином. По этому поводу ведутся научные дискуссии среди ученых блока юридических наук.

Согласно позиции Л.Н. Масленниковой под *уголовным делом* (далее – УД) понимается процесс уголовного судопроизводства (производство процессуальных действий и принятие процессуальных решений), который документируется. Совокупность таких документов именуется *материалами уголовного дела*[2].

В то же время, как указывают те же авторы [Конин, Кудрявцева, Петров 2022], понятие «уголовно-процессуальное производство», как и понятие «уголовное судопроизводство», является более широким, нежели понятие «уголовное дело». Так, например, в стадии

---

[1] Сервис электронного документооборота Единой системы информационно-аналитического обеспечения деятельности МВД России.

[2] Уголовно-процессуальное право Российской Федерации: Учебник / Отв. ред. П.А. Лупинская. 2-е изд., перераб. и доп. М.: Норма, 2009. 1072 с.

исполнения приговора УД уже отсутствует, но уголовно-процессуальное производство продолжается по вопросам, перечисленным в ст. 397 УПК РФ. Вместе с тем совокупность процессуальных действий и решений в стадии исполнения приговора в судебной практике принято именовать *материалами судебного производства*, а не уголовным делом. Судебно-контрольное производство на досудебных стадиях также принято именовать материалами *судебного производства по судебному контролю*.

Достаточно интересное мнение высказывают С.В. Супрун и Р. Ганболд. С их точки зрения,

> *уголовное дело* – совокупность процессуальных документов, удостоверяющих деятельность органов предварительного расследования, прокурора и суда по установлению, исследованию и разрешению уголовно-правовых и уголовно-процессуальных отношений, возникающих между участниками уголовного судопроизводства со стороны обвинения и защиты в результате совершения общественно опасного деяния, запрещенного уголовным законом [Супрун, Ганболд 2019].

В.В. Конин предлагает рассматривать термин «уголовное дело» не только с позиции УП, но и криминалистики, как взаимосвязанных и дополняющих друг друга наук криминального цикла. По его мнению,

> с позиций уголовного процесса УД можно рассматривать в следующих видах:
> – как систему, объединяющую в себе оперативно-розыскные, следственные и процессуальные, а также судебные решения, в том числе по результатам судебного контроля, образующие доказательственную и процессуальную совокупность, позволяющую следователю, дознавателю, прокурору и суду сделать вывод о виновности либо невиновности лица, привлеченного к уголовной ответственности;
> – как собранные в одном месте, систематизированные, а по окончании расследования сшитые и пронумерованные документы, содержащие информацию о проведенных в процессе расследования оперативно-розыскных, судебных, следственных и процессуальных действиях, избранных мерах пресечения и иных мерах процессуального принуждения, осуществленных в связи с расследуемым преступлением, для последующего рассмотрения по существу предъявленного обвинения в суде [Конин 2021].

Таким образом, одни ученые определяют термин «уголовное дело» как некий процесс в пространстве и времени, другие связы-

вают данный термин с процессуальными документами, в которых отражены результаты тех или иных оперативно-розыскных, следственных, процессуальных и судебных действий.

Исходя из этого, можно дать следующее определение цифрового уголовного дела, опираясь на определение авторов В.В. Конина, А.В. Кудрявцевой и А.В. Петрова [Конин, Кудрявцева, Петров 2022].

Цифровое (электронное) уголовное дело (далее – ЦУД) – собранные в одной базе данные о проведенных оперативно-розыскных, следственных и судебных действиях, выполненные и сохраненные в цифровом виде в информационной системе на электронном носителе, имеющие непосредственное отношение к расследуемому преступлению.

Исходя из определения, будем рассматривать ЦУД как электронный информационный ресурс.

Постановка задачи

На основе анализа современных информационных технологий и технологий защиты информации необходимо определить основные пути процесса цифровизации УД на различных стадиях ***жизненного цикла*** (далее – ЖЦ) УД.

Жизненный цикл уголовного дела можно определить как период существования УД (ЦУД) от момента возбуждения до сдачи в архив.

С одной стороны, логичнее ЖЦ ЦУД привязать к стадиям уголовного процесса. Согласно УПК РФ[3] эти стадии включают:

- возбуждение уголовного дела;
- предварительное расследование;
- подготовка к судебному заседанию;
- судебное разбирательство;
- производство в суде апелляционной инстанции (апелляция);
- исполнение приговора;
- производство в суде кассационной инстанции (кассация);
- производство в надзорной инстанции (надзор);
- возобновление производства по уголовному делу ввиду новых или вновь открывшихся обстоятельств;
- завершение УД.

[3] Основные категории уголовного процесса // Адвокатское бюро «Антонов и партнеры». URL: https://pravo163.ru/osnovnye-kategorii-ugolovnogo-processa/ (дата обращения 11.06.2023).

Разумеется, не каждое УД проходит все перечисленные этапы ЖЦ.

Однако, рассматривая ЦУД как информационный ресурс, такие стадии ЖЦ не являются корректными. С точки зрения ЖЦ информационного ресурса можно выделить следующие *стадии ЖЦ ЦУД*:

- формирование ЦУД – соответствует стадии возбуждения УД;
- использование (эксплуатация) ЦУД – соответствует остальным стадиям уголовного процесса;
- вывод ЦУД из использования (эксплуатации) – соответствует последней стадии уголовного процесса и сдачи дела в архив.

Преимущества и недостатки цифрового уголовного дела

У процесса цифровизации УП имеются как сторонники, ратующие за тотальную цифровизацию уголовного процесса, так и противники, выступающие категорически против цифровизации одной, пожалуй, из самых консервативных областей человеческой деятельности. Есть третья категория, которые не видят ничего плохого в цифровизации, но не особенно и поддерживают данную тенденцию. Ряд авторов [Миронова 2023; Носко 2023; Зуев, Титова 2019; Головко 2019; Зуев 2018] едва касаются достоинств цифровизации уголовного процесса и сразу переходят к недостаткам. Это понятно, так как, как уже сказано выше, уголовный процесс – одна из самых консервативных сфер общественной деятельности, как затрагивающая права и свободы граждан, так и влияющая на судьбу отдельно взятого человека.

На сегодняшний день внедрение информационных технологий (далее – ИТ) в процесс комплектования уголовного дела большей частью состоит в том, что процессуальные и иные документы (протоколы, акты, запросы и пр.) могут набираться на компьютере, но затем они распечатываются, подписываются участниками следственного действия, при необходимости, скрепляются печатью органа дознания или предварительного расследования. Однако в этом случае мы опять-таки наблюдаем традиционное, «бумажное» УД, созданное с использованием ИТ. В данной статье рассмотрим именно процесс формирования ЦУД в составе некой информационной системы без создания бумажных копий. В работе профессора С.В. Зуева [Зуев 2018]

указывается, что в 2005 г. в Бельгии создан проект электронного правосудия *Phoenix*. В Саудовской Аравии несколько лет назад перешли на электронное правосудие, сократив сроки расследования на 80%. Заметно продвинулись в цифровизации судопроизводства Южная Корея, Сингапур, Эстония. В Грузии в 2011 г. осуществлен переход на цифровой формат УД.

В качестве основных преимуществ ЦУД перед УД в традиционной форме можно выделить следующие:

– ускорение сроков расследования;
– существенное сокращение бумажного документооборота;
– затруднение фальсификации уголовного дела со стороны сотрудника органа дознания или предварительного следствия;
– сокращение времени при знакомстве подследственных с материалами УД;
– существенное облегчение копирования материалов УД.

К недостаткам внедрения ЦУД можно отнести следующие:

– удорожание инфраструктуры, особенно на этапе внедрения;
– вопросы, связанные с рядом процессуальных действий;
– психологические проблемы с точки зрения восприятия ЦУД участниками процесса;
– кадровые проблемы.

Кроме того, профессор С.В. Зуев [Зуев 2018] выделяет следующие недостатки:

– сложность в обеспечении информационной безопасности;
– возможность фальсификации информации следователем.

Рассмотрим достоинства и недостатки ЦУД более подробно. Начнем с достоинств.

1. Ускорение сроков расследования.

За счет использования систем электронного документооборота, элементов искусственного интеллекта может в значительной мере сократиться время передачи ЦУД из одной инстанции в другую, формирование и направление различных процессуальных документов (постановлений, поручений, ходатайств, заключений, протоколов и т. д.) между участниками уголовного процесса, участниками УП и внешними абонентами.

Также сокращение сроков расследования будет достигаться за счет автоматизированного поиска по другим уголовным делам с целью выявления схожего почерка преступления, одних и тех же фигурантов и т. п. Это и ряд других функций реализованы в АПК «Невод» [Янушко, Бабанин, Кузнецова, Петрушенко, Чекмарев 2011]. Кроме того, существует интегрированный банк данных (ИБД-М) ИСОД МВД России, предназначенный для формирова-

ния и ведения розыскных, криминалистических и профилактических учетов территориальных органов МВД России.

Например, как указывает в аналитической статье М. Сазонова[4], при использовании экспериментального решения в виде программного обеспечения для автоматической обработки заявлений ФНС России о выдаче судебных приказов, которое используется в трех судебных участках мировых судей Белгородской области, время, затрачиваемое на подготовку судебного акта, уменьшилось на 84%, а время на заполнение карточки судебного дела в электронной картотеке – на 96%. Разумеется, в уголовном производстве эти цифры могут отличаться. Как было указано выше, в Саудовской Аравии с переходом на электронное правосудие сроки расследования сократились на 80%.

2. Существенное сокращение бумажного документооборота.

Данное преимущество вполне очевидно. Внедрение ЦУД приведет к значительному сокращению использования бумаги и иных канцелярских товаров. В то же время полностью исключить бумажный документооборот в ближайшей перспективе вряд ли удастся. Пример – запрос органа дознания, предварительного расследования, судебных органов в различные организации вне правоохранительной и судебной систем. В данном случае ответы на запросы должны быть отсканированы и приобщены к ЦУД.

3. Затруднение фальсификации уголовного дела со стороны сотрудника органа дознания или предварительного следствия.

Вряд ли является секретом, что нередки случаи, когда сотрудники органов дознания и предварительного расследования вносят изменения в уголовное дело по тем или иным причинам, подменяют материалы и т. п.

Например, как указывает профессиональный адвокат А.А. Суворов[5], нумерация УД должна производиться исключительно графитным карандашом. В то же время каждый, кто так или иначе вовлекался в сферу уголовного судопроизводства, обращал внимание, что нумерация страниц многократно меняется в ходе производства уголовного дела путем стирания ранее проведен-

[4] Право в цифре: какие разработки есть уже сейчас? // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/article/1554367/ (дата обращения 29.07.2023).

[5] Уголовное дело // Юридический кабинет Андрея Суворова. URL: https://suvorov.legal/ugolovnoe-delo/#Нумерация_уголовного_дела (дата обращения 29.07.2023).

ной нумерации (в некоторых случаях до дыр). С точки зрения законности данный вопрос законодательно не регламентируется. При этом, как представляется, все материалы уголовного дела, предоставленные для ознакомления участникам процесса, следует предъявлять исключительно пронумерованными носителем, который невозможно стереть либо вытравить, что исключает возможность замены страниц дела. Объясняется это прежде всего тем, что на практике следователи после ознакомления участников УП с материалами УД производят «чистку» ненужной для обвинения информации, содержащейся в деле, или, напротив, «наполнение» необходимыми (в ряде случаев и незаконно полученными) сведениями, о которых не следует знать участникам УП со стороны защиты в ходе предварительного расследования.

Проблему фальсификации в значительной степени можно решить автоматическим заполнением ряда полей ЦУД (наименование или код органа, возбудившего УД, наименование или код подразделения, номер дела, нумерация листов и т. д.), запретом изменения каждого материала (документа) ЦУД после его окончательного размещения путем программно-аппаратных, технических, организационных (например, правило трех и более лиц) и правовых мер. В качестве примера рассмотрим постановление о возбуждении уголовного дела. Когда следователь подготовил данный документ в текстовом редакторе и подписал своей электронной цифровой подписью (далее – ЭЦП), документ переводится в графическую форму, формируется хэш-функция (дайджест) документа и сохраняется в папке ресурсов данного ЦУД. Такие поля, как номер и дата постановления, номера листов, должны проставляться автоматически по заданной форме и в принятой системе кодирования.

Естественно, если уголовное дело или входящий в его состав документ изначально сфабрикованы, здесь трудно что-либо сделать. Только возбуждение нового уголовного дела по факту фальсификации.

Также должны быть приложены видео- и аудиозаписи процессуальных действий с их расшифровкой, где это возможно (например, протокол допроса и аудио- и/или видеозапись допроса). В этом случае аудио- и видеофайлы должны быть приложены к ЦУД с защитой от фальсификации.

4. Сокращение времени при знакомстве подследственных с материалами УД и существенное облегчение копирования материалов УД.

При наличии цифровой инфраструктуры уголовного процесса подследственный может ознакомиться с материалами своего

уголовного дела в месте содержания. Другие участники процесса также могут получить доступ к ЦУД у себя в кабинетах.

В целях защиты информации должны быть предусмотрены механизмы идентификации лиц, которые знакомятся с ЦУД, и фиксация данного факта, согласно требованиям документов ФСТЭК России.

Существенно облегчается копирование ЦУД или отдельных его частей. Возможно, потребуется необходимость создания некой первичной мастер-копии ЦУД, создаваемой инициатором. Права на копирование и сохранение ЦУД на компьютер участника процесса должно быть регламентировано и приняты меры по разграничению доступа и фиксации факта копирования.

Вопросы информационной безопасности и защиты информации ЦУД планируется рассмотреть в последующих публикациях.

Теперь перейдем к недостаткам.

1. Удорожание инфраструктуры, особенно на этапе внедрения.

Создание инфраструктуры цифрового УП потребует существенных капиталовложений. Сейчас информационные системы участников уголовного процесса разрозненны и соединяются через всемирную сеть Интернет, которая является средой «нулевого доверия». То есть обмен информацией с данными предварительного расследования без принятия мер защиты исключен. Кроме того, ряд уголовных дел может содержать сведения, составляющие государственную тайну.

Как вариант решения данной проблемы можно назвать создание единой закрытой информационной системы уголовного судопроизводства (наподобие ИСОД МВД России), куда будут включены сети органов предварительного расследования и дознания, судебных органов, а также подразделений судебно-медицинской экспертизы Минздрава России, ФМБА России и Минобороны России.

Другой вариант – использование соответствующих сервисов федеральных органов исполнительной власти и судебной системы и их объединение в подобие единой системы уголовного судопроизводства. Скорее всего, потребуется разработка таких сервисов, и возникнет необходимость согласования этих сервисов разных ведомств по различным параметрам (формат формализованных документов, протоколы обмена и ряд других).

Если рассматривать МВД России, то можно создать подобный сервис в системе ИСОД, где он может быть замкнут на многие прикладные сервисы системы, например СЦУО, «Следопыт-М», «Ксенон-2», ИБД-М, ЦИАДИС и др.

Потребуется закупка большого количества компьютеров, оргтехники, суперкомпьютеров, программно-аппаратных систем виртуализации и защиты информации, сетевых устройств и прочей техники.

Потребуется разработка формализованных электронных бланков различных процессуальных документов, соответствующего программного обеспечения, а также, возможно, протоколов передачи для сетевого обмена формализованными бланками между участниками процесса.

Также может возникнуть необходимость в оцифровке бумажных уголовных дел, находящихся в архивах, что потребует огромного количества ресурсов (временных, людских, финансовых, технических).

2. Вопросы, связанные с рядом процессуальных действий.

Здесь существует ряд проблем, требующих технических, организационных и правовых решений.

И первая проблема, которую следует отметить, состоит в разработке и оформлении ряда процессуальных документов. Если с оформлением таких документов, как постановления, поручения органам дознания, экспертно-криминалистическим подразделениям, запросы и т. п., особых проблем не возникнет – автор документа и/или вышестоящее должностное лицо подписывает документ своей усиленной ЭЦП, то при производстве обыска, выемки, осмотра места происшествия, допроса, очной ставки такие участники следственных действий, как понятые, свидетели, подозреваемые, подследственные, в подавляющем большинстве случаев ЭЦП не имеют. Обязать же граждан иметь ЭЦП не является решением проблемы, так как криптоконтейнер может быть утерян, похищен, выброшен, случайно поврежден или умышленно уничтожен.

Существует, по крайней мере, три варианта решения данной проблемы:

– формирование временной ЭЦП понятого, допрашиваемого или иного лица, не имеющего усиленной ЭЦП, с хранением криптоконтейнера на сервере (облаке) системы электронного уголовного судопроизводства с фиксацией данного действия на видео или без такового;
– использование графических планшетов с вводом ручной подписи в персональный компьютер;
– использование квазистабильных биометрических характеристик участников уголовного процесса (рисунки папиллярных узоров пальцев рук, радужной оболочки или сетчатки глаза).

У этих вариантов есть свои преимущества и недостатки, как в техническом, так и в процессуальном плане.

Еще одна проблема связана с хранением вещественных доказательств при УД. Как справедливо отмечает профессор Л.В. Головко [Головко 2019], можно перевести материальные объекты в 3D-форму и разметить с ЦУД, но что делать со следами, например, пальцев рук на носителе или с генетическим материалом на предмете (кровь, слюна и т. д.)? Они могут понадобиться для проведения повторных экспертиз. И это действительно серьезная проблема с точки зрения процессуального законодательства. С другой стороны, такие вещественные доказательства можно хранить в отдельных условиях в отдельных хранилищах, так же как, например, оружие, как указано в подп. «а» п. 1 ч. 2 ст. 82 УПК РФ или п. 3 Правил хранения, учета и передачи вещественных доказательств по уголовным делам[6]. Для этого необходимо принятие соответствующих нормативных правовых актов и соответствующее финансирование выделения (постройки, расширения) специализированных помещений, что представляет собой отдельную проблему.

Опять же, как утверждает профессор Л.В. Головко [Головко 2019], при передаче ЦУД в суд одна, цифровая, часть поступает в суд практически мгновенно, другая (вещественные доказательства) спустя какое-то время. Возникает вопрос. В какой момент дело считается поступившим в суд? С какого момента отсчитываются сроки? Как отмечает профессор Л.В. Головко, ориентироваться придется на материальную часть ЦУД. Однако авторы данной статьи не согласны с профессором Л.В. Головко, что это снижает все достоинства цифровизации УП. С нашей точки зрения, снижение будет незначительное. Однако данный вопрос носит дискуссионный характер.

Опять-таки специалисты по уголовному процессу [Зуев 2018; Головко 2019; Носко 2023] критикуют дистанционную подачу заявлений о преступлении, допрос или очную ставку с применением систем видеоконференцсвязи, и аргументы их совершенно справедливы. С другой стороны, допрос или подача заявления в кабинете следователя никоим образом не влияет на цифровизацию УД.

Также необходимо вести учет вещественных доказательств. Сотрудники ФКУ НПО «Специальная техника и связь» МВД России И.А. Кубасов, А.В. Калугин, С.А Крючков и Ю.А. Волобринская [Кубасов, Калугин, Крючков, Волобринская 2021] предлагают в

[6] Постановление Правительства РФ от 8 мая 2015 г. № 449 «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам» // Информационно-правовой портал ГАРАНТ.РУ. URL: https://base.garant.ru/71018836/#block_1000 (дата обращения 29.07.2023).

ИСОД МВД России создать сервис по сквозному автоматизированному учету вещественных доказательств.

3. Психологические проблемы с точки зрения восприятия ЦУД участниками процесса.

Здесь возникают проблемы, связанные, с одной стороны, с возможной угрозой разрушения стереотипного восприятия процессуальных действий. С точки зрения профессора С.В. Зуева [Зуев 2018], «оперирование электронной (цифровой) информацией не вполне вписывается в традиционную систему следственных действий».

С другой стороны, недоверие людей к цифровому пространству. Это связано с периодически появляющимися в средствах массовой информации сообщениях об утечке персональных данных клиентов различных организаций, включая банки. А в данном случае речь идет о тайне следствия и судопроизводства. Психологию человека изменить сложно, однако данная проблема решается ужесточением ответственности за передачу информации лицам, не имеющим права доступа к ней, и применением технических средств защиты информации от утечки, например DLP-систем, технических средств и систем защиты информации от утечки по ПЭМИН[7].

По данным аналитического отчета компании InfoWatch, большая часть утечек происходит по вине персонала компании[8]. Однако с 2018 г. в России неуклонно растет доля утечек информации по вине внешних нарушителей. Вместе с тем, как утверждают эксперты InfoWatch некоторое время назад, исследование утечек по вектору воздействия все сложнее проводить по общепринятым критериям – внешний/внутренний. Появилось все больше утечек, где на основе найденных сведений определить вектор воздействия было затруднительно. Особенно это касается утечек 2021 и 2022 гг. В ряде случаев имеющиеся сведения указывали на то, что на конфиденциальные данные той или иной организации нарушители воздействовали как изнутри, так и снаружи информационного контура, т. е. находились в сговоре. В исследование был введен новый термин – «гибридный вектор утечки». Распределение утечек по вектору воздействия показано на рис. 1.

В 2017–2021 гг. доля неопределенных случаев утечек не превышала 5%.

---

[7] ПЭМИН – побочные электромагнитные излучения и наводки.

[8] Россия: утечки информации ограниченного доступа в 2022 г.: Аналитический отчет. Экспертно-аналитический центр InfoWatch. М., 2023. 24 с.

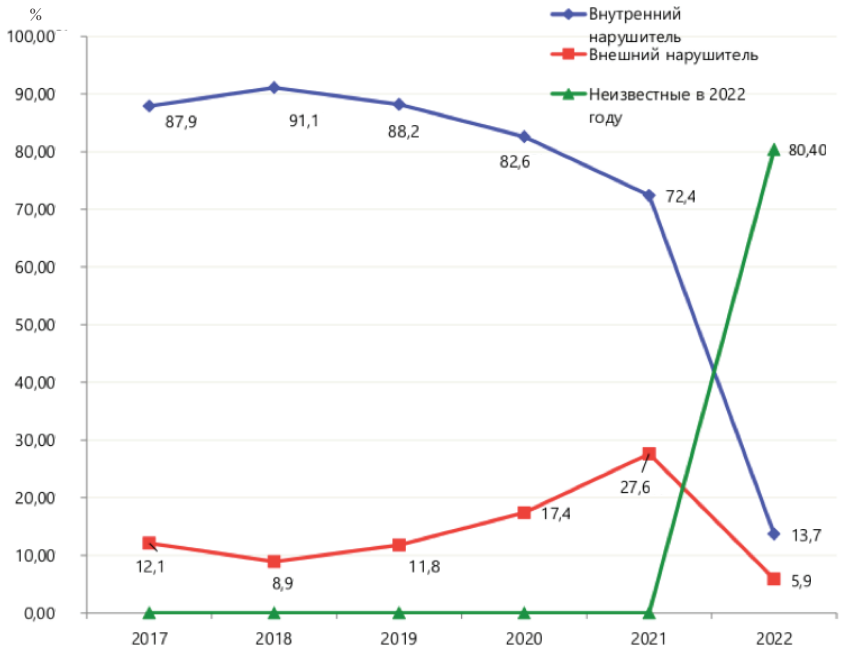

Рис. 1. Распределение утечек информации по вектору воздействия (внешний/внутренний), %: Россия[9]

Атаки на объекты критической информационной инфраструктуры и федеральные органы исполнительной власти России были и будут, их воздействие будет усиливаться.

С другой стороны, утечка информации возможна и с бумажного носителя, если недобросовестный следователь произведет копирование или фотографирование материалов УД с целью передачи информации заинтересованным лицам. С применением механизмов защиты информации это сделать будет сложнее.

Еще один аспект психологических проблем связан с верой в то, что уничтожить информацию в информационных системах гораздо легче, чем на бумаге. Как говорится, бумага надежнее и горит легче. Однако это тоже весьма спорный вопрос. Естественно, для чтения документа на бумаге не нужны электронные устройства, в то же время хранение информации в информационных системах представляется более надежным (при соблюдении определенных правил).

[9] Россия: утечки информации ограниченного доступа в 2022 г.

4. Кадровые проблемы.

Кадровые проблемы при цифровизации УД можно также рассматривать в нескольких аспектах.

Первый аспект связан с подготовкой новых и переобучением существующих сотрудников–участников УП. Как показывает практика, в том числе личная авторов, люди далеко не всегда горят желанием усваивать что-либо новое. Чем старше человек, тем сложнее ему переобучаться. Потребуется освоение новых программных продуктов, переход на отечественные операционные системы, которые отличаются от привычной многим линейки *Windows*. Кроме того, потребуется обучение сотрудников не просто основам информационной безопасности, но и более углубленное изучение вопросов первоначального реагирования на различные компьютерные атаки, в первую очередь связанные с фишингом и иными атаками социальной инженерии. Это обучение должно носить периодический характер.

Еще один аспект связан с профессионализмом лиц, ведущих расследование. В 2016 г. В.В. Зозуля [Зозуля 2016] предлагал на законодательном уровне предусмотреть возможность осуществления видеозаписи при проведении следственных действий с автоматической системой видеозаписи в служебных помещениях органов предварительного расследования в уведомительном порядке. Таким образом, при проведении и видеофиксации ряда следственных действий (допрос, очная ставка и т. д.) на видеозаписи будут наглядно видны все ошибки и промахи лица, проводящего следственные действия.

Рассмотрим еще два недостатка, сформулированных профессором С.В. Зуевым.

5. Сложность в обеспечении информационной безопасности.

На самом деле «сложность» весьма относительна. Защиту информации придется обеспечивать в любом случае, ибо этого требуют регуляторы и здравый смысл. В ряде случаев, а цифровизация УД относится именно к ним, необходимо выполнять требования регуляторов по защите информации.

Стоимость защиты информации различается в зависимости от вида информации, степени ее чувствительности и ценности для владельца, обязанности внедрять те или иные средства защиты информации и т. д. По данным SecurityLab.ru[10], разброс на защиту

[10] Каким должен быть процент на ИБ от ИТ-бюджета? // SecurityLab.ru. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/282933.php (дата обращения 29.07.2023).

информации значительный: от 4,3 до 13% от ИТ-бюджета организации – 39% организаций тратят от 6 до 10% на соблюдение правил безопасности; еще 39% организаций тратят от 11 до 15%; 11% – от 16 до 20% и 7% – от 21 до 25% своего ИТ-бюджета. Как отмечает ресурс Security Forward[11], среднестатистический бизнес инвестирует в кибербезопасность от 6 до 14% своего годового ИТ-бюджета. Это составляет менее четверти от общего бюджета, выделяемого на кибербезопасность в целом. Большинство компаний тратят в среднем около 10% своего ИТ-бюджета. Похожие цифры приводит ресурс Netsurion[12] – в среднем уровень расходов на обеспечение безопасности в размере 3–6% от общего ИТ-бюджета считается нормой. Если добавить расходы на обеспечение соответствия требованиям в рамках обеспечения безопасности, это составит еще 3–6% от ИТ-бюджета. Если учесть расходы на обеспечение непрерывности бизнеса, то это еще 2%, в результате чего они составят 10–14% от общего ИТ-бюджета организации. Необходимо отметить, что требования отечественного регулятора в области защиты информации жестче требований европейского [Mityushin 2021].

По мнению авторов данной статьи, затраты на защиту информации, составляющей государственную тайну могут достигать 50% и более от ИТ-бюджета организации.

Одной из проблем защиты информации является отсутствие тех или иных программно-аппаратных и технических средств защиты информации вендоров, которые ушли с российского рынка из-за начала Россией специальной военной операции. Для цифровизации уголовного процесса и обработки большого объема информации, интеграции разных министерств и ведомств, реализации технических мер защиты в режиме реального времени требуются защищенные высокопроизводительные вычислительные национальные системы.

6. Возможность фальсификации информации следователем.

Об этом было сказано чуть выше. Если УД сфабриковано изначально, тут что-либо сделать тяжело. Однако после того, как процессуальное лицо сформировало документ и подписало его своей

[11] How Much Do Companies Spend On Cybersecurity? // Security Forward. URL: https://www.securityforward.com/how-much-do-companies-spend-on-cybersecurity/ (дата обращения 29.07.2023).

[12] IT Security: How Much Should You Spend? // Netsurion. URL: https://www.netsurion.com/articles/it-security-how-much-should-you-spend (дата обращения 29.07.2023).

ЭЦП, с помощью технических и организационных мер защиты возможность фальсификации ЦУД можно практически полностью исключить.

Особенности информационной инфраструктуры

Как уже отмечалось выше, потребуется необходимость создания прикладных сервисов в имеющихся информационных системах ведомств с тесной интеграцией ведомственных сервисов между собой либо создание единого цифрового пространства системы уголовного судопроизводства. В данном случае к этой системе будут подключаться различные сервисы ведомственных информационно-аналитических систем.

По большому счету придется объединить в единый суперкластер ряд прикладных сервисов информационно-аналитических систем СК России, ФСБ России, МВД России, ФССП России, ФСИН России, ФПС ГПС МЧС России, ФТС России, Прокуратуры РФ, Судебной системы Российской Федерации, военной полиции Минобороны России, подразделений судебно-медицинской экспертизы Минздрава России, ФМБА России и Минобороны России. Здесь возможен ряд проблем организационного плана и вопросов межведомственного взаимодействия.

Также необходимо отметить, что с учетом развития вычислительной техники и технологий проектирования мы переходим от изучения традиционных информационных систем персонального пользования, мейнфреймов, кластеров к исследованию суперкластеров с рекордно высокими показателями производительности. Сегодня области приложений суперкомпьютерной техники в России, США, Канаде, Германии, Франции, Китае, Японии и ряде ведущих зарубежных стран значительно расширились.

Однако в России в настоящее время отечественные суперкомпьютеры серийно не производятся. Различными предприятиями ведутся работы по созданию и поставкам вычислительных систем кластерного типа высокой производительности, основу которых составляют коммерчески доступные компоненты и сборочные единицы импортного производства. Их отставание от заказных систем, создаваемых за рубежом, по производительности и защищенности на несколько порядков ниже.

На сегодняшний день разработка и сертификация систем защиты информации в суперкомпьютерных вычислительных системах носит ненормированный характер из-за отсутствия стандартов на ее

использование. Существующие и успешно внедренные программно-технические решения промышленного комплекса России не учитывают специфики суперкомпьютеров с позиции безопасности в виде дополнительных проблем управления доступом с учетом параллелизма и новых угроз. Данная проблема постепенно решается.

Необходима реализация и исполнение очень жестких требований по разграничению доступа субъектов к информационным ресурсам.

Информационная система должна работать с использованием облачных технологий, технологий распределенного реестра, возможно, системы виртуальных рабочих столов и ряда других технологий защиты информации.

Целесообразно разработку проводить с использованием инженерно-организационного подхода, реализующего продуктивное сотрудничество между командами разработки, безопасности и эксплуатации DevSecOps.

Заключение

Задача по переводу уголовных дел полностью в цифровую форму весьма сложна и многофакторна. У цифрового уголовного дела по сравнению с традиционным («бумажным») имеется целый ряд преимуществ, имеются и недостатки. В то же время процесс цифровой трансформации общества идет вперед, и возможно, что такая консервативная область, как уголовное судопроизводство, также со временем «оцифруется».

На пути этой трансформации стоит много проблем и задач технического, организационного, человеческого, нравственно-психологического плана, и одна из самых сложных – вопросы межведомственного взаимодействия.

В то же время, по мнению авторов, данные вопросы со временем могут быть решены совместной работой как специалистов в области ИТ-технологий, информационной безопасности и других технических специальностей, так и специалистов в области уголовного процесса, судебной экспертизы, уголовного права и других научных специальностей правового блока.

Литература

Головко 2019 – *Головко Л.В.* Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25.

Зозуля 2016 – *Зозуля В.В.* К вопросу о применении видеозаписи при производстве следственных действий с участием несовершеннолетних // Уголовно-процессуальная охрана прав и законных интересов несовершеннолетних. 2016. № 1 (3). С. 47–51.

Зуев 2018 – *Зуев С.В.* Электронное уголовное дело: за и против // Правопорядок: история, теория и практика. 2018. № 4 (19). С. 6–12.

Зуев, Титова 2019 – *Зуев С.В.*, *Титова А.С.* Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства // Правопорядок: история, теория, практика. 2019. № 1. С. 49–54.

Конин 2021 – *Конин В.В.* Термин «уголовное дело»: что под этим следует понимать? // Современное право. 2021. № 8. С. 114–118.

Конин, Кудрявцева, Петров 2022 – *Конин В.В.*, *Кудрявцева А.В.*, *Петров А.В.* Уголовное дело – переход от бумажного носителя в цифровой формат // Вестник Томского государственного университета. Право. 2022. № 45. С. 81–99. DOI: 10.17223/22253513/45/6.

Кубасов, Калугин, Крючков, Волобринская 2021 – *Кубасов И.А., Калугин А.В., Крючков С.А., Волобринская Ю.А.* Создание сервиса ИСОД МВД России учета вещественных доказательств // Академическая мысль. 2021. № 3 (16). С. 79–83.

Миронова 2023 – *Миронова Е.Ю.* Нравственные начала уголовного процесса в условиях цифровизации: принципиальная незыблемость или неизбежная трансформация // Актуальные проблемы российского права. 2023. Т. 18. № 1. С. 136–149. DOI: 10.17803/1994-1471.2023.146.1.136-149.

Носко 2023 – *Носко П.В.* Перспективы внедрения цифровых технологий в уголовный процесс: какие проблемы могут возникнуть? // Юриспруденция в современном обществе: проблемы регулирования правовых отношений: Сб. ст. Международной научно-практической конференции. Пенза, 2023. С. 82–89.

Супрун, Ганболд 2019 – *Супрун С.В.*, *Ганболд Р.* Предварительное расследование России и Монголии: актуальные проблемы определения содержания понятий «дознанное дело», «уголовное дело», «уголовное преследование», «прекращение уголовного дела» // Вестник Санкт-Петербургского университета МВД России. 2019. № 4 (84). С. 137–145.

Янушко, Бабанин, Кузнецова, Петрушенко, Чекмарев 2011 – *Янушко А.В.*, *Бабанин А.В.*, *Кузнецова О.А.*, *Петрушенко С.В.*, *Чекмарев М.Ю.* Защищенный аппаратно-программный комплекс центра хранения электронных копий материалов уголовных дел // Безопасность информационных технологий. 2011. № 1. Т. 18. С. 21–29

Mityushin 2021 – *Mityushin D.A.* Issues and possibilities of personal data remote processing in the COVID19 Pandemic nvironment // Lecture Notes in Networks and Systems. 2021. Vol. 232. P. 86–94.

References

Golovko, L.V. (2019), "The digitalization in criminal procedure. A local optimization or the global revolution", *Vestnik ekonomicheskoj bezopasnosti*, no. 1, pp. 15–25.

Konin, V.V. (2021), "The term "criminal case". What should be understood by it?", *Sovremennoe pravo*, no. 8, pp. 114–118.

Konin, V.V., Kudryavtseva, A.V. and Petrov, A.V. (2022), "Criminal case – transition from paper to digital format", *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo*, *Tomsk State University Journal of Law*, no. 45. pp. 88–99, DOI: 10.17223/22253513/45/6.

Kubasov, I.A, Kalugin, A.V., Kryuchkov, S.A. and Volobrinskaya, Yu.A. (2021), "Creation of ISOD Ministry of Internal Affairs of the Russian Federation service of accounting of physical evidence", *Akademicheskaya mysl'*, no. 3 (16), pp. 79–83.

Mironova, E.Yu. (2023), "Moral Principles of the Criminal Procedure in the context of Digitalization: Fundamental Inviolability or Inevitable Transformation", *Aktual'nye problemy rossiiskogo prava*, no. 18 (1), pp. 136–149. DOI: 10.17803/1994-1471.2023.146.1.136-149.

Mityushin, D.A. (2021), "Issues and possibilities of personal data remote processing in the COVID19 Pandemic environment", *Lecture Notes in Networks and Systems*, vol. 232, pp. 86–94.

Nosko, P.V. (2023), "Prospects for the introduction of digital technologies in criminal proceedings: What problems may arise?", *Yurisprudentsiya v sovremennom obshchestve: problemy regulirovaniya pravovyh otnoshenii. Sbornik statei Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Jurisprudence in modern society. Issues of the legal relations regulation. Collection of articles of the International scientific and practical conference], Penza, Russia, pp. 82–89.

Suprun, S.V. and Ganbold, R. (2019), "Preliminary investigation of Russia and Mongolia. current issues in defining the content of concepts 'investigated case', 'criminal case', 'criminal prosecution', 'termination of criminal proceedings' ", *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii – Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia*, no. 4 (84), pp. 137–145, DOI: 10.35750/20718284-2019-4-137-145.

Yanusko, A.V., Babanin, A.V., Kuznetsova, O.A., Petrushenko, S.V. and Chekmaryov, M.Y. (2011), "Protected hardware and software complex of the center for storing electronic copies of criminal case files", *Bezopasnost' Informatsionnykh Tekhnologii*, no. 1, vol. 18, pp. 21–29.

Zozulya, V.V. (2016), "On the use of videotaping in investigative actions involving minors", *Ugolovno-protsessualnaya okhrana prav i zakonnykh interesov nesovershennoletnikh*, no. 1 (3), pp. 47–51.

Zuev, S.V. (2018), "Weakness of the information approach in the light of digitalization of criminal proceedings", *Legal order. History, theory, practice*, no. 1, pp. 49–54.

Zuev, S.V. and Titova, A.S. (2019), "Electronic criminal case. Pros and cons", *Legal order. History, theory, practice*, no. 1, pp. 49–54.

Информация об авторах

Дмитрий А. Митюшин, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; dalexx@inbox.ru

Андрей С. Моляков, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; andrei_molyakov@mail.ru

Information about the authors

Dmitrii A. Mityushin, Cand. of Sci. (Computer Science), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; dalexx@inbox.ru

Andrei S. Molyakov, Cand. of Sci. (Computer Science), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; andrei_molyakov@mail.ru

УДК 004.42
DOI: 10.28995/2686-679X-2023-4-47-69

Разработка алгоритма распознавания изображения посредством комбинации алгоритмов поиска по форме и текстуре

Марина С. Шаповалова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, mshapovalova84@gmail.com

Илья Ю. Елгин
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, ilia.elgin@yandex.ru

Аннотация. В статье рассматриваются методы распознавания изображения по контуру, по выделению цветовых характеристик объекта и распознавания объекта с различных ракурсов. Каждый из этих методов имеет свои особенности реализации, преимущества и недостатки. В работе рассмотрен метод поиска по форме и текстурным характеристикам посредством анализа Тамура, таких как гистограммы отдельных цветов и глубина текстуры. Также рассмотрен алгоритм получения дескрипторов Фурье, который позволяет сопоставить формы областей методами сопоставления графов.

Для описания контура изображения при выделении объекта из фона применяется Грид-метод, который позволяет определить контур изображения, а затем выполнить поиск по этому контуру, сопоставив его с эталоном. В работе реализован поиск изображения по всем трем параметрам одновременно за счет комбинации описанных выше методов при уменьшении ошибок при работе алгоритма. Данный метод не будет зависеть от ракурса исходного и распознаваемого изображений, от разницы качества съемки исходного и распознаваемого изображений. Алгоритм поиска по изображению предполагает сравнение искомого изображения с эталонами, которые хранятся в базе данных. Сопоставление с эталоном производится за счет определения характеристик, присущих товару или группе товаров. В работе приведено исследование устойчивости к ошибкам предлагаемого метода, корректности распознавания им изображений, а также рассмотрено его быстродействие.

Ключевые слова: анализ Тамура, дескриптор Фурье, Грид-метод, распознавание изображений, распознавание по фото

Для цитирования: *Шаповалова М.С., Елгин И.Ю.* Разработка алгоритма распознавания изображения посредством комбинации алгоритмов поиска по форме и текстуре // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 47–69. DOI: 10.28995/2686-679X-2023-4-47-69

Development of an image recognition algorithm through a combination of shape and texture search algorithms

Marina S. Shapovalova
Bauman Moscow State Technical University, Moscow, Russia,
mshapovalova84@gmail.com

Il'ya Yu. Elgin
Bauman Moscow State Technical University, Moscow, Russia,
ilia.elgin@yandex.ru

Abstract. The article discusses image's recognizing methods by a contour, for an object's color characteristics highlighting, and object's recognizing by an various angles. Each of these methods has its own implementation features, advantages and disadvantages. The paper considers a search method for shape and texture characteristics through Tamura analysis, such as histograms of individual colors and texture depth. An algorithm is also considered for obtaining Fourier descriptors, which allows you to match the shapes of areas using graph matching methods. To describe the image's contour when selecting an object from the background, the Grid method is used. This method allows you determination the image's contour, and then search for this contour, comparing it with the standard. The Grid method is used to describe the image's outline with it's selection from the background.

The work implements an image search for all three parameters simultaneously during to a methods combination that described above for errors reducing in the algorithm. This method will not depend on the original and recognized images angle, on the shooting quality difference between the original and recognized images. The image searching algorithm involves comparing the image with the samples, that stored in the database. Comparison with the sample can be made with determining the characteristics inherent in the product or products' group.

The paper presents of the resistance to errors study to the proposed method, the correctness of image's recognition by it and also considers its speed. The article considers image's recognizing methods by a contour, by an object's color characteristics highlighting, and object's recognizing from various angles. Each of these methods has its own implementation features, advantages and disad-

vantages. The paper considers a search method for shape and texture characteristics through Tamura analysis, such as histograms of individual colors and texture depth. An algorithm is also considered for obtaining Fourier descriptors, which allows matching the shapes of areas by graph matching methods. To describe the image's contour when selecting an object from the background, the Grid method is used allowing to determin**e** the image's contour and then search for this contour, comparing it with the standard. In the paper, an image search using all the three parameters simultaneously is realized by combining the methods described above while reducing the errors in the algorithm. Such a method will not depend on the original and recognized images angle, on the shooting quality difference between the original and recognized images. The image searching algorithm involves comparing the image with the reference standards stored in the database. Benchmarking is done by identifying the characteristics inherent in the product or products' group

The paper presents a study in the resistance to errors of the proposed method, in the correctness of image's recognition by it and also considers its processing speed.

Keywords: Tamura analysis, Fourier descriptor, Grid method, image recognition, photo recognition

For citation: Shapovalova, M.S. and Elgin, I.Yu. (2023), "Development of an image recognition algorithm through a combination of shape and texture search algorithms", *RSUH/RGGU Bulletin. "Computer Sience. Informaton security. Mathematics" Series*, no. 4, pp. 47–69, DOI: 10.28995/2686-679X-2023-4-47-69

Введение

В настоящее время большой популярностью пользуются интернет-магазины, которые являются распространенным способом покупки одежды для многих потребителей. Их ассортимент может быть очень большим, поэтому возникает потребность в поиске нужного товара среди всех предложений. Часто возникают ситуации, когда покупатели не знают точного названия товара, который они хотели бы приобрести, однако у них есть примерное или точное изображение искомого товара, например, когда такая вещь у них уже есть или существует ее визуальный концепт. Для упрощения поиска товаров в данном случае используется поиск товаров по изображению.

Поиск по изображению – это технология, которая позволяет найти изображения, схожие с изображением, предоставленным пользователем. Данный вид поиска использует цифровые изображения вместо словесных описаний. С помощью данной технологии

можно осуществить поиск товаров, основываясь на изображениях самих товаров [Волосатова 2021][1].

Сервис поиска одежды и вещей по изображению предоставляют такие интернет-площадки, как Wildberries, Beagle, Aliexpress и др. Такой подход позволяет покупателю быстро найти нужный товар, не тратя время на поиск по текстовым описаниям, а также уменьшить вероятность ошибки при выборе товара.

Товар, размещенный в интернет-магазине, имеет одно или несколько изображений. В случае наличия нескольких изображений они демонстрируют товар с разных ракурсов. Данные изображения продавцы стараются делать в большом разрешении, чтобы были видны мелкие детали товаров. Товары размещаются в центре изображения, съемка производится при хорошем освещении товара ровным белым светом на однотонном контрастном фоне. При поиске изображений нужно проводить сравнения со всеми изображениями товара, так как под разными углами форма и текстура товара на изображении могут отличаться. Также нужно учитывать, что изображение, предоставляемое пользователем, может иметь меньшее разрешение, быть не таким контрастным или с чуть иным цветом вследствие освещения, чем изображение товара на сайте.

При поиске по изображению система использует алгоритмы компьютерного зрения для анализа основных характеристик изображения, таких как цвет, форма объектов изображения, текстура, происходит поиск в базе данных с использованием этих характеристик для сопоставления товаров. Важным фактором при поиске товаров по изображению является его разрешение. Кроме того, системы поиска могут использовать несколько изображений товаров для улучшения его точности[2].

Поиск товаров по изображению осуществляется на основе распознавания основных характеристик товара, таких как форма, цвет, текстура, как для всего изображения товара, так и для отдельных его областей. Технологии машинного обучения позволяют определить значимость этих характеристик, определить наиболее значимые из них, затем произвести поиск по всему ассортименту.

По изображению одежды можно определить ее следующие характеристики:

---

[1] *Крайнов А., Штуркин Н.* Технология поиска похожих изображений // Блог Яндекса, 20.10.2010. URL: https://yandex.ru/blog/company/30316 (дата обращения 10.04.2023).

[2] *Табатчикова Е.* Сервисы распознавания одежды по фото в Яндекс Маркете, «Вайлдберриз», «Ламоде» // Тинькофф журнал, 27.07.2020. URL: https://journal.tinkoff.ru/list/shmotka-po-fotke/ (дата обращения 20.04.2023).

– вид – изображение позволяет определить тип одежды по форме товара или по его составным частям;
– цвет – нужный оттенок цвета одежды;
– детали – рисунок/принт, вышивка, карманы, пуговицы и др., определяют по текстуре товара и отдельных его частей;
– ткань – материал, из которого сделана одежда, определяется по текстуре;
– стиль – по изображению можно судить о стиле одежды, определяется по форме, текстуре, цвету товара и его составных объектов, а также их взаимному расположению. Например, верхняя одежда (пальто, плащ, куртка), брюки (джинсы, брюки, шорты) и т. д.;
– форма и силуэт – изображение может показать, как одежда выглядит на модели, и определить форму и силуэт изделия.

Выделение объектов изображения будет производиться на основе их формы. Выделяются их контуры, после чего область изображения, имеющую замкнутый контур, считается отдельным объектом. Для определения цветовых характеристик объекта воспользуемся методом гистограмм, для каждой цветовой составляющей будет строиться гистограмма. Текстурные характеристики будут определяться анализом Тамура[3].

Для определения более сложных элементов текстуры данные способы будут применяться несколько раз с уменьшением размера области анализа текстуры в два раза.

Представим форму объекта как набор последовательных двумерных векторов с определенной длиной. При работе с длинами не будем учитывать направление вектора, представляя его в виде отрезка. Образующий форму угол между текущим и предыдущим отрезком будет углом вектора, а длина вектора – длина отрезка, деленная на минимальное расстояние от центра объекта до точек его контура. Для упрощения хранения и сравнения характеристик формы воспользуемся преобразованием Фурье, которое преобразует изображение в частотную область по формуле (1).

$$F(u,v) = \sum_{x=1}^{M} \sum_{y=1}^{N} f(x,y) e^{-j \cdot 2\pi \left(\frac{v \cdot u}{M} + \frac{u \cdot x}{N}\right)}, \quad (1)$$

где $f(x, y)$ – значение яркости цвета пикселя, M, N – размеры изображения.

[3] *Табатчикова Е.* Указ. соч.

Также вычисляется энтропический центр Фурье по формуле (2).

$$E(u, v) = R^2(u, v) + I^2(u, v), \quad (2)$$

где $R(u, v)$ и $I(u, v)$ являются действительной и мнимой частями соответственно.

Для разделения энергетического спектра Фурье использовались несколько прямоугольных колец разных размеров, но одинаковой формы. Далее определяется *FSEP* по формуле (3).

$$\text{FSEP} = \frac{E_{\text{cen}}}{\sum_{u=0}^{M} \sum_{v=0}^{N} E(u, v)}, \quad (3)$$

где E_{cen} – энергия центрального кольца. Уровни *FSEP* можно сравнить[4].

Структурное описание формы, как правило, представляет собой реляционный граф, поэтому для сопоставления описаний формы используются методы сопоставления графов. Сопоставление формы областей методами сопоставления графов является весомым преимуществом, поскольку описание обычно включает в себя пространственные отношения, инвариантные относительно большинства двумерных преобразований. Однако недостатком такого подхода является то, что сопоставление графов выполняется очень медленно, поскольку временные затраты растут экспоненциально с увеличением количества элементов[5].

Алгоритм получения дескрипторов Фурье:

– найти центр масс фигуры;
– для каждого угла задать длину вектора от центра до точки пересечения с контуром;
– получится одномерная функция, которую можно разложить по базису Фурье, посчитать коэффициенты Фурье, взять в качестве элементов вектора признаков [Фурман 2003].

---

[4] *Хасан А.А.* Реализация преобразования Фурье для фильтрации изображений // Современные концепции развития науки: Сб. ст. Международной научно-практической конференции 16 марта 2018 г. Ч. 1. Пермь: МЦИИ Омега Сайнс, 2018. С. 72–75. URL: https://os-russia.com/SBORNIKI/KON-200-1.pdf (дата обращения 20.04.2023).

[5] *Живрин Я.Э., Алкзир Н.Б.* Методы определения объектов на изображениях // Молодой ученый. 2018. № 7 (193). С. 8–19. URL: https://moluch.ru/archive/193/48447/ (дата обращения 20.04.2023).

Также применяется Грид-метод для описания контура. Он состоит из двух этапов:

– наложение сетки на изображение;
– формирование вектора признаков из 1 и 0 в зависимости от того, пересекает ли область клеточку или нет.

Чтобы добиться инвариантности, нормализуем изображение вдоль главной оси. Таким образом добиваемся инвариантности относительно поворота и масштаба.

Инвариантные моменты – это математический способ описания формы объекта. Существует такое понятие, как моменты двумерных непрерывных функций, которые вычисляются по формулам (4–5):

– момент порядка $(+q)$ двумерной непрерывной функции:

$$m_{pq} = \iint x^p y^q f(x, y)\, dx \cdot dy; \qquad (4)$$

– центральные моменты для (x, y) – дискретного изображения:

$$m_{pq} = \sum_x \sum_y \left(x - \frac{m_{\backslash 1 \backslash 0}}{m_{\backslash 0 \backslash 0}} \right)^p \cdot \left(y - \frac{m_{\backslash 0 \backslash 1}}{m_{\backslash 0 \backslash 0}} \right)^q. \qquad (5)^6$$

С использованием нормированных центральных моментов был выделен набор из семи инвариантных к параллельному переносу, повороту и изменению масштаба, на основе их формируется вектор признаков[7].

Метод поиска, основанный на форме объектов изображения, дает возможность определения самих объектов. Данный метод устойчив к параллельному переносу, изменению масштаба и повороту объектов, на его работу не влияют незначительные изменения освещения. Однако в методе поиска по форме не учитывается положение объектов относительно друг друга и объекты схожие по форме, но разные по своей природе могут восприниматься как идентичные.

Метод Тамура описывает шесть атрибутов характеристик текстуры: контрастность, шероховатость или зернистость, направленность, регулярность и линейность.

---

[6] *Горев А.Ю., Шлеймович М.П., Юдинцева А.О.* Контекстный поиск изображения в web-системах // Вестник Казанского технического университета. 2014. Т. 17. № 19. С. 377–380. URL: https://cyberleninka.ru/article/n/kontekstnyy-poisk-izobrazheniy-v-web-sistemah (дата обращения 20.04.2023).

[7] *Хасан А.А.* Указ. соч.

Для этого вычисляется среднее значение по соседним пикселям с размером окрестности, кратным степени 2: 1×1, 2×2, 32×32 по формуле (6).

$$A_{k(x,y)} = \frac{1}{2^{2k}} \sum_{i=x-2^{2k-1}}^{x+2^{2k-1}-1} \sum_{j=y-2^{2k-1}}^{y+2^{2k-1}-1} f(x,y), \quad (6)$$

где $f(x, y)$ – яркость пикселя[8].

Для каждой точки вычисляется разность между средними значениями и непересекающихся окрестностей в горизонтальном и вертикальном направлениях по формуле (7).

$$E_{k,h}(x, y) = |A_k(x + 2^{k-1}, y) - A_k(x - 2^{k-1}, y)|. \quad (7)[9]$$

Для каждой точки вычисляется лучшее значение размера окрестности по формуле (8).

$$S_{\text{best}} = 2^k, \quad (8)$$

где k максимизирует энергию в обоих направлениях[10].

Вычисляется среднее значение по формуле (9).

$$F_{\text{coa}} = \frac{1}{\text{MN}} \sum_{i}^{M} \sum_{j}^{N} S_{\text{best}}(i,j). \quad (9)[11]$$

Направленность определяет общее направление в изображении или производные между различными ориентациями или паттернами. Вычисляется по формуле (10).

$$F_{\text{dir}} = 1 - r \cdot n_p \cdot \sum_{p}^{N_p} \sum_{\varphi \in W_p} (\varphi - \varphi_p)^2 H_D(\varphi), \quad (10)$$

где M × N – размерность исходного изображения[12].

---

[8] *Хасан А.А., Титов В.С., Панищева О.Н.* Параллельный алгоритм вычисления характеристик текстур на изображениях // Интеллектуальные и информационные системы: Сб. матер. Всероссийской научно-технической конференции. Тула, 2019. С. 24–28. URL: https://www.elibrary.ru/item.asp?id=41345614 (дата обращения 20.04.2023).

[9] Там же.

[10] Там же.

[11] Там же.

[12] Там же.

Контрастность определяет разность интенсивностей соседних пикселей, на этот параметр влияет динамика изменения яркости на изображении, поляризация распределений черного и белого цветов и четкость границ. Вычисляется по формуле (11).

$$F_{\text{con}} = \frac{\sigma}{\sqrt[4]{\frac{\mu_4}{\sigma^4}}}, \quad (11)$$

где μ_4 обозначает четвертый момент, а σ обозначает дисперсию [Болотова 2016].

Для нашей задачи подойдут два способа определения значимости критериев.

Первый способ основан на разбиении всех товаров по группам. Для группы определяется значимость каждого из критериев. Товар на пользовательском изображении по каким-либо шаблонным критериям относится к одной из групп. Значимость критериев для него выставляется такой же, как и для данной группы. Данный способ предполагает выделение одинаковых по значимости критериев групп, их определяющих характеристик, а также необходимость экспертной оценки значимости характеристик для каждой группы, что весьма сложно, а иногда невозможно.

Второй способ основан на ранжировании значимости критериев на основе их дисперсии. Суть метода заключается в том, чтобы выбирать те критерии, которые имеют наибольшую вариацию в данных. Это означает, что выбранные критерии наиболее важны для разделения объектов на различные классы.

Метод наибольшей дисперсии основан на предположении о том, что критерии, которые имеют большую вариацию, могут лучше разделять объекты на различные классы [Косоруков 2019].

Данный метод не учитывает взаимосвязь между признаками и может не определить значимость признаков, которые хотя и имеют низкую вариацию, но важны для разделения классов. Метод наибольшей дисперсии не является универсальным и может быть неэффективным в случаях, когда имеются категориальные или нечисловые признаки.

Если скомбинировать данные методы, можно получить следующий результат: Разобьем все товары на иерархические группы, например, группа «верхняя одежда» будет иметь подгруппы: «куртки», «пальто», «пуховики», «жилеты». Для каждого иерархического уровня будут существовать свои дисперсии критериев, на основе которых им будут даваться веса после определения, к какой группе относится товар. Эти действия проделываются для подгрупп данной группы и т. д., пока мы не дойдем до конкретных

товаров. При этом группы будут обладать усредненными характеристиками своих подгрупп или товаров. Чем меньше дисперсия характеристики будет внутри группы, тем более характерной будет данная характеристика для группы.

Разрабатываемый метод включает выделение объектов изображения и вычисление их характеристик. Далее следуют этапы определения значимости этих характеристик и выбор наиболее подходящих вариантов. В том случае, если среди выбранных вариантов есть группы, то для их элементов повторяются последние два этапа. В конечном итоге мы имеем множество подходящих товаров. Основные этапы метода представлены в виде IDEF0 диаграммы на рис. 1.

Рис. 1. Метод поиска товаров по изображению

Для работы метода должна существовать база данных, в которой находятся группы, товары и их вычисленные характеристики. При добавлении нового товара в базу для его изображения вычисляются характеристики цвета объектов изображения, формы этих объектов и текстурные признаки Тамура: контрастность, шероховатость, направленность, регулярность и линейность. После этого данный товар относят к одной из групп и добавляют его вместе с характеристиками в базу данных. Характеристики групп верхних уровней пересчитываются как средние характеристики одинаковых объектов всех элементов, входящих в них.

Характеристики изображений представлены в виде описаний объектов изображения. Структура характеристик объектов представлена в табл. 1.

Таблица 1

Название поля	Тип	Значение
Цвет Красный	Массив 128 целых чисел	Гистограмма красной цветовой составляющей
Цвет Зеленый	Массив 128 целых чисел	Гистограмма зеленой цветовой составляющей
Цвет Синий	Массив 128 целых чисел	Гистограмма синей цветовой составляющей
Контрастность	Массив 4 дробных чисел	Контраст текстуры для 4 масштабов
Шерховатость	Массив 4 дробных чисел	Шероховатость текстуры для 4 масштабов
Зернистость	Массив 4 дробных чисел	Зернистость текстуры для 4 масштабов
Направленность	Массив 4 дробных чисел	Направленность текстуры для 4 масштабов
Регулярность	Массив 4 дробных чисел	Регулярность текстуры для 4 масштабов
Линейность	Массив 4 дробных чисел	Линейность текстуры для 4 масштабов
Форма	Массив комплексных чисел	Двумерные преобразования Фурье над векторами, образующими форму объекта
Принадлежность	Идентификатор	Указывает, к какому товару или группе этот объект относится

Информация о группах и товарах находится в базе данных. Группы и товары имеют свои идентификаторы. Для каждой группы или товара указывается какая группа его содержит, при этом существует корневая группа с идентификатором 0. Для возможности различить группу и конкретный товар группы помечаются типом группы, а товары типом товаров. В структурах объектов указывается, к какой группе или товару этот объект относится.

Для товаров указываются их артикул и изображение. В табл. 2 приведена структура данных для товаров и групп.

Таблица 2

Название поля	Тип	Значение
Идентификатор	Целое число	Идентификатор
Группа	Целое число	Идентификатор группы, к которой принадлежит данный элемент
Тип	Целое число	Указывает, является ли элемент группой или товаром
Артикул	Строка	Артикул товара
Изображение	Ссылка	Ссылка на изображение товара

Данные, представленные в базе, обрабатываются алгоритмами, которые реализуют многокритериальный выбор. Рассмотрим эти алгоритмы более подробно.

Основной алгоритм работы метода представлен в виде схемы на рис. 2.

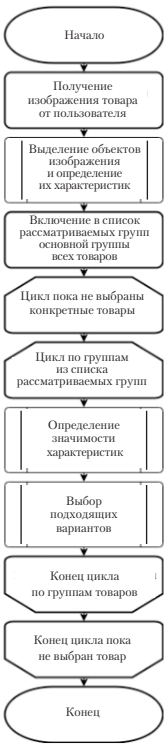

Рис. 2. Схема основного алгоритма работы метода

Алгоритм многокритериального выбора выполняется следующим образом.

1. Загрузка изображения и извлечение его характеристик:
– извлечение значений красного, зеленого и синего цветов для каждого пикселя изображения;
– создание гистограммы для каждой цветовой составляющей, которая отображает распределение значений цвета в изображении;
– извлечение значений контрастности, шероховатости, зернистости, направленности, регулярности и линейности текстуры для 4 масштабов;
– применение двумерных преобразований Фурье к векторам, образующим форму объекта, и сохранение результатов в поле «Форма».
2. Определение весов для каждого критерия:
– определение веса для каждой цветовой составляющей на основе значимости цвета в контексте решаемой задачи;
– определение веса для каждого критерия текстуры на основе значимости текстуры в контексте решаемой задачи;
– определение веса для критерия формы на основе значимости формы в контексте решаемой задачи.
3. Нормализация характеристик:
– нормализация значений цветовых составляющих и текстурных характеристик для каждого пикселя и масштаба соответственно;
– нормализация значений формы;
– расчет общей оценки для каждого объекта;
– умножение значений каждой характеристики на ее вес;
– суммирование взвешенных значений характеристик для получения общей оценки.
4. Выбор объекта с наивысшей общей оценкой:
– выбор объекта с наивысшей общей оценкой в качестве рекомендации или определение степени соответствия каждого объекта заданным критериям.

Алгоритм многокритериального выбора по картинке позволяет учесть различные характеристики изображения и применить их для принятия решения на основе заданных критериев.

Данный алгоритм использует несколько других алгоритмов, изложенных ниже. Схема алгоритма выделения объектов и вычисления их характеристик изображена на рис. 3. Данный алгоритм в качестве входных аргументов получает изображение, после обработки которого возвращает множество объектов в виде наборов визуальных характеристик объектов изображения.

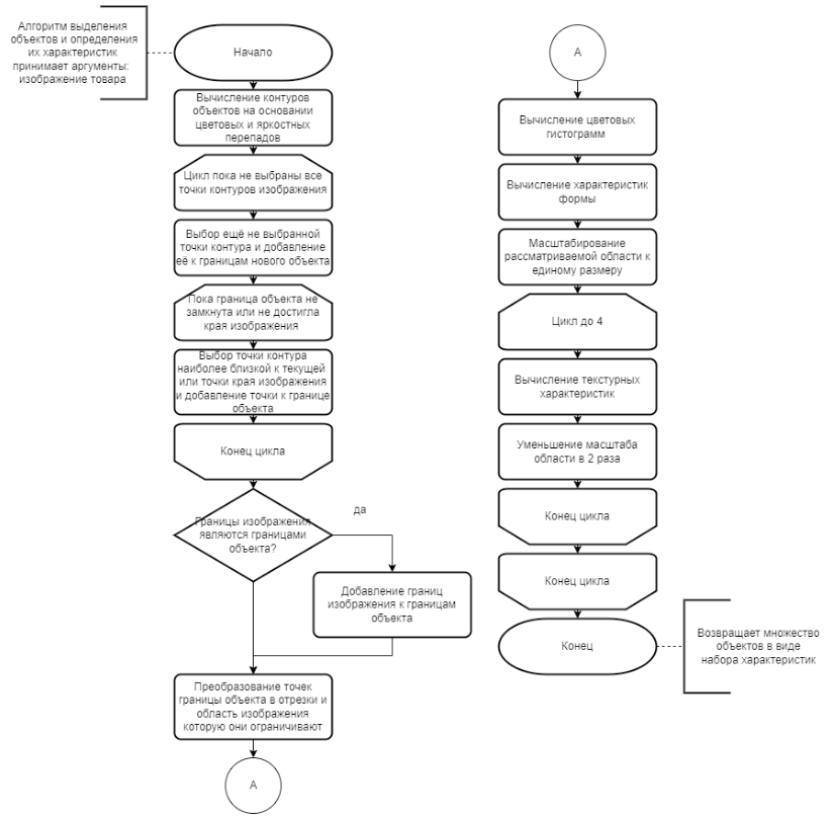

Рис. 3. Схема алгоритма выделения объектов и вычисления их характеристик

Алгоритм находит контуры объектов за счет перепадов цвета и яркости. На этом основании формируется массив точек контура объекта. Затем отсекается фон изображения. На основе полученных результатов вычисляются цветовые гистограммы, а затем – характеристики формы с помощью преобразований Фурье. После определения характеристик формы производится масштабирование изображения и вычисляются его текстурные характеристики, которые будут описывать все поля табл. 1, за исключением поля «Принадлежность», поскольку важно, чтобы распознанный товар принадлежал определенной группе.

Алгоритм определения принадлежности товара к группе и значимости характеристик как для групп, так и для отдельных товаров

представлен на рис. 4. Данный алгоритм в качестве входных аргументов получает идентификатор группы, среди подгрупп которой должен производиться выбор. Алгоритм возвращает набор весов значимости характеристик объектов.

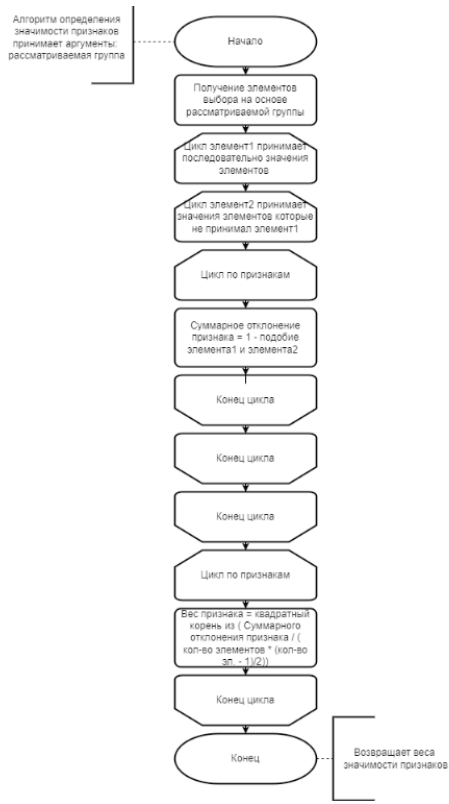

Рис. 4. Схема алгоритма определения значимости признаков

Наиболее значимые признаки позволят определить принадлежность товара к определенной группе. Группа имеет фиксированное количество признаков, определение веса/значимости признака товара дает возможность отнести его к группе. Поэтому для каждого товара выделяются признаки, производится его сравнение с образцом и определяется вес каждого из признаков. Алгоритм в качестве входных аргументов получает идентификатор группы, среди подгрупп которой должен производиться выбор. Алгоритм

возвращает набор весов значимости характеристик объектов. Далее производится выбор подходящих вариантов для товара. Схема этого алгоритма изображена на рис. 5.

Рис. 5. Схема алгоритма выбора подходящих вариантов

Данный алгоритм принимает аргументы, записанные в виде, представленном в табл. 1. Он выделяет объекты на изображении на основе цветовых гистограмм и функции схожести характеристик и схожести формы. Вычисляет подобие как сумму функций подобия, умноженных на весовые коэффициенты. А затем на основе показателей подобия группы производится добавление элемента в список выбранных.

Программное средство, позволяющее осуществлять поиск по изображению на основе цвета, формы и текстуры, реализовано на языке C# и использует СУБД PostreSQL с инструментарием пакета Npgsql. Пакет AForge имеет реализацию алгоритма Кэнни для выделения контуров на изображении. Для вычисления преобразований Фурье применяется функционал MathNet.

В качестве входных данных пользователь задает путь до изображения одного из следующих форматов: jpg, png, bmp и числовую характеристику – допустимое отклонение от наилучшего варианта, которая представляет собой дробное число в пределах от 0 до 100.

В качестве результата работы программа возвращает множество товаров в виде их изображений и артикулов, а также она предоставляет возможность добавления товара и группы товаров. При добавлении товара вводится индекс группы, в которую он входит, в виде числа, артикул в виде строки и путь до изображения форматов: jpg, png, bmp. При добавлении группы вводится индекс группы, в которую он входит, в виде числа и ее название.

Для создания необходимых таблиц в базе данных используется SQL-скрипт, приведенный в листинге 1.

Листинг 1

```
    CREATE TABLE elements (id SERIAL PRIMARY KEY, group_
id INT ,type INT ,
    articul VARCHAR(100), image BYTEA);
    CREATE TABLE objects (id SERIAL PRIMARY KEY, eleme
nt_id INT ,
    r_color INT[], g_color INT[], b_color INT[],
    texture_contrast DOUBLE PRECISION[],
    texture_roughness DOUBLE PRECISION[],
    texture_grain DOUBLE PRECISION[],
    texture_focus DOUBLE PRECISION[],
    texture_regularity DOUBLE PRECISION[],
    texture_linearity DOUBLE PRECISION[],
    form Text);
```

На рис. 6, 7 приведены примеры работы приложения.

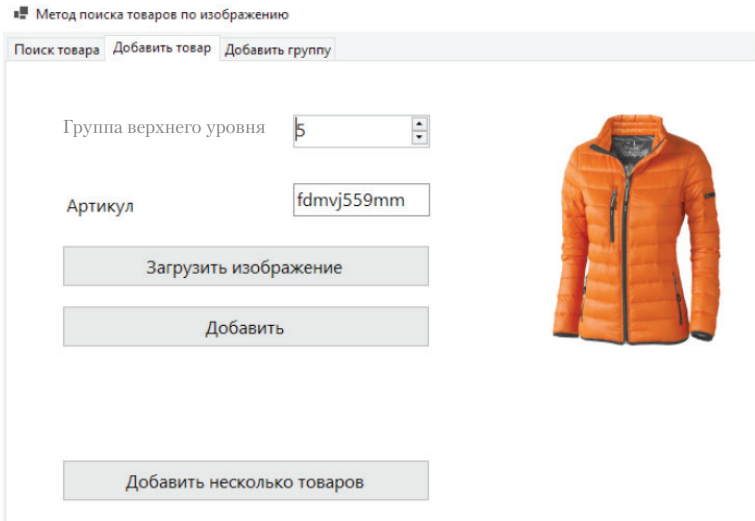

Рис. 6. Пример добавления товара

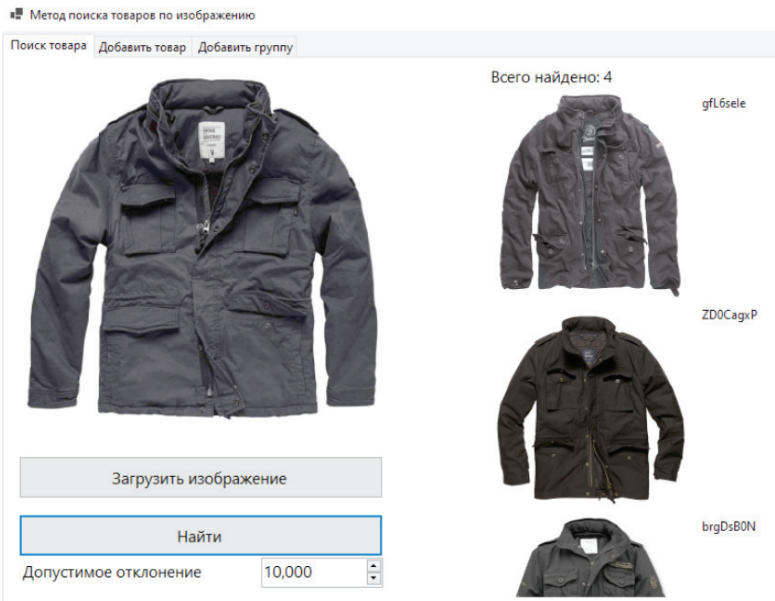

Рис. 7. Пример поиска товара

Для проведения исследования работы реализованного метода поиска товаров по изображению был создан набор из 1000 изображений одежды.

Для исследований будет использоваться ЭВМ со следующими характеристиками:

– операционная система: Windows 10;
– оперативная память: 8 гб;
– процессор: Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz;
– количество логических ядер: 4.

Исследования проводились с увеличением количества товаров в базе данных с 200 до 1000 с шагом 200. Разбиение товаров по группам не проводилось. Замеры времени проводились только на этапе поиска товаров, определение признаков поискового изображения в расчет не бралось. Время измерялось в миллисекундах.

В качестве результатов замера времени было использовано среднее значение от 20 запросов поиска 5 разных товаров. Результаты замеров приведены в табл. 3.

Таблица 3

Зависимость времени поиска
от количества товаров в базе данных

Количество товаров	Результат в миллисекундах
200	3842
400	7772
600	12028
800	16103
1000	20178

Как видно из табл. 3, зависимость времени работы метода от количества товаров в базе данных можно линейно интерполировать, следовательно, время работы прямо пропорционально количеству товаров в базе данных.

Исследования проводились на базе данных с количеством товаров 1000, равномерно распределенных по группам. Исследования проводились на группах двух уровней: 1 – подгруппы нулевой группы и 2 – подгруппы групп 1-го уровня.

Замеры времени проводились только на этапе поиска товаров, определение признаков поискового изображения в расчет не бралось. Время измерялось в миллисекундах.

В качестве результатов замера времени было использовано среднее значение от 20 запросов поиска 5 разных товаров. Результаты замеров приведены в табл. 4.

Таблица 4

Зависимость времени поиска от группировки товаров

Количество групп 1-го уровня	Количество групп 2-го уровня	Результат в миллисекундах
0	0	20 178
2	0	10 270
3	0	6757
2	2	5750
2	3	3582
3	2	3496
3	3	2349

Как можно заметить из данных, приведенных в табл. 4, разбиение товаров на группы существенно ускоряет работу метода, при этом наибольшее влияние на время работы оказывает количество групп нижних уровней, а время работы кратно зависит от их количества.

Исследования проводились на базе данных с числом товаров 1000, равномерно распределенных по созданным группам. Последовательно в базу данных вносились новые группы, являющиеся подгруппами предыдущих. Товары равномерно распределялись между группами. Поиск производился на основе 100 товаров, модели которых представлены в базе данных. Ошибкой считается возвращение товара не той модели. В табл. 5 приведены результаты этого исследования.

Таблица 5

Зависимость количества ошибок от количества уровней групп товаров

Количество уровней групп	Количество ошибок, в %
0	5
1	12
2	15
3	15

Для случая с тремя уровнями групп некоторые из результатов поиска расписаны в табл. 6. В данной таблице приведены примеры поиска некоторых товаров и количества попаданий при их поиске в нужные группы.

Из табл. 6 можно увидеть, что объединение товаров в группы увеличивает количество ошибок. Связано это с добавлением ошибки неверного выбора группы при поиске товара. Можно также заметить, что с увеличением количества уровней групп количество ошибок начинает расти медленнее. Это связано с тем, что в группы высоких уровней объединены товары, визуально более похожие друг на друга, чем в группах низких уровней, что приводит к уменьшению ошибки при выборе алгоритмом нужной группы среди групп высоких уровней. По результатам исследования метод поиска показал линейную зависимость времени от количества товаров в базе данных, при этом группировка товаров способна существенно ускорить поиск, однако увеличивает количество ошибок.

Таблица 6

Попадание поиска по группам

Название искомого товара и количество изображений	Группа 1-го уровня. Количество попаданий в нее	Группа 2-го уровня. Количество попаданий в нее	Группа 3-го уровня. Количество попаданий в нее
Синяя футболка 30	Одежда 27	Футболки 26	Синие футболки 26
Черная куртка 20	Одежда 16	Куртки 16	Черные куртки 16
Белые кроссовки 30	Обувь 28	Кроссовки 27	Белые кроссовки 27
Синие джинсы 20	Брюки 18	Джинсы 18	Синие джинсы 18

Таким образом, комбинация выделения формы посредством алгоритмов Фурье: определение цветовых характеристик объектов изображения, формы этих объектов и текстурных признаков Тамура: контрастность, шероховатость, направленность, регулярность и линейность – позволяют определить товар по его изображению с достаточно высокой точностью. Однако группировка товаров по признакам, например, таких, как «Синие джинсы»,

дает очень большой рост ошибок. Авторы предполагают такую группировку товаров избыточной, и предлагают сделать группировку товаров с меньшим количеством уровней вложенности или группировку товаров по другим характеристикам. Однако алгоритм проявляет достаточную устойчивость и точность распознавания изображений и может быть протестирован при других уровнях группировки.

Литература

Болотова 2016 – *Болотова Ю.А., Друки А.А., Спицын В.Г.* Методы и алгоритмы интеллектуальной обработки цифровых изображений: Учеб. пособие. Томск: Национальный исследовательский Томский политехнический университет, 2016. 208 с.

Волосатова 2021 – *Волосатова Т.М., Зубова Г.С., Князева С.Ю., Филиппов М.В.* Разработка и реализация алгоритмов построения точной карты пространства // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 8–29. DOI: 10.28995/2686-679X2021-4-8-29.

Фурман 2003 – *Фурман Я.А.* Введение в контурный анализ. Приложения к обработке изображений и сигналов. М.: ФИЗМАТЛИТ, 2003. 592 с.

Косоруков 2019 – *Косоруков О.А.* Модели исследования операций: Учеб. / О.А. Косоруков, М.А. Халиков, Г.П. Фомин. М.: РУСАЙНС, 2019. 190 с.

References

Bolotova Yu., Druki A. and Spitsyn, V. (2016), *Metody i algoritmy intellektual'noi obrabotki tsifrovykh izobrazhenii: ucheb posob*. [Methods and algorithms for intellectual processing of digital images. Study guide], National Research Tomsk Polytechnic University, Tomsk, Russia, 208 p.

Furman, Ya. (2003), *Vvedenie v konturnyi analiz. Prilozheniya k obrabotke izobrazhenii i signalov* [Introduction to contour analysis. Applications to image and signal processing], FIZMATLIT, Moscow, Russia, 592 p.

Kosorukov, O., Khalikov, M. and Fomin, G. (2019), *Modeli issledovaniya operatsii: ucheb*. [Operations Research Models. Textbook], RUSAINS, Moscow, Russia, 190 p.

Volosatova, T.M., Zubova, G.S., Knyazeva, S.Yu. and Filippov, M.V. (2021), "Design, development and implementation of precision space mapping algorithm", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 8–29, DOI: 10.28995/2686-679X2021-4-8-29.

Информация об авторах

Марина *С. Шаповалова,* кандидат педагогических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, mshapovalova84@gmail.com

Илья Ю. Елгин, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, ilia.elgin@yandex.ru

Information about the authors

Marina S. Shapovalova, Cand. of Sci. (Pedagogy), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005, mshapovalova84@gmail.com

Il'ya Yu. Elgin, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005, ilia.elgin@yandex.ru

УДК 004.056
DOI: 10.28995/2686-679X-2023-4-70-91

Техническая защита визуальной информации в офисных помещениях методом инфракрасной засветки

Владимир В. Гришачев
Российский государственный гуманитарный университет, Москва, Россия, grishachev@mail.ru

Виктория Э. Щеголева
Российский государственный гуманитарный университет, Москва, Россия, vischglv@gmail.com

Аннотация. В работе представлены результаты качественного теоретического анализа и экспериментальных исследований влияния инфракрасного излучения (засветки) на работу веб-камеры. Используемые в скрытом наблюдении видеокамеры изготавливаются на основе кремниевых ПЗС-матриц. Чувствительность кремниевых ПЗС-матриц к оптическому излучению превышает чувствительность человеческого глаза в несколько раз, и она смещена по спектру в невидимую глазом инфракрасную область. Управление экспозицией и диафрагмой видеокамеры позволяет в широких пределах изменять чувствительность камеры, подстраиваясь к изменению внешнего освещения. Невидимое глазом инфракрасное излучение оказывает существенное влияние на формирование регистрируемого видеоизображения, полностью отсечь которое без существенного ухудшения характеристик видеосъемки не представляется возможным. Формирование в помещении однородного и изотропного по направлению освещения в инфракрасной области может нейтрализовать любое скрытое наблюдение на основе видеокамер. Исследования показали возможность деструктивного воздействия на видеосъемку без разрушения электроники видеокамеры инфракрасного излучения, которое не оказывает влияния на комфортабельность нахождения сотрудников в защищаемом помещении. Предложены методы защиты офисного помещения от скрытого видеонаблюдения и методика изучения воздействия инфракрасного излучения на веб-камеру для курса физических основ защиты информации.

Ключевые слова: техническая защита визуальной информации, скрытое видеонаблюдение, видеокамера, инфракрасная засветка

Для цитирования: Гришачев В.В., Щеголева В.Э. Техническая защита визуальной информации в офисных помещениях методом инфракрасной засветки // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 70–91. DOI: 10.28995/2686-679X-2023-4-70-91

Technical protection of visual information in office premises by the method of infrared illumination

Vladimir V. Grishachev
Russian State University for the Humanities, Moscow, Russia; grishachev@mail.ru

Viktoriya E. Schegoleva
Russian State University for the Humanities, Moscow, Russia; vischglv@gmail.com

Abstract. The paper presents the results of qualitative theoretical analysis and experimental researches of the influence of infrared radiation (illumination) on a webcam operation. The video cameras used in hidden surveillance are made on the basis of silicon CCD-matrix. The sensitivity of silicon CCD-matrix to optical radiation exceeds the sensitivity of the human eye by several times, and it is shifted along the spectrum to the infrared region not visible to the eye. Controlling the exposure and aperture of the video camera allows changing the sensitivity of the camera within a wide range, adjusting to changes in external illumination. Infrared radiation invisible to the eye has a significant effect on the formation of the recorded video image, and it cannot be completely cut off without a significant deterioration in the characteristics of video shooting. The formation of the uniform and isotropic illumination in the infrared region in the room can neutralize any covert surveillance based on video cameras. Researches have shown the possibility of destructive effects of the infrared radiation on video shooting without destroying electronics in the camera, which does not affect the comfort of employees in a protected room. The authors propose methods of protecting office premises from hidden video surveillance and a methodology for studying the effects of infrared radiation on a webcam in the course of the physical basics of information protection.

Keywords: technical protection of visual information, hidden video surveillance, video camera, infrared illumination

For citation: Grishachev, V.V. and Schegoleva, V.E. (2023), "Technical protection of visual information in office premises by the method of infrared illumination", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 4, pp. 70–91, DOI: 10.28995/2686-679X-2023-4-70-91

Введение

К визуальной (видовой, зрительной) информации относится воспринимаемая человеком органами зрения (глазами) информация в виде отображения окружающей среды, рисунков, текстов, графиков и т. д. Визуальная информация формирует основной поток всей воспринимаемой информации, что определяет ее значение для обеспечения безопасности деятельности человека, организаций, государства в виде контроля, получения и распространения.

Представление визуальной информации техническими средствами реализуется в статическом (фотоинформация) и динамическом (видеоинформация) видах. Общее деление систем фотографирования и видеонаблюдения можно провести по используемой рабочей части спектра электромагнитного излучения, в которой выделяется визуальная информация инфракрасного, видимого и рентгеновского диапазона спектра. Технические средства наблюдения позволяют визуализировать неэлектромагнитные излучения, несущие информацию о пространственной структуре окружающей среды и объектов, например, путем преобразования акустического поля, потока электронов в видимое плоское изображение.

Одной из основных угроз несанкционированного получения визуальной информации в помещении является негласное видеонаблюдение и документирование путем скрытой (закамуфлированной, замаскированной) видеокамерой [Хорев 2008; Хорев 2010; Алферов 2012; Тельный 2013]. Получаемая подобным образом визуальная информация позволяет делать выводы об идентификации присутствующих, используемого оборудования, пространственных характеристик помещения и т. д., а также фиксировать отображаемые документы. Все это влияет на состояние информационной безопасности организации, подвергаемой подобным угрозам.

1. Техническая разведка и защита визуальной информации

Основу средств технической визуальной разведки составляют видеокамеры, обладающие признаками маскировки под бытовые предметы, малой апертурой входной оптики, высокой светочувствительностью и другими признаками, которые делают съемку скрытой и подпадают под запрет общедоступного использования [Хорев 2008;

Хорев 2010; Алферов 2012; Тельный 2013][1,2]. Обсуждение конструкции, устройства и общих принципов работы бытовых видеокамер позволяет оценить угрозы, исходящие от них на бытовом уровне, и экстраполировать на более опасные применения не только обычных видеокамер, но и специальных средств визуального наблюдения.

1.1. Видеокамера – устройство наблюдения и документирования. Обобщенную структуру системы технической видеофиксации [Хорев 2008; Хорев 2010; Алферов 2012; Тельный 2013; Дамьяновски Владо 2020] окружающей обстановки можно представить в виде функционально связанных между собой подсистем (рис. 1). Оптический блок состоит из входной/выходной оптики (1), оптического канала (2) и предназначен для формирования и передачи изображения в виде оптического потока для последующего преобразования в электрический сигнал. Электронный блок (4) состоит из системы преобразования оптического изображения в аналоговый или цифровой электрический сигнал (3), в качестве которой используется ПЗС-матрица, а также для первичной обработки и формирования обратной связи. Сформированный электрический сигнал с визуальной информацией через проводные или беспроводные системы (5) поступает в систему регистрации (6) видеоинформации на электронный носитель. Электрическое питание системы (7) осуществляется автономным источником питания (батарея, аккумулятор с подзарядкой от фотоэлементов и другое) или питанием от электрической сети камуфлирующего оборудования.

Обсудим работу каждой подсистемы более подробно [Хорев 2008; Хорев 2010; Алферов 2012; Тельный 2013; Дамьяновски Владо 2020]. Входная оптика имеет различную структуру в зависимости от назначения: при наблюдении удаленных на десятки и сотни метров объектов требуется сложная оптическая система из нескольких линз с большой апертурой, при наблюдении объектов на дальности в несколько метров и ближе необходима более простая оптическая система вплоть до одной линзы с малой апертурой.

Скрытое видеонаблюдение производится с входным зрачком (объективом) диаметром порядка 1 мм пинхольного типа, что позволяет проводить эффективную маскировку. Использование короткофокусной линзы с фокусным расстоянием несколько миллиметров позволяет расположить ПЗС-матрицу на малом расстоянии, что

---

[1] Федеральный закон «Об оперативной и розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ, ст. 6, ч. 6.

[2] ПП РФ от 10 марта 2000 г. № 214 и Примечание к ст. 138.1. Список видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию.

уменьшает общие размеры средства визуальной разведки до нескольких миллиметров. В некоторых случаях для повышения скрытности оптический канал можно удлинить до сотен метров путем использования волоконно-оптических эндоскопов, т. е. жгутов из оптоволокна [Хацевич 2002]. Такая система позволяет удалить электронные компоненты от диэлектрических элементов входной оптики и повысить скрытность от обнаружения по электромагнитному излучению или отклику.

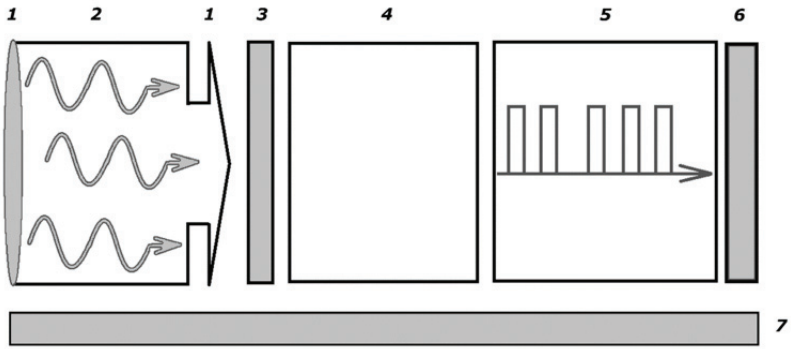

Рис. 1. Обобщенная блок-схема средства технической разведки визуальной информации (системы скрытого видеонаблюдения):
1 – входная/выходная оптика,
2 – оптический канал/оптическая система управления,
3 – оптоэлектронный преобразователь (ПЗС-матрица),
4 – система обработки видеоинформации,
5 – кабельный или эфирный канал передачи,
6 – система хранения информации,
7 – система питания

На эффективность видеонаблюдения влияет поле зрения оптической системы, т. е. пространственный угол обзора, который охватывает наблюдаемое пространство. Его величина зависит от отношения размеров регистрирующей матрицы к фокусному расстоянию. Чем меньше размер ПЗС-матрицы и больше фокусное расстояние, тем меньше пространственный угол, который захватывается полем зрения. Для скрытого видеонаблюдения узкое поле зрения может быть использовано в редких случаях фиксации документов с близкого расстояния с высоким разрешением. Чаще требуется широкое поле зрения с углами от 60 градусов. В случае

максимального поля зрения может быть использован объектив «рыбий глаз» с углом обзора более 180 градусов.

1.2. ПЗС-матрица видеокамеры. Качество съемки определяется не только параметрами оптической системы, но и характеристиками системы фиксации изображения, в качестве которой в видимой и ближней инфракрасной области спектра оптического излучения может быть использована кремниевая ПЗС-матрица. Разрешающая способность матрицы определяется размерами и общим числом светочувствительных ячеек (пикселей), т. е. размерами пикселей и плотностью их размещения. Современные ПЗС-матрицы имеют размер пиксела несколько мкм и образуют матрицу с общим числом от 0.3 Мп (формат VGA) и более 8,8 Мп (формат 4K) при видеосъемках с частотой от 25 (стандарт PAL и SECAM) до 30 (стандарт NTSC) кадров в сек. Видеокамеры позволяют проводить съемку при различных уровнях освещенности от освещенности в солнечный безоблачный день с уровнем выше 100 000 люкс до безлунной ночи с уровнем 0,0001 люкс.

Широкий охват динамического диапазона освещенности достигается путем использования высокочувствительных кремниевых детекторов, чувствительность которых к свету выше возможностей человеческого глаза в несколько раз и смещена по спектру в невидимую глазом инфракрасную (ИК) часть оптического спектра (рис. 2). Для приближения чувствительности ПЗС-матрицы к чувствительности глаза человека в оптической системе используют инфракрасный отсекающий светофильтр (рис. 3). В системах видеонаблюдения, используемых как днем, так и ночью, светофильтры не используются или используются с меньшим ослаблением. Для получения хорошего изображения ночью применяется автоматически включающаяся инфракрасная подсветка. Дополнительная регулировка светового потока, направляемого на регистрирующую матрицу, осуществляется автоматическим управлением диафрагмой в оптической системе, а также электронной регулировкой времени экспозиции.

Таким образом, отличительной особенностью кремниевой ПЗС-матрицы является высокая светочувствительность, смещенная в невидимую глазом инфракрасную область спектра, что можно использовать для деструктивного воздействия на работу систем скрытого видеонаблюдения.

Управление параметрами оптической системы и обработки видеоинформации в электронном виде производится в системе обработки, который в зависимости от объема видеоинформации может требовать значительных вычислительных ресурсов. В случае получения видеоинформации в цвете и цифровом виде объем обрабатываемой информации возрастает в три и более раз, что требует повышения вычислительных, энергетических и других ресурсов.

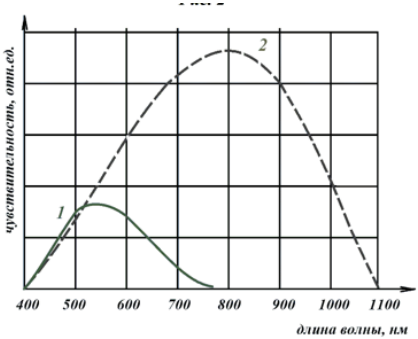

Рис. 2.
Спектральная чувствительность человеческого глаза (1) и ПЗС-матрицы без фильтра (2) [Дамьяновски Владо 2020]

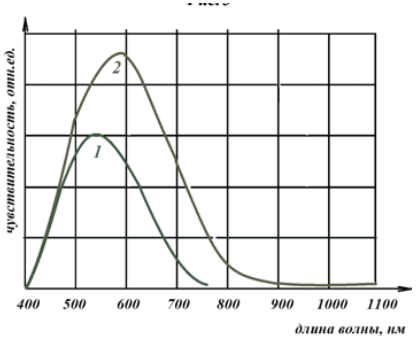

Рис. 3.
Изменение спектральной чувствительности ПЗС-матрицы при использовании инфракрасного отсекающего фильтра:
1 – спектральная чувствительность человеческого глаза,
2 – спектральная характеристика черно-белой ПЗС-матрицы с инфракрасным отсекающим фильтром [Дамьяновски Владо 2020]

Следующий элемент системы скрытого видеонаблюдения образует система передачи видеоинформации в аналоговом или цифровом виде в систему регистрации. Передача может проводиться по скрытым кабельным системам, путем использования штатных кабельных систем связи, а также по беспроводным (эфирным) радиоинтерфейсам, таким как Bluetooth, WiFi и другие. Эфирные каналы связи обладают демаскирующими признаками, по которым может быть обнаружено скрытое видеонаблюдение.

Завершающий элемент всей системы скрытого видеонаблюдения образуется системой регистрации видеоинформации на носитель, в качестве которого может выступать карта памяти формата microSD.

1.3. Техническая защита визуальной информации от скрытого видеонаблюдения. В модели угроз визуальной информации методом скрытого видеонаблюдения основной элемент – видеокамера, поэтому общие методы противодействия можно разделить на два вида.

1. Обнаружение (выявление) видеокамер по демаскирующим признакам [Хорев 2015]. К демаскирующим признакам относится входная оптика, которая должна быть направлена на объект наблюдения. Положение объекта наблюдения определено, поэтому определено и направление оптических элементов, которые могут создавать блики при их освещении искусственными источниками на нехарактерных длинах волн для естественного освещения. Например, при освещении красным светом при поиске глазом или невидимым глазом инфракрасным светом при поиске прибором ночного видения. Также к демаскирующим признакам относится электромагнитное излучение от электронных элементов работающей системы видеонаблюдения. Обнаружение неработающих электронных элементов возможно методами нелинейной локации.

2. Нейтрализация работы системы скрытого видеонаблюдения методами деструктивного воздействия на электронику путем создания сильных электромагнитных импульсов, влияющих на работу; создание электромагнитных помех для беспроводной передачи видеоинформации. Отдельно можно выделить способ нейтрализации путем засветки оптики.

Засветка оптики систем скрытого видеонаблюдения [Гридин 1983; Смелков 2001; Куликов 2001; Куликов 2002; Смелков 2004; Уваров 2006; Уваров 2001; Гонта 2006; Гонта 2007]. Как было отмечено выше, чувствительность кремниевой ПЗС-матрицы выше в невидимой инфракрасной части оптического спектра, поэтому включение ИК-прожектора сильно влияет на работу матрицы, при этом не изменяет освещенность в помещении, выраженную в люксах (для человека). Созданием критической ИК освещенности (засветки) может вывести видеокамеру из рабочего состояния и не позволить создать качественное изображение окружающей обстановки. Воздействие ИК засветки эквивалентно воздействию видимого оптического излучения, они вводят ПЗС-матрицу в состояние переполнения накопленного в пикселах заряда, что приводит к увеличению видеосигнала и уменьшению контраста между соседними точками в изображении (появлению «смаза»), когда соседние точки одинаково ярки и становятся неразличимыми. Дополнительно при воздействии яркого видимого или мощного ИК излучения происходит перетекание заряда из одного пиксела в соседние, что также приводит к нарушению функционирования видеокамеры. Путем автоматической регулировки экспозиции ПЗС-матрицы или электромеханической подстройкой диафрагмы достигается уменьшение освещенности, и изображение восстанавливается. Аналогичные процессы происходят при падении внешней освещенности: величина накопленного заряда падает, пропа-

дает контраст изображения, он становится одинаково темным по всему кадру. Система управления должна увеличить интегральный световой поток, падающий на ПЗС-матрицу, изменяя те же самые параметры – диафрагму и экспозицию.

Таким образом, провоцируя периодическое изменение мощности внешнего ИК излучения со временем близким или меньшим времени адаптации (релаксации) системы управления видеокамеры, можно добиться невозможности получения устойчивого видеоизображения. Для деструктивного воздействия на видеокамеру необходимо определить такой параметр ИК засветки, как время релаксации t, т. е. время, необходимое для адаптации (подстройки) к изменению уровня освещенности видимым излучением или мощности ИК излучения, которые одинаковы по результирующему воздействию. Следующий параметр – глубина модуляции эффективной засветки h, которая может зависеть от уровня освещенности в помещении P. Еще один параметр – коэффициент эффективности засветки c, который определяет отношение эффективной мощности ИК излучателя в видимой области относительно засветки от источника видимого излучения. Данных параметров достаточно для количественной оценки деструктивности действия ИК засветки.

1.4. Общая характеристика угрозы скрытого видеонаблюдения. Модель угрозы и защиты визуальной информации в офисном помещении от скрытого видеонаблюдения определяется особенностями защищаемого помещения, возможностями нарушителя и используемых технических средств визуальной разведки. Эффективность функционирования любой системы технической защиты не может быть абсолютной, но можно задать общие требования к техническим средствам защиты визуальной информации в зависимости от задач.

Модель помещения. В качестве защищаемого помещения определим офисное помещение с характерным размером L, освещенностью в соответствии с требованиями нормативных документов[3] для работы в помещении с искусственным освещением P_0, в помещении нет преграждающих свету препятствий, нет затемненных участков, потолки и стены окрашены в светлые тона с высокими рассеивающими видимый свет и отражающими ИК излучение параметрами, которые создают комфортные для работы условия.

[3] Свод правил СП 52.13330.2016 «Естественное и искусственное освещение». Актуализированная редакция СНиП 23-05-95* (утв. приказом Министерства строительства и жилищно-коммунального хозяйства РФ от 7 ноября 2016 г. № 777/пр). Дата введения 8 мая 2017 г.

Модель нарушителя. Основная угроза исходит от внутреннего нарушителя, такого как сотрудник фирмы, посетитель и другие. Угрозами внешнего нарушителя пренебрегаем, так как от прямого проникновения света через окна помещение защищено закрытыми жалюзи или шторами.

Модель скрытого видеонаблюдения. В соответствии с общей характеристикой видеокамер сделаем ограничения, свойственные видеокамерам скрытого наблюдения, – это минимальные размеры, которые не позволяют использовать все возможности оптических систем и электронного управления, поэтому примем за основу, что видеокамера с объективом малого диаметра около 1 мм обладает высокой чувствительностью менее 0,1 люкс с фиксированным фокусом при поле зрения более 60° с автономной системой питания и хранения информации, с электронной автоматической регулировкой управления экспозицией. Видеокамера может размещаться на стенах помещения, быть встроена в мебель или оборудование, располагаться на одежде присутствующих в помещении (носимая видеокамера). Высокая чувствительность видеокамеры предполагает отсутствие в оптической системе отсекающих ИК излучение фильтров, что облегчает ее засветку. Наличие обратной связи времени экспонирования и уровня засветки накладывает повышенные требования к системе обработки и питания.

Модель защиты методом ИК засветки. Обеспечение защиты требует определить мощность, количество, управление и структуру размещения в помещении ИК источников.

2. Экспериментальное исследование деструктивного воздействия ИК засветки

Исследование возможностей ИК засветки проводилось на стандартном оборудовании, не имеющем ограничений в распространении, но физические принципы построения исследовательской системы являются общими со специальными устройствами, что позволяет сделать технические предложения по защите от скрытого видеонаблюдения не только на основе общедоступных систем. Моделирование скрытой видеокамеры осуществлялось бытовой веб-камерой Logitech Webcam C200 с оптическим разрешением 640 × 480 (VGA) для съемки видео с частотой 30 кадров в секунду на 0.30 мегапиксельной матрице, подключаемой к персональному компьютеру по USB 2.0 интерфейсу, контроль качества получаемого видео в реальном времени осуществлялся на мониторе компьютера.

2.1. Характеристика приборов и методика измерений. Предельная чувствительность по световому потоку определялась экспериментально путем помещения видеокамеры в темную комнату с контролируемым люксметром Ю116 освещенностью. Изображение с видеокамеры выводилось на монитор, и при уменьшении освещенности наблюдалось исчезновение изображения при освещенности 1 люкс. Измерение угла поля зрения проводилось по оптической схеме (рис. 4), когда ИК-прожектор или обычный светодиодный источник видимого света перемещался перпендикулярно оптической оси объектива видеокамеры до полного исчезновения источника. Угол поля зрения составил порядка 45°.

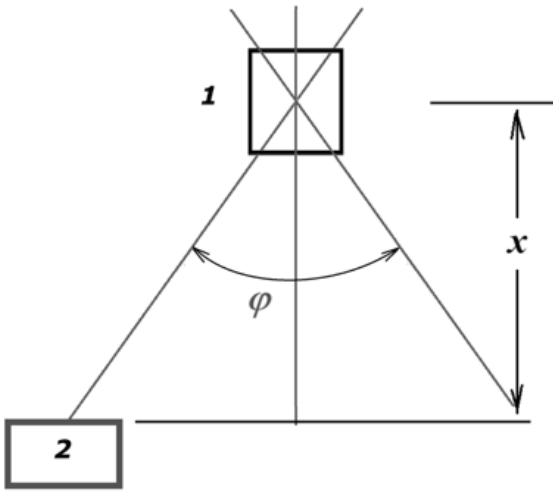

Рис. 4. Оптическая схема определения угла поля зрения (*j*) веб-камеры (1) путем перемещения источника света (2) на расстоянии *x* перпендикулярно оптической оси камеры

В качестве источников света использовался светодиодный источник видимого света (фонарик), который формировал освещенность порядка 150 люкс на расстоянии 20 см. В качестве источника ИК излучения использовался уличный ИК-прожектор для видеонаблюдения KDM-6044A с длиной волны максимума интенсивности излучения на 850 нм при угле обзора не более 45° с потребляемой мощностью около 1 Вт от 12 В источника питания (по паспортным данным). ИК-прожектор создавал освещенность в видимой области света порядка 7 люкс, но по эффективности

воздействия соответствовал светодиодному фонарику видимого света, размещенному на том же расстоянии 20 см. Таким образом, светодиодный фонарик и уличный ИК-прожектор оказывали одинаковое воздействие на веб-камеру. Поэтому исследования воздействия оптического излучения проводились как видимым светом, так и ИК излучением.

2.2. Экспериментальная установка. Исследование воздействия видимого и инфракрасного излучения на видеокамеру проводилось на экспериментальной установке (рис. 5), состоящей из исследуемой веб-камеры (1, 2), и рядом с ней в одной плоскости размещался люксметр (3, 4), с помощью которого контролировался уровень освещенности в видимой области.

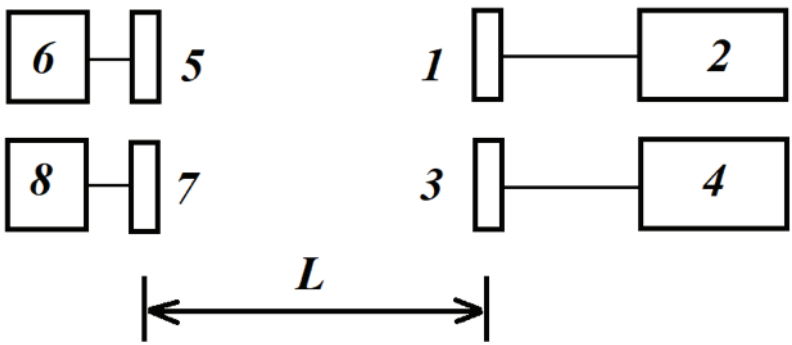

Рис. 5. Блок-схема экспериментальной установки по исследованию деструктивного воздействия засветки ИК излучением на работу веб-камеры: 1, 2 – веб-камера Logitech Webcam C200, подключенная к персональному компьютеру; 3, 4 – люксметр Ю116 с измерительным блоком; 5, 6 – источник белого света с блоком питания; 7, 8 – ИК-прожектор KDM-6044A с блоком питания; *L* – расстояние между источниками и приемниками оптического излучения

Параметры люксметра Ю116 соответствовали восприятию человеческого глаза и позволяли измерять фоновую освещенность и освещенность от дополнительных источников видимого белого света (5, 6) и инфракрасного источника (7, 8). Расстояние *L* между плоскостями источников (5, 6) и приемников (1, 3) света варьировалось в небольших пределах от 10 до 50 см, что связано с малой мощностью источников света. Фоновая освещенность

составила порядка 300 люкс, что по нормативным документам соответствовало нормальным рабочим условиям освещенности в офисе.

2.3. Результаты исследования воздействия ИК излучения на видеокамеру. Экспериментальное исследование влияния ИК излучения на видеокамеру показало возможность осуществить такую засветку камеры, что производить видеосъемку не представляется возможным (рис. 6). В веб-камере присутствует система электронной подстройки под фоновую освещенность, т. е. при резком изменении освещенности за некоторое время t релаксации происходит адаптация веб-камеры к уровню освещенности. Во время адаптации видеоизображение имеет низкое качество и не позволяет получить достоверную видеокартину. Экспериментально полученное значение t составило 2–3 секунды при фоновой освещенности 300 люкс и величине резкого (менее 1 секунды) изменения освещенности белым светом на не менее чем 50% (глубиной модуляции h). Такой же эффект наблюдался с ИК-прожектором, с помощью которого создавалась освещенность 7 люкс в видимой области за счет инфракрасной части спектра. Эффективность засветки определялась фоновой освещенностью – чем меньше освещенность, тем меньше требуется дополнительного освещения для деструктивного воздействия на камеру. В нашем случае глубина модуляции $h = 0.5$ по видимому световому потоку со временем 2–3 секунды. Она сохраняется и для инфракрасного излучения.

Оценим мощность ИК излучения, требуемую для деструктивной засветки инфракрасным излучением при фоновой освещенности 300 люкс в условиях эксперимента. Освещенность в 1 люкс соответствует интенсивности света 0,001464 Вт/м^2 на длине волны 555 нм. Тогда 150 люкс белого света будет соответствовать интенсивности много меньшей, чем 0,22 Вт/м^2, данная освещенность белого света приводит к эффективному деструктивному действию, так же как ИК-прожектор на длине волны 850 нм. Чувствительность к инфракрасному излучению веб-камеры без отсекающего фильтра (рис. 2–3) приблизительно в 3 раза выше относительно видимого света, т. е. мощность эффективной ИК засветки 0,07 Вт/м^2. Это соответствует эффективности преобразования $k = 7\%$ для используемого светодиодного ИК-прожектора с общей потребляемой мощностью 1 ВТ. Среднее значение КПД светодиода выше 30%, полученная оценка КПД занижена вследствие учета всех возможных потерь в устройстве, т. е. это КПД всего ИК-прожектора.

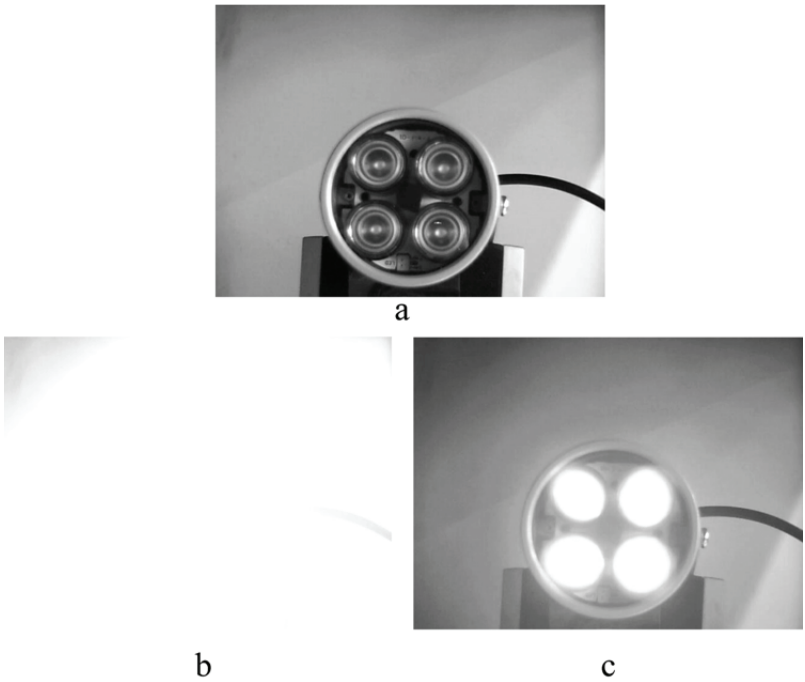

Рис. 6. Эксперимент по наблюдению отклика веб-камеры
на воздействие ИК-прожектора.
Фотографии ИК-прожектора на расстоянии 25 см
от веб-камеры при разрешении 1280 × 960 пикселей:
a) выключенный ИК-прожектор;
b) в момент включения ИК-прожектора;
c) изображение через 2–3 секунды

Таким образом, для обеспечения деструктивного воздействия на видеокамеру, используемую для скрытой видеосъемки, будет достаточно обеспечить засветку невидимым глазу ближним ИК излучением на длинах волн от 750 нм интенсивностью порядка 0,07 Вт/м^2, по крайней мере веб-камер типа Logitech Webcam C200 с гораздо меньшей чувствительностью и углом поля зрения, чем применяемые для скрытой видеосъемки.

3. Предложения по технической защите визуальной информации от скрытого видеонаблюдения методом ИК засветки

Проведенный экспериментальный и теоретический анализ показывает, что для эффективного деструктивного воздействия на срытое видеонаблюдение необходимо обеспечить освещенность видеокамеры невидимым глазом ИК излучением ближнего диапазона приблизительно от 750 до 900 нм со связью с фоновой освещенностью видимым светом с коэффициентом $\mu = 5 \cdot 10^{-4}$ (Вт/м^2)/люкс, т. е. интенсивностью переменного ИК излучения амплитудой порядка 0,5 мВт/м^2 на каждый люкс фонового освещения в видимой области и при импульсном или гармоническом изменении с частотой порядка $f = (1/\tau) = 0{,}5–0{,}3$ Гц, что обеспечивает защиту от скрытого видеонаблюдения высокочувствительными видеокамерами с электронной системой адаптации к освещенности.

3.1. Пример реализации противодействия скрытому видеонаблюдению (рис. 7). Скрытая видеосъемка ведется в помещении фоновой освещенностью P_0 в люксах. Определим мощность N точечного источника ИК излучения с пространственным углом обзора φ_i, совпадающим или большим углом поля зрения φ_v видеокамеры для эффективной деструктивной засветки. При попадании в поле зрения видеокамеры ИК источника излучение от него доходит до ПЗС-матрицы даже при расположении на краю поля зрения. При угле обзора источника меньшего угла поля зрения ($\varphi_i < \varphi_v$) видеокамеры расположение на краю зоны поля зрения ИК излучение не попадает на ПЗС-матрицу.

Интенсивность I ИК излучения на входе видеокамеры от ИК-прожектора, направленного на видеокамеру и находящегося в ее поле зрения на расстоянии L, должна иметь переменную интенсивность, меняющуюся с частотой f и амплитудой интенсивности $I_0 = \mu P_0$, т. е. интенсивность ИК засветки

$$I = \mu P_0 \left[1 - \sin(2\pi f \cdot t)\right] \text{ для гармонического воздействия.}$$

Полная интегральная мощность источника инфракрасного излучения при КПД k на расстоянии L составит

$$N = \frac{\pi \sin^2\left(\varphi_i/2\right) L^2 I_0}{k} = \frac{\mu}{k} \pi \sin^2\left(\varphi_i/2\right) L^2 P_0 .$$

В случае, приближенном к параметрам эксперимента, имеем $P_0 = 300$ люкс, $\mu = 5 \cdot 10^{-4}$ (Вт/м^2)/люкс, $k = 0{,}07$, $L = 5$ м и $\varphi_i = 60^0 > \varphi_v$ получим потребляемую ИК-прожектором электрическую мощность менее $N = 45$ Вт. Для уменьшения мощности источника можно увеличить плотность размещения ИК-прожекторов, увеличить их КПД, использовать встроенные в системы освещения помещения ИК источники.

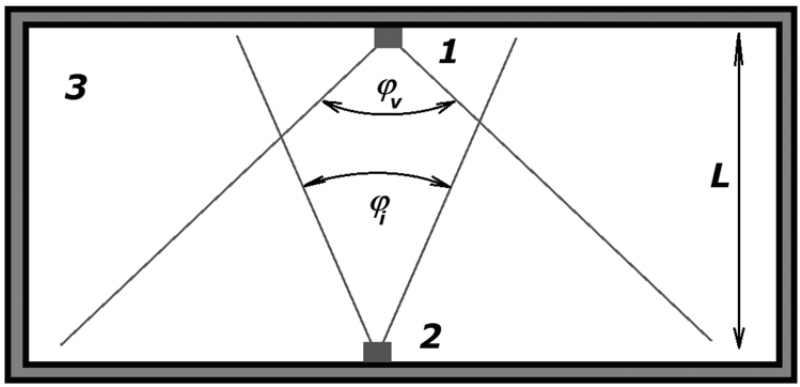

Рис. 7. Схема расположения видеокамеры (1)
и ИК-прожектора (2) в защищаемом помещении (3),
где φ_v – угол поля зрения видеокамеры,
φ_i – угол обзора ИК-прожектора,
L – расстояние между стенами

Применение ИК засветки имеет свои преимущества кроме защитных функций. Использование инфракрасного излучения не оказывает влияние на комфортабельность освещения в защищаемом помещении, при этом само излучение оказывает положительное воздействие на человека, как обычное тепловое излучение. Переменное ИК излучение в отличие от непрерывного понижает энергетические затраты на защиту в 1,5 раза. Управление засветкой может производиться дистанционно или централизованно из помещений служб безопасности.

3.2. Предложение по защите офисного помещения. Обсудим некоторые аспекты защиты помещения от скрытого видеонаблюдения в соответствии с поставленной задачей. Основное требование к защитной ИК засветке состоит в равномерности освещения по всем направлениям с переменной мощностью, амплитуда которого должна определяться уровнем фонового освещения в видимой области

и определенной структуре размещения ИК источников излучения. Достижение этой цели можно осуществить путем равномерного ИК освещения по периметру защищаемого помещения (рис. 8). Наиболее эффективное расположение ИК-прожекторов с углом обзора не менее 60° на уровне двух метров от пола по длине всего периметра для обеспечения наибольшего охвата стен помещения. Плотность расположения камер связывается с углом поля зрения камеры (в нашей оценке не менее 60°). Все источники, попадающие в угол поля зрения, дают вклад в засветку, поэтому в зависимости от мощности ИК источников плотность расположения будет определяться длиной охвата периметра модельной видеокамеры по противоположной стене как наиболее удаленных участков.

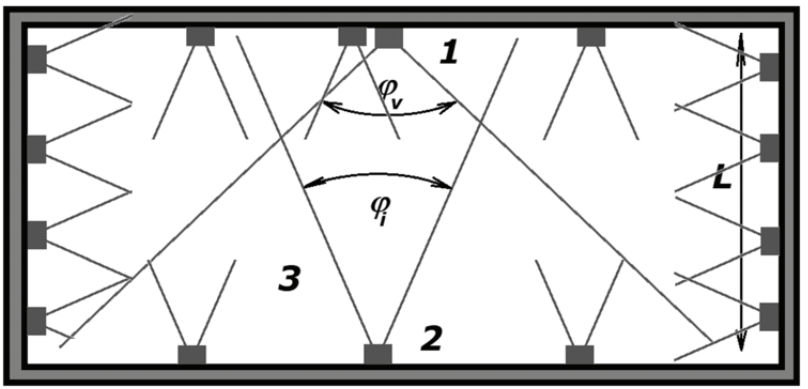

Рис. 8. Принципиальная схема расположения нейтрализующих скрытую видеокамеру (1) ИК-прожекторов (2) в защищаемом помещении (3)

Эффективная засветка требует n камер мощностью N каждая, т. е. засветка обеспечивается интенсивностью ИК излучения порядка $I_0 = nkN/L^2$, тогда плотность размещения ИК источников по периметру составит

$$\frac{L}{n}\sin\left(\varphi_v/2\right).$$

Линейное по стене расположение источников засветки не является самым эффективным, так же как засветка одним источником. Формирование «смаза» и перетекание заряда по пикселам ПЗС-матрицы происходит более эффективно, если точки формирования распределены по матрице, тогда засветка происходит более

быстро и охватывает всю матрицу с первых моментов воздействия. Распределение ИК источников в шахматном порядке по стене защищаемого помещения при большем числе источников с меньшей мощностью создаст более эффективную и однородную засветку при более быстром формировании деструктивного воздействия на изображение. В этом случае модуляцию засветки потребуется производить на большей частоте, чтобы отследить восстановление эффективной экспозиции электроникой камеры. Дополнительно эффективность защиты можно повысить использованием источников ИК излучения различной мощности, когда источники большей мощности за меньшее время формируют точечную засветку, а источники с меньшей мощностью формируют однородное по изображению засветку. Мощные источники ИК излучения можно разместить по углам помещения у потолка.

Эффективность функционирования засветки может быть повышена путем встраивания в существующие настольные и потолочные светодиодные лампы ИК диодов с возможностью электронного управления по силовым электрическим сетям. Дополнительные встроенные ИК диоды позволят более равномерно осветить инфракрасным излучением помещение и не допустить образования неосвещенных участков и направлений.

3.3. Лабораторное моделирование скрытого видеонаблюдения на базе веб-камеры персонального компьютера. На основе проведенных практических исследований по засветке веб-камеры видимым светом и инфракрасным излучением предложено включить в изучение физики разведки и защиты информации (дисциплина «Физические основы защиты информации») данные исследования. Знание работы веб-камеры и воздействия на нее внешних излучений позволит понять работу систем скрытого видеонаблюдения и возможности воздействия на нее с целью нейтрализации. Для этого была разработана конструкция лабораторной экспериментальной установки и предложены упражнения по проведению измерений параметров источников света и работы веб-камеры.

Экспериментальная установка (рис. 9) состоит из источников видимого белого (1) и инфракрасного (2) оптического излучения, которые направлены и находятся на изменяемом расстоянии от фотоэлемента (3) люксметра Ю116 с измерительным блоком (6), регистрирующего освещенность веб-камеры Logitech Webcam C200 (4), и персонального компьютера для контроля видеоизображения от веб-камеры.

Источник (1) имеет диаграмму направленности, близкой к прожекторному источнику видимого света, в качестве источника инфракрасного излучения (2) используется уличный ИК-про-

жектор подсветки в темное время суток для видеонаблюдения KDM-6044A. С помощью фотоэлемента (3) с насадками можно контролировать освещенность создаваемой на входе веб-камеры по гальванометру (6) люксметра Ю116. Качество формируемого изображения от веб-камеры Logitech Webcam C200 контролируется по монитору персонального компьютера.

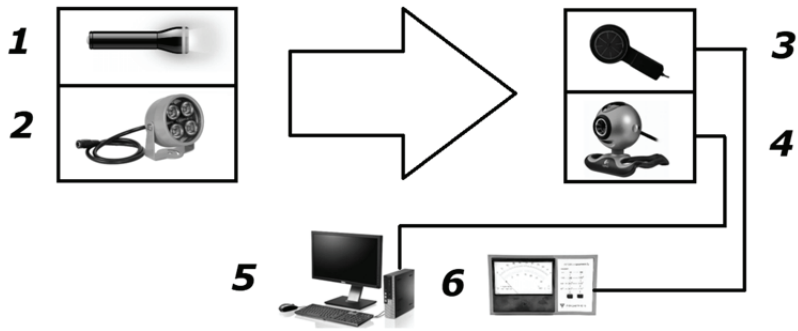

Рис. 9. Блок-схема экспериментальной установки
по исследованию воздействия оптического излучения на веб-камеру:
1 – источник видимого (белого) излучения;
2 – источник инфракрасного излучения;
3 – фотоэлемент с насадками люксметра Ю116;
4 – веб-камера Logitech Webcam C200;
5 – персональный компьютер,
6 – гальванометр люксметра Ю116

В качестве упражнений по изучению работы оптических систем и видеонаблюдения предлагается исследовать световые характеристики источников оптического излучения; оптические характеристики веб-камеры. На основе проведенных исследований провести обработку и в отчете представить следующие характеристики: графики зависимости освещенности от расстояния; коэффициент эффективности засветки ИК излучением χ; глубину модуляции для эффективной засветки веб-камеры η_w и η_{ir}.

Заключение

Представленный качественный анализ и экспериментальные исследования показывают возможность эффективного противодействия скрытому видеонаблюдению путем инфракрасной засветки

защищаемого помещения, которое не влияет на комфортабельность нахождения в помещении. Разработанная методика измерений может быть эффективно использована при подготовке специалистов в области защиты информации.

Литература

Алферов 2012 – *Алферов В.Ю., Федюнин А.Е., Перетятько Н.М.* Специальная техника органов внутренних дел. Использование средств оперативного наблюдения в борьбе с преступностью: Учеб. пособие. Саратов: ССЭИ РЭУ им. Г.В. Плеханова, 2012. 88 с.

Гонта 2006 – *Гонта А.С.* Характеристики изображения: контраст, динамический диапазон, резкость // Алгоритм безопасности. 2006. № 5. С. 56–60.

Гонта 2007 – *Гонта А.С.* Резкость изображения и оборудование CCTV // Алгоритм безопасности. 2007. № 1. С. 30–32.

Гридин 1983 – *Гридин А.С., Салин В.И., Сущев Г.А., Подгорский Е.Г., Ратников А.Н., Трофимов М.Н.* Оценка устойчивости фотоприемника на ПЗС к световым перегрузкам // Техника средств связи, серия «Техника телевидения». 1983. Вып. 2. С. 28–32.

Дамьяновски Владо 2020 – *Дамьяновски Владо.* Библия видеонаблюдения: Пер. с англ. М.: Секьюрити фокус, 2020. 470 с. (Серия «Энциклопедия безопасности»)

Куликов 2001 – *Куликов А.Н.* Телевизионное наблюдение при ярком солнечном свете // Специальная техника. 2001. № 1. С. 11–20.

Куликов 2002 – *Куликов А.Н.* Реальная разрешающая способность телевизионной камеры // Специальная техника. 2002. № 2. С. 20–26.

Смелков 2001 – *Смелков В.М.* Метод минимизации искажений телевизионной камеры при работе в условиях световой перегрузки // Специальная техника. 2001. № 5. С. 13–17.

Смелков 2004 – *Смелков В.М.* Оценка времени восстановления телевизионной камеры на ПЗС-матрице после воздействия световой перегрузки // Специальная техника. 2004. № 1. С. 34–41.

Тельный 2013 – *Тельный А.В.* Инженерно-техническая защита информации. Системы охранного телевидения: Учеб. пособие. Владимир: ВлГУ, 2013. 144 с.

Хацевич 2002 – *Хацевич Т.Н., Михайлов И.О.* Эндоскопы: Учеб. пособие. Новосибирск: СГГА, 2002. 196 с.

Уваров 2006 – *Уваров Н.Е.* Средства повышения контраста ТВ-изображений // Грани безопасности. 2006. № 2 (38). С. 22–25.

Уваров 2001 – *Уваров Н.Е.* Динамика воспроизведения контраста ТВ-камерой // БДИ. 2001. № 6.

Хорев 2008 – *Хорев А.А.* Техническая защита информации: Учеб. пособие для студентов вузов: В 3 т. Т. 1: Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. 436 с.

Хорев 2010 – *Хорев А.А.* Средства скрытого видеонаблюдения и съемки (по материалам иностранной печати) // Специальная техника. 2010. № 3. С. 2–23.

Хорев 2015 – *Хорев А.А.* Средства выявления систем скрытого видеонаблюдения // Специальная техника. 2015. № 6. С. 53–61.

References

Alferov, V.Yu., Fedyunin, A.E. and Peretyatko, N.M. (2012), *Spetsial'naya tekhnika organov vnutrennikh del. Ispol'zovanie sredstv operativnogo nablyudeniya v bor'be s prestupnost'yu: ucheb. posobie* [Using of special equipment by the internal affairs bodies. The use of operational surveillance tools in the fight against crime. Study guide], SSEI REU im. G.V. Plekhanova, Saratov, Russia.

Dam'yanovski Vlado (2020), *Bibliya videonablyudeniya: Per. s angl.* [Video Surveillance Bible. Transl. from English], Security focus, Moscow, Russia. (Series "Encyclopedia of Security")

Gonta, A.S. (2007), "Image sharpness and CCTV equipment", *Security algorithm*, no. 1. pp. 30–32.

Gonta, A.S. (2006), "Image characteristics. Contrast, dynamic range, sharpness", *Special'naya tekhnika*, no. 5. pp. 56–60.

Gridin, A.S., Salin, V.I., Sushchev, G.A., Podgorsky, E.G., Ratnikov, A.N. and Trofimov, M.N. (1983), "Assessment of the stability of a CCD photodetector to light overloads", *Communications equipment, series "Television Equipment"*, issue 2, pp. 28–32.

Hatsevich, T.N. and Mikhailov, I.O. (2002), *Endoskopy: ucheb. posobie.* [Endoscopes. Study guide], SGGA, Novosibirsk, Russia.

Horev, A.A. (2015), "Means of detecting hidden video surveillance systems", *Special'naya tekhnika*, no. 6, pp. 53–61.

Horev, A.A. (2008), *Tekhnicheskaya zashchita informatsii: ucheb. posobie dlya studentov vuzov. V 3 t. Tom 1. Tekhnicheskie kanaly utechki informatsii* [Technical protection of information: Study guide for students. In 3 vols. Vol. 1. Technical channels of information leakage], NPC "Analytics", Moscow, Russia.

Horev, A.A. (2010), "Means of hidden video surveillance and shooting (based on foreign press materials)", *Special'naya tekhnika*, no. 3, pp. 2–23.

Kulikov, A.N. (2001), "Television surveillance in bright sunlight", *Special'naya tekhnika*, no. 1, pp. 11–20.

Kulikov, A.N. (2002), "Real resolution of a television camera", *Special'naya tekhnika*, no. 2, pp. 20–26.

Smelkov, V.M. (2001), "Method of minimizing distortions of a television camera when working under conditions of the light overload", *Special'naya tekhnika*, no. 5, pp. 13–17.

Smelkov, V.M. (2004), "Estimation of the recovery time for a television camera on a CCD matrix after exposure to the light overload", *Special'naya tekhnika*, no. 1, pp. 34–41.

Tel'nyi, A.V. (2013), *Inzhenerno-tekhnicheskaya zashchita informatsii. Sistemy okhrannogo televideniya: ucheb. posobie* [Engineering and technical protection of information. Security television systems. Study guide], VlSU, Vladimir, Russia.

Uvarov, N.E. (2006), "Means of increasing the contrast of TV images", *Facets of security*, no. 2 (38), pp. 22–25.

Uvarov, N.E. (2001), "Dynamics of the contrast reproduction by a TV camera", *Security, Reliability, Information (BDI)*, no. 6.

Информация об авторах

Владимир В. Гришачев, кандидат физико-математических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; grishachev@mail.ru

Виктория Э. Щеголева, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; vischglv@gmail.com

Information about the author

Vladimir V. Grishachev, Cand. of Sci. (Physics and Mathematics), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; grishachev@mail.ru

Viktoriya E. Schegoleva, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; vischglv@gmail.com

УДК 003.26
DOI: 10.28995/2686-679X-2023-4-92-107

Криптографическое значение манускрипта Войнича

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Аннотация. В статье проводится анализ современных подходов к дешифрованию текста манускрипта Войнича. Работа содержит краткий обзор истории обнаружения рукописи и анализ основных версий об авторстве и первых владельцах манускрипта, месте и времени его создания и его содержании. Уделяется внимание изучению ключевых подходов к определению криптографических методов, которые могли использоваться автором или авторами сочинения, и анализу проблем дешифрования текста рукописи, стоящих перед современными исследователями. В статье проводится обзор других зашифрованных рукописей, время и место создания которых позволяют провести сравнение с манускриптом Войнича по ряду выделенных критериев. Особое внимание уделяется анализу проблем определения языка манускрипта, который предполагает выбор одного или нескольких естественных языков, относящихся к той или иной языковой группе, искусственного языка или «языка», состоящего из беспорядочного набора символов. Рассматриваются проблемы транслитерации символов рукописи, используемых для создания машиночитаемых версий текста. Проводится анализ перспектив изучения криптографического содержания рукописи. Уделяется внимание содержанию ряда докладов международной конференции, посвященной исследованию манускрипта Войнича, проведенной Университетом Мальты в ноябре–декабре 2022 г. Автором подчеркивается необходимость междисциплинарного подхода к изучению рукописи Войнича, требующего объединения усилий криптологов, математиков, историков, филологов, лингвистов для успешной разгадки содержания манускрипта Войнича.

Ключевые слова: манускрипт Войнича, криптография, история криптографии, шифрование

Для цитирования: Русецкая И.А. Криптографическое значение манускрипта Войнича // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 92–107. DOI: 10.28995/2686-679X-2023-4-92-107

Cryptographic meaning of the Voynich manuscript

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia;
irkom@mail.ru

Abstract. The article analyzes modern approaches to deciphering the text of the Voynich manuscript. The work contains a brief overview in the history of the manuscript discovery and an analysis of the main versions about the authorship and the first owners of the manuscript, the place and time of its creation and its content. The author pays attention to the study of key approaches to the definition of cryptographic methods that could be used by the author or authors of the essay and the analysis of the manuscript text decrypting issues facing modern researchers. The article provides a review of other encrypted manuscripts, the time and place of creation of which allow comparison with the Voynich manuscript according to a number of selected criteria. Particular attention is paid to analyzing the challenges of defining the manuscript language, what involves the choice of one or more natural languages within one or the other language group, an artificial language or "language" consisting of a random set of characters. Difficulties with transliteration of manuscript symbols used to create machine-readable versions of the text are considered. An analysis of the prospects for studying the cryptographic content of the manuscript is carried out. Attention is paid to the content of a number of reports of the international conference on the study of the Voynich manuscript, held by the University of Malta in November–December 2022. The author emphasizes the need for an interdisciplinary approach to the study of the Voynich manuscript, which requires the combined efforts of cryptologists, mathematicians, historians, philologists, linguists to successfully unravel the content of the manuscript Voynich.

Keywords: Voynich manuscript, cryptography, history of cryptography, encryption

For citation: Rusetskaya, I.A. (2023), "Cryptographic meaning of the Voynich manuscript", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 92–107, DOI: 10.28995/2686-679X-2023-4-92-107

Введение

Рукопись, получившая название «манускрипт Войнича», является до настоящего времени одной из самых загадочных рукописей: неизвестно ни имя (или имена) ее авторов, ни время и место ее создания, ни содержание текста и смысл сопровождающих

его иллюстраций. Изучением рукописи Войнича на протяжении многих десятилетий занимались историки, лингвисты, филологи и криптологи разных стран. Криптографическое значение манускрипта может считаться одним из наиболее важных, поскольку именно инструменты, находящиеся в распоряжении криптологов, могут позволить наконец раскрыть содержание текста.

Тема изучения и расшифровки содержания рукописи Войнича остается актуальной до настоящего времени, свидетельством чему может служить множество появляющихся научных публикаций, организация исследовательских коллективов и конференций. Так, международной конференцией, посвященной исследованию манускрипта Войнича, стала International Conference on the Voynich Manuscript, проведенная Университетом Мальты в ноябре–декабре 2022 г.[1]

Целью данной работы является анализ современных тенденций в изучении криптографического содержания рукописи Войнича.

Так как в рамках небольшого исследования не представляется возможным раскрыть все аспекты рассматриваемой темы, в данной статье будет сделан акцент на анализе следующих вопросов:

– краткий обзор истории обнаружения рукописи и анализ основных версий об авторстве манускрипта, месте и времени его создания и его содержании;
– изучение основных подходов к определению криптографических методов, которые могли использоваться автором сочинения;
– анализ проблем дешифрования текста рукописи, стоящих перед исследователями;
– обзор других зашифрованных рукописей, время и место создания которых позволяют провести сравнение с манускриптом Войнича по выделенным критериям;
– анализ перспектив изучения криптографического содержания рукописи.

Анализ рукописи Войнича и основных подходов к дешифрованию текста

Рукопись Войнича получила свое название по имени антиквара и библиофила Вильфрида Михала Войнича (1865–1930), который случайно обнаружил ее в монастыре иезуитов в Италии в 1912 г.

[1] International Conference on the Voynich Manuscript. URL: https://www.um.edu.mt/event/voynich2022 (дата обращения 25.06.2023).

Войнич, представитель дворянского польско-литовского рода, родился на территории Российской империи, за участие в социал-демократическом движении был арестован и сослан в Сибирь, откуда бежал в Германию, затем перебрался в Лондон, а позднее поселился в Нью-Йорке, занимаясь антикварным бизнесом. После находки рукописи Войнич много времени посвятил попыткам раскрыть ее содержание, в том числе с помощью профессиональных исследователей криптограмм, но не добился успеха. В 1961 г. манускрипт был куплен у вдовы Войнича[2] и несколько лет спустя подарен библиотеке редких книг Бейнеке Йельского университета США[3].

Оригинал рукописи до настоящего времени находится в библиотеке Йельского Университета, которая предлагает всем желающим ознакомиться с электронной версией манускрипта[4]. Существует также много печатных репринтных изданий рукописи, в частности вышедшее в России с предисловием С. Зотова [Манускрипт Войнича 2021].

Рукопись включает в себя около 240 страниц текста. Приблизительность подсчета связана с тем, что некоторые страницы удлинены по горизонтали и сложены. По всей вероятности, в манускрипте не хватает еще около 32 страниц.

Радиоуглеродный анализ 2009 г. показал, что манускрипт создан в Европе, текст его был написан несколькими людьми, по меньшей мере двумя; иллюстрации также были созданы несколькими авторами[5]. Документ был написан птичьим пером железо-галловыми чернилами[6]. Они получались из так называемых «чер-

---

[2] Жена В.М. Войнича Этель Лилиан Войнич (1864–1960) была дочерью знаменитого математика Джорджа Буля и стала автором широко читаемого в России и СССР романа «Овод», двух его менее известных приквелов, а также отчасти автобиографического романа о полной лишений жизни английской девушки в царской России.

[3] *Katz F.P.* From Voynich to the Beinecke // Proceedings of the 1st International Conference on the Voynich Manuscript 2022. November 30–December 1, 2022. University of Malta. URL: https://ceur-ws.org/Vol-3313/paper14.pdf (дата обращения 28.06.2023).

[4] Voynich manuscript // Yale University library. Beinecke Rare Book and Manuscript Library. Beinecke MS 408. URL: https://collections.library.yale.edu/catalog/2002046 (дата обращения 25.06.2023).

[5] *Zandbergen R.* Radio-carbon dating of the Voynich MS. 2022. URL: http://www.voynich.nu/extra/carbon.html (дата обращения 10.06.2023).

[6] *Домнина Е.* Манускрипт Войнича // Постнаука, 30.05.2017. URL: https://postnauka.org/faq/75490 (дата обращения 12.08.2023).

нильных орешков», которые представляют собой образуемые личинками насекомых наросты на листьях и ветвях некоторых видов дубов. Пергамен, изготовленный из выделанной телячьей кожи, датируется первой половиной XV в., как и текст с иллюстрациями. Анализ почерка писца указывает на то, что алфавит был ему знаком: за одно обмакивание пера у него получалось написать около восьми слов. Маргиналии, представляющие собой заметки на полях рукописи, составляют записи из латинских букв, а также символов алфавита, отличающегося от алфавита, использующегося в основном тексте. Так, найденные внутри рисунков растений и под краской отдельные латинские буквы и слово *rot* (нем. «красный»), возможно, являлись указаниями на цвет рисунка от автора текста[7].

Иллюстрации были сделаны зеленой, синей, белой и красно-коричневой красками из природных компонентов. На некоторых иллюстрациях заметны следы выцветшей желтой краски.

Текст манускрипта Войнича написан разборчивым, но неизвестным шрифтом, состоящим из знаков, собранных в слова, которые разделены пробелами. Всего в тексте насчитывается более 170 тыс. знаков, хотя алфавит и невелик (20–30 букв), если считать, что используемые символы можно назвать буквами, выражающими отдельные звуки или слоги.

Манускрипт не является палимпсестом, то есть на использованном пергамене не был нанесен текст, позднее соскобленный.

Можно предполагать, что писцу и иллюстратору (или коллективу авторов) потребовалось не меньше года работы над рукописью.

Текст рукописи, по всей вероятности, так же как пергамен и чернила, был создан в Европе. В качестве косвенных свидетельств этого могут выступать характерные для многих западноевропейских рукописей (например, травников и сочинений по астрологии) ботанические рисунки, круговые астрологические диаграммы; изображение замка с крепостной стеной, украшенной зубцами в виде ласточкиного хвоста, что напоминает об итальянских постройках, и т. п.

Группировка иллюстраций в книге позволила условно разделить ее на несколько разделов: ботанический, астрономический, биологический (бальнеологический), космологический, фармацевтический и рецептный.

Ботаническая часть содержит рисунки различных растений, большая часть которых не идентифицируется однозначно.

---

[7] *Шкляева Т.* Загадки манускрипта Войнича // Nasledie.digital, 26.12.2022. URL: https://nasledie.digital/articles/zagadki-manuskripta-vojnicha/?ysclid=ll53yrxfor698918372 (дата обращения 27.06.2023).

Астрономическая часть, состоящая из изображения диаграмм, включает астрологические и различные другие символы, в том числе знаки зодиака. К некоторым диаграммам есть текстовые пояснения.

Иллюстрации биологического раздела представляют собой по большей части изображения купающихся обнаженных женщин.

Изображения космологической части включают круговые диаграммы неизвестного содержания, отдаленно напоминающие карты местности; на них также изображаются замки и вулкан.

Фармакологическая часть иллюстраций представляет собой изображения растений и отдельных их частей, таких как корни и листья.

Наконец, последняя, рецептная часть не включает в себя иллюстрации, а текст ее делится на абзацы или разделы, каждый из которых отмечен изображением цветка или звезды.

Автор манускрипта неизвестен, и хотя версий выдвигалось множество, ни одна из них не может считаться убедительной.

Существуют подтвержденные письменными источниками предположения о нескольких первых владельцах рукописи.

По всей вероятности, манускрипт мог быть куплен для библиотеки императора Рудольфа II в 1599 г. у медика Карла Видеманна, который был дружен с врачом, ботаником и исследователем Востока Леонардом Раувольфом[8].

Рукопись, вероятно, находилась в распоряжении Якоба Хорчицкого (1575–1622), известного также как Якоб Синапий, медика, алхимика и личного врача Рудольфа II, а также куратора его ботанического сада.

Подтвержденным владельцем книги был пражский алхимик Георг (Йиржи) Барш (Georgius Barschius). Отправленное им в 1639 г. письмо иезуиту Атанасию Кирхеру (1602–1680), прославившемуся среди современников как знаток египтологии, с просьбой расшифровать таинственный текст, было обнаружено современным исследователем Рене Цандбергеном [Prinke, Zandbergen 2017].

Вместе с манускриптом Войнич приобрел вложенное в него письмо, датируемое 1665 или 1666 г., в котором врач, ученый и ректор Пражского университета Ян Маркус Марци (1595–1667) также обращается к Атанасию Кирхеру с просьбой о дешифровке.

По всей вероятности, затем рукопись хранилась вместе с остальной перепиской Кирхера в распоряжении ордена иезуитов.

---

[8] *Guzy S.* Book Transactions of Emperor Rudolf II, 1576–1612: New Findings on the Earliest Ownership of the Voynich Manuscript // Proceedings of the 1st International Conference on the Voynich Manuscript 2022.

Рассмотрим основные использованные подходы к дешифрованию текста рукописи.

Одной из основных проблем при дешифровании является определение языка, на котором написан манускрипт Войнича.

По признаку происхождения языка существует два варианта ответа на этот вопрос: язык может являться естественным или искусственным.

К числу предполагаемых естественных языков исследователи относят:

1. Романо-германские, в том числе их микс. Использование в рукописи языков этой группы считается наиболее вероятным. При этом «латинская» гипотеза происхождения манускрипта была одной из основных на протяжении XX в. Так, гипотеза Джозефа Фили, выдвинутая им в 1943 г., состояла в том, что манускрипт написан на средневековой латыни с использованием сокращений, без огласовки, пробелов и некоторых повторяющихся слогов. Почти во всем тексте латынь «реверсивна», то есть зеркально развернута [Быченков 2019]. По версии российской группы ученых из Института прикладной математики им. М.В. Келдыша, проводившей сравнительный анализ статистических закономерностей европейских языков и манускрипта Войнича, текст рукописи написан на смешанном языке с пропуском гласных, при этом 60% текста написано на одном из языков западногерманской группы (английский/немецкий), а 40% текста – на языке романской группы (итальянский/испанский) и/или на латинском[9].

2. Семитские языки. Так, по недавней версии 2020 г. египтолога Райнера Ханнига, в манускрипте использовался один из семитских языков, смешанный с латынью[10]. Версии с использованием иврита придерживается и Г. Кондрак, использовавший для дешифрования текста нейросети[11].

---

[9] *Арутюнов А.А.* Статистические закономерности европейских языков и анализ рукописи Войнича / А.А. Арутюнов [и др.] // Препринты ИПМ им. М.В. Келдыша. 2016. № 52. 36 с. URL: http://library.keldysh.ru/preprint.asp?id=2016-52 (дата обращения 25.06.2023).

[10] *Shaw G.* The Voynich Manuscript's mysteries endure more than a century after its discovery // The Art Newspaper 25 August 2022. URL: https://www.theartnewspaper.com/2022/08/25/voynich-manuscript-mystery-explainer (дата обращения 10.07.2023).

[11] *Hauer B., Kondrak G.* Decoding Anagrammed Texts Written in an Unknown Language and Script // Transactions of the Association for Computational Linguistics. 2016. T. 4. P. 75–86. URL: https://transacl.org/ojs/index.php/tacl/article/view/821/174 (дата обращения 29.06.2023).

3. Славянские языки. Например, в 1978 г. филолог Джон Стожко предположил, что в рукопись написана на украинском языке без использования гласных.

4. Экзотические языки (например, сино-тибетской или австроазиатской групп).

5. Исчезнувшие сегодня, так называемые мертвые языки, в том числе относящиеся к рассмотренным выше языковым группам. Например, по одной из маловероятных гипотез, это мог быть язык, используемый христианским еретическим движением катаров в средневековой Европе (Лео Левитов, 1987 г.), или «протороманский язык», который представляет собой фактически название для народной латыни (Джерард Чешир, 2019 г.), и др. Последние два варианта языков относятся к романо-германской группе. Гипотезы об использовании «забытого языка» придерживается также физик из Манчестерского университета Марчело Монтемурро (версия выдвинута в публичном докладе 2013 г.).

У ряда исследователей возникла концепция использования автором рукописи искусственного языка. Предпосылкой для рассмотрения такой гипотезы может считаться своеобразная внутренняя структура «слов» в рукописи, описанная выше. Такую концепцию рассматривал, например, Уильям Фридман (1891–1969), который считается «отцом американской криптологии» и прославился, в частности, взломом японского «Пурпурного кода» (Purple code) в начале Второй мировой войны. Фридман предположил, что текст манускрипта написан на специально созданном для этого искусственном языке.

Из известных более чем ста искусственных языков большая часть базируется на тех или иных принципах объединения нескольких естественных языков (как, например, эсперанто, интерлингва, волапюк и др.). И хотя можно привести примеры языков, на которых общаются придуманные герои литературных сочинений (например, «эльфийский» язык квенья Дж.Р.Р. Толкина), по мнению исследователей, они незначительно отличаются от естественных по своим статистическим характеристикам[12].

При использовании любого из этих языков возможно его как случайное, так и умышленное видоизменение, создающее сложности при дешифровании рукописи:

– применение аббревиатур;
– использование «смеси» из двух и более языков;
– пропуск определенных букв, например обозначающих гласные звуки;

[12] *Арутюнов А.А.* Указ. соч.

– ложные пробелы между словами;
– добавление бессмысленных символов-«пустышек»;
– ошибки и неграмотность составителя текста;
– искажение порядка расположения слов в ряде мест рукописи из-за неправильного порядка нумерации листов манускрипта и пр.

В дополнение к указанным сложностям необходимо рассматривать возможность шифрования текста автором рукописи. В таком случае, принимая за гипотезу, что рукопись создана европейскими авторами в раннее Новое время и учитывая развитие идей криптографии в Европе в этот период, можно предположить, что в тексте манускрипта, вероятнее всего, использовались следующие криптографические методы (один из них или несколько):

– шифр перестановки, предполагающий перестановку знаков внутри текста в соответствии с определенными правилами;
– шифр простой замены, предполагающий замену каждой буквы в тексте определенным символом или набором символов;
– применение полиалфавитного шифра замены, то есть использование одинаковых знаков, которые в разных частях рукописи соответствуют разным буквам, при этом существует утерянный ключ, без которого нельзя прочесть текст;
– кодирование двух и более символов языка одним символом рукописи [Русецкая 2014].

Рассматривая версии об определении языка, на котором написана рукопись, следует также учесть вероятность того, что текст является мистификацией, то есть представляет собой бессмысленный набор знаков. Например, британские исследователи Г. Рагг и Г. Тайлор в начале 2000-х гг. выступили с утверждением, что рукопись Войнича представляет собой мистификацию и лишь создает видимость осмысленного текста [Rugg, Taylor 2016].

Однако большинство исследователей придерживаются версии о том, что манускрипт имеет строгое лингвистическое построение, а не представляет собой случайный набор символов. Об этом говорят, например, повторяющиеся слова. Так, в ботаническом разделе употребляются одни специфические слова, а в астрономическом – другие. Текст рукописи можно считать осмысленным и на основании статистических подсчетов, в противном случае отклонение от статистики букв, являющейся характерной для словаря естественного языка, было бы существенно больше[13].

[13] *Арутюнов А.А.* Указ. соч.

Для компьютерного дешифрования манускрипта необходима транслитерация использованных символов, например, в латиницу для создания машиночитаемой версии текста. Такая транслитерация также наталкивается на ряд сложностей, связанных с особенностями рукописного текста и определением того, что должно являться транслитерируемым знаком, а значит, какое количество каких именно символов можно выделить в тексте. Первую машиночитаемую версию текста манускрипта предложил Фридман в 1946 г.[14]

Наиболее распространенными сегодня можно считать так называемую «европейскую транскрипцию» отображения знаков манускрипта в латиницу EVA, а также транскрипцию Takahashi с другими частотами выделенных символов. Существуют более точные транслитерации, но они часто считаются слишком сложными в использовании. Существует также вариант с использованием надмножества всех существующих транслитерационных алфавитов, который позволяет представить все транслитерации в одном «супералфавите»[15].

В заключение следует остановиться на том, что если предполагать, что текст манускрипта зашифрован, то следует учитывать, что рукопись Войнича является далеко не единственным зашифрованным сочинением и при попытках ее дешифрования имеет смысл проанализировать особенности других произведений, которые удалось расшифровать, а также причины, по которым они были зашифрованы. При этом сравнение с манускриптом Войнича можно проводить по нескольким критериям, например по вероятности совпадения тематики сочинения и типу использованных операций с символами текста.

Так, современные исследователи Элонка Дунин и Клаус Шмех проанализировали книги из списка 118 зашифрованных книг, включающего манускрипт Войнича, 78 из которых являются рукописями, а остальные печатными изданиями[16].

Проведенная авторами классификация рукописей по их назначению включает следующие 10 видов:

---

[14] *Reeds J.* William F. Friedman's Transcription of the Voynich Manuscript. URL: https://www.ic.unicamp.br/~stolfi/voynich/mirror/reeds/docs/wff.pdf (дата обращения 30.07.2023).

[15] *Zandbergen R.* Transliteration of the Voynich MS text // Proceedings of the 1st International Conference on the Voynich Manuscript 2022.

[16] *Schmeh K.* List of Encrypted Books, 2022. URL: https://scienceblogs.de/klausis-krypto kolumne/klaus-schmehs-list-of-encrypted-books/ (дата обращения 25.06.2023).

– дневники;
– сочинения, касающиеся тайных обществ;
– записные книжки (по сравнению с дневниками записные книжки обычно не датированы и часто слабо структурированы);
– религиозные сочинения;
– оккультные книги, содержащие в себе тайное знание;
– литературные произведения: романы, мемуары, сборники стихов;
– тексты, созданные как криптозагадки;
– мистификации, то есть тексты, напоминающие шифрованные, но с бессмысленным содержанием;
– произведения искусства, в которых шифрование является частью художественного замысла;
– иные сочинения, не отнесенные к перечисленным группам в силу недостатка информации, к которым можно отнести, например, тексты, созданные людьми, находящимися в состоянии измененного сознания[17]. Подобная версия выдвигалась и в отношении рукописи Войнича в середине 2000-х гг. американскими лингвистами Джерри Кенеди и Робом Черчиллем, которые сделали предположение, что автор рукописи находился в состоянии транса. Исследователи обратили внимание на то, что иллюстрации манускрипта напоминают рисунки Хильдегарды Бингенской, немецкой средневековой монахини, автора сохранившихся записей о мистических видениях.

На основе анализа текстов, относящихся к каждой из перечисленных групп, авторы исследования делают вывод о том, что рукопись Войнича, вероятнее всего, может быть отнесена к одной из двух категорий: к сочинениям-мистификациям и к трудам, заключающим в себе тайное знание.

Рассматривая классификацию зашифрованных сочинений по времени их создания, авторы приходят к выводу, что рукопись Войнича является одной из старейших или даже самой старой работой в их виртуальной коллекции.

Помимо рукописи Войнича, в XV в. были создано еще пять книг из упоминаемого списка, имеющих некоторое визуальное сходство с манускриптом Войнича и созданных примерно в то же время. Три из них были написаны инженером и врачом из

[17] *Dunin E., Schmeh K.* The Voynich Manuscript Compared with Other Encrypted Books // Proceedings of the 1st International Conference on the Voynich Manuscript 2022.

Венеции Джованни Фонтана (1395–1455). В его сочинениях описывается широкий ряд технических конструкций, текст сопровождается многочисленными иллюстрациями, на многих из которых показаны устройства, которые на практике вряд ли смогли бы работать. Часть текста этих трех книг зашифрована. Еще одна зашифрованная книга, созданная в 1426 г., по всей вероятности, в Баварии – Codex Palatinus Germanicus 597, трактат о магии, алхимии и астрологии с иллюстрациями, хранящийся в Университетской библиотеке Гейдельберга[18]. Значительная часть рукописи написана с помощью шифра (который был вскрыт в наши дни). Еще одна зашифрованная книга XV в. – третья часть «Стеганографии» Иоанна Тритемия (1462–1516), которую долго не удавалось вскрыть из-за отсутствия ключа. Тритемий использовал в этой части своей работы пример шифра, построенного на принципах многоалфавитной замены букв цифрами, которая рассматривалась им самим в шестой книге его сочинения «Полиграфия», содержащей описание различных способов шифрования [Ernst 1998]. Среди современных исследователей версия о том, что «Стеганография» имеет главным образом криптографическое содержание, а не является пособием по черной магии, предлагающим читателям методы общения с духами, является наиболее распространенной среди исследователей [Русецкая 2017].

Таким образом, все пять сочинений, написанных примерно в ту же эпоху, что и рукопись Войнича, из рассматриваемого списка либо являются книгами, скрывающими секретное знание от непосвященных, либо мистификациями.

Из 118 зашифрованных книг из рассматриваемого списка только 15 не расшифрованы к настоящему моменту, а все остальные уже удалось прочесть. За исключением манускрипта Войнича, все прочие нерасшифрованные произведения были созданы за последние 100 лет. Стоит выделить две зашифрованные книги XV–XVI вв., которые были раскрыты относительно недавно – за последние 30 лет. Это Кодекс Рохонци[19] и «Книга Soyga» («Альдарайя»). Как и манускрипт Войнича, эти сочинения представляли собой загадку для ученых на протяжении нескольких веков. Кодекс

[18] Codex Palatinus Germanicus 597 – ‘Cisioianus’; Sammlung alchemischer und medizinischer Rezepte und Traktate. Universitätsbibliothek Heidelberg. URL: https://www.ciphermysteries.com/2009/05/15/cod-pal-germ-597s-cipher (дата обращения 25.07.2023).

[19] Цифровую версию Кодекса Рохонци можно найти здесь: Dacia.org. URL: https://www.dacia.org/codex/original/original (дата обращения 11.08.2023).

Рохонци – это сочинение религиозного содержания, написанное неизвестными символами. «Книга Soyga» – трактат по магии, демонологии и астрологии. Хотя исследователь Джим Ридс расшифровал алгоритм построения и кодовые слова, использованные при создании таблиц сочинения, их содержание и значение остаются не до конца понятными[20].

Если рассматривать криптографическое содержание зашифрованных книг из указанного списка, то из 118 книг в 62 использовался моноалфавитный шифр замены. «Книга Soyga» содержит последовательности букв, созданные с помощью простого математического алгоритма[21]. Кодекс Рохонци – единственная известная нам книга, которая, по-видимому, была создана с использованием такого криптографического приема, как кодирование, а не шифрование [Király, Tokai 2018].

Таким образом, рукопись Войнича является необычным, не имеющим аналогов документом. Это одна из старейших из известных зашифрованных книг, которые еще не расшифрованы. Текст рукописи отличается от практически всех остальных сочинений, с которыми современные ученые сталкивались в работах подобного рода. Сравнение с другими зашифрованными сочинениями, однако, указывает на вероятность того, что манускрипт Войнича может относиться к числу книг, зашифрованных с помощью шифров замены и содержащих некие знания, которые автор считал нужным скрыть или являющихся мистификацией.

Заключение

Итак, в данной работе были выделены основные тенденции изучения криптографического содержания знаменитой рукописи Войнича, актуальные в последние десятилетия, к основным из которых можно отнести: использование современных средств изучения содержания и формы рукописи, таких как нейросети и методы радиоуглеродного датирования материала, а также знания

[20] *Reeds J.* John Dee and the Magic Tables in the Book of Soyga // John Dee: Interdisciplinary Studies in English Renaissance Thought, International Archives of the History of Ideas, no. 193. Dordrecht, Netherlands. New York: Springer, 2006. P. 177–204. URL: https://web.archive.org/web/20070305174955/http://www.dtc.umn.edu/~reedsj/soyga.pdf (дата обращения 11.08.2023).

[21] *Dunin E., Schmeh K.* The Voynich Manuscript Compared with Other Encrypted Books // Proceedings of the 1st International Conference on the Voynich Manuscript 2022.

о целях, особенностях и обстоятельствах создания текстов других зашифрованных сочинений, созданных примерно в это время в этом регионе.

При этом следует учитывать существующие сложности в дешифровании рукописи, среди которых можно выделить отсутствие достоверной информации о месте, обстоятельствах и цели создания рукописи, языке, на котором она была написана, ее авторе или авторах. Отдельную трудность при дешифровании могут составлять различные случайные или сознательно сделанные автором рукописи изменения в тексте, например использование сокращений, нескольких языков или диалектических форм одного языка, ошибки и т. п.

Таким образом, задача прочтения текста рукописи Войнича должна решаться с учетом междисциплинарного подхода к изучению манускрипта. Работа над текстом с использованием возможностей современных информационных технологий должна сопровождаться продолжением исторического исследования происхождения рукописи и обстоятельств ее создания, анализом лингвистических особенностей текста, палеографическим анализом манускрипта и пр. Только комплексный подход к изучению рассматриваемого документа может дать ясный ответ на вопрос о содержании одной из самых загадочных рукописей.

Литература

Быченков 2019 – *Быченков Р.О., Вахрамеева К.А., Олехнович О.Г.* Рукопись Войнича, история и попытки дешифровки текста // Актуальные вопросы современной медицинской науки и здравоохранения: Материалы IV Международной (74 Всероссийской) научно-практической конференции молодых ученых и студентов, Всероссийского форума медицинских и фармацевтических вузов, посвященных 100-летию со дня рождения ректора Свердловского государственного медицинского института, профессора В.Н. Климова, Екатеринбург, 10–12 апреля 2019 года. Т. 3. Екатеринбург: Уральский государственный медицинский университет, 2019. С. 89–94.

Манускрипт Войнича 2021 – Манускрипт Войнича / Предисл. С. Зотова. М.: АСТ, 2021. 237 с. (Страдающее Средневековье).

Русецкая 2014 – *Русецкая И.А.* История криптографии в Западной Европе в раннее Новое время. СПб.: Центр гуманитарных инициатив; Университетская книга-СПб., 2014.

Русецкая 2017 – *Русецкая И.А.* Вклад Иоанна Тритемия в развитие европейской криптографии (к 555-летию со дня рождения) // Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». 2017. № 4 (10). С. 130–140.

Русецкая 2021 – *Русецкая И.А.* Криптография: от прошлого к будущему // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 47–57.

Ernst 1998 – *Ernst T.* The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia // Cryptologia. 1998. Vol. 22 (4). P. 327.

Király, Tokai 2018 – *Király L. Z., Tokai G.* Cracking the code of the Rohonc Codex // Cryptologia. 2018. Vol. 42 (4). P. 285–315.

Prinke, Zandbergen 2017 – *Prinke R., Zandbergen R.* The unsolved enigma of the Voynich manuscript // The Voynich Manuscript. The world's most mysterious and esoteric codex. London, 2017. P. 15–40.

Rugg, Taylor 2016 – *Rugg G., Taylor G.* Hoaxing statistical features of the Voynich Manuscript // Cryptologia. 2016. Vol. 41 (3). P. 247–268.

References

Bychenkov, R.O. (2019), "Voynich's manuscript, history and attempts to decipher the text", in Bychenkov, R.O., Vakhrameeva, K.A. and Olekhnovich, O.G. (eds.), *Current issues of modern medical science and health care. Proceedings of the 4th International (74th All-Russian) Scientific and Practical Conference of Young Scientists and Students, All-Russian Forum of Medical and Pharmaceutical Universities, commemorating the 100th anniversary of the birth of V.N. Klimov, the rector of the Sverdlovsk State Medical Institute, professor*, Yekaterinburg, April 10–12, 2019, Vol. 3, Ural State Medical University, Yekaterinburg, Russia, pp. 89–94.

Rusetskaya, I.A. (2017), "The contribution of John Trithemy to the development of European cryptography (on the 555th anniversary of his birth)", *RSUH/RGGU Bulletin. "Records Management and Archival Studies. Computer Science. Data Protection and Information Security" Series*, vol. 4 (10), pp. 130–140.

Rusetskaya, I.A. (2014), History of cryptography in Western Europe in early modern times, Tsentr gumanitarnykh initsiativ; Universitetskaya kniga-SPb, St. Petersburg, Russia.

Rusetskaya, I.A. (2021), "Cryptography. From the past to the future", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 4, pp. 47–57.

Ernst, T. (1998), "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia", *Cryptologia,* vol. 22 (4), pp. 327.

Király, L.Z. and Tokai, G. (2018), "Cracking the code of the Rohonc Codex", *Cryptologia*, vol. 42 (4), pp. 285–315.

Prinke, R. and Zandbergen, R. (2017), "The unsolved enigma of the Voynich manuscript", *The Voynich Manuscript. The world's most mysterious and esoteric codex*, London, UK, pp. 15–40.

Rugg, G. and Taylor, G. (2016), "Hoaxing statistical features of the Voynich Manuscript", *Cryptologia,* vol. 41 (3), pp. 247–268.

Voynich Manuscript (2021), in Zotov, S. (foreword), AST, Moscow, Russia, 237 p. (Suffering Middle Ages).

Информация об авторе

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the author

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; irkom@mail.ru

УДК 517
DOI: 10.28995/2686-679X-2023-4-108-118

К определению некоторых понятий теории числовых последовательностей в классическом математическом анализе

Аллаберди Г. Галканов
Государственный гуманитарно-технологический университет, Орехово-Зуево, Московская область, Россия, agalkanov@yandex.ru

Аннотация. Понятие предела числовой последовательности является давно установившимся понятием в курсе математического анализа. Оно является определяемым понятием, и его определение оформилось в форме "$\varepsilon - m$" определения, или определения по Коши. В данной работе показано, что классическое определение допускает дальнейшее улучшение в смысле более логичного сведения к ранее введенным понятиям в максимально естественной форме. Определение, предлагаемое автором, названо τ-определением. Показано, что определение по Коши и τ-определение эквивалентны. Путем их сравнения выявлены определенные плюсы последнего. Рассмотрены также некоторые свойства предела и их новые доказательства. Дано новое доказательство единственности предела сходящейся числовой последовательности, и показана логическая уязвимость традиционного доказательства; дано новое доказательство ограниченности сходящейся числовой последовательности. Предложено новое определение фундаментальной последовательности и доказательство эквивалентности сходимости и фундаментальности числовой последовательности. Показано, что для знакопеременных числовых последовательностей понятие условной сходимости не имеет смысла, хотя для знакопеременных числовых рядов это понятие существует. Введены признаки сравнения для неотрицательных последовательностей сумм, предваряющие такие же признаки для неотрицательных числовых рядов.

Ключевые слова: числовая последовательность, бесконечно малая последовательность, предел, сходимость, критерий сходимости, фундаментальная последовательность

Для цитирования: Галканов А.Г. К определению некоторых понятий теории числовых последовательностей в классическом математическом анализе // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 4. С. 108–118. DOI: 10.28995/2686-679X-2023-4-108-118

On defining some concepts of the theory of number sequences in classical mathematical analysis

Allaberdi G. Galkanov
State Humanitarian-Technological University,
Orekhovo-Zuevo, Moscow Region, Russia, agalkanov@yandex.ru

Abstract. The concept of the limit of a numerical sequence is a long-established concept in the course of mathematical analysis. It is a defined concept and its definition took shape in the form of an "$\varepsilon - m$" definition or definition according to Cauchy. The article shows that the classical definition can be further improved in the sense of a more logical reduction to previously introduced concepts in the most natural form. The definition proposed by the author is called the τ-definition. It is shown that the Cauchy definition and τ-definition are equivalent. By comparing them, certain advantages of the latter were revealed. Some properties of the limit and their new proofs are also considered. The article also gives a new proof of the uniqueness of the limit as well as the boundedness of a convergent numerical sequence and shows the logical vulnerability of the traditional proof. A new definition of a fundamental sequence and a proof of the equivalence of the convergence and fundamental nature of a numerical sequence are proposed. It is shown that for sign-alternating numerical sequences the concept of conditional convergence does not make sense, although this concept exists for sign-alternating numerical sequences. Comparison criteria for non-negative sequences of sums are introduced, preceding the same criteria for non-negative numerical series.

Keywords: numerical sequence, infinitesimal sequence, limit, convergence, convergence criterion, fundamental sequence

For citation: Galkanov, A.G. (2023), "On definition of some concepts of the theory of number sequences in classical mathematical analysis", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 108–118, DOI: 10.28995/2686-679X-2023-4-108-118

Данная работа является естественным продолжением работ автора [Галканов 2011, 2019, 2020, 2022] по поиску новых форм представления установившихся понятий, формулировок теорем и новых методов доказательства в математике.

Обозначения

N – множество натуральных чисел;
$Z_0 = \{0, 1, 2, ...\}$;
R – множество действительных чисел;

БМП – бесконечно малая числовая последовательность;
Θ – множество бесконечно малых числовых последовательностей;
Ψ – множество сходящихся числовых последовательностей;
Φ – множество фундаментальных числовых последовательностей.

Определения

Пусть $\{c_n\}$ – некоторая числовая последовательность (в дальнейшем просто последовательность), $\{0\}$ – стационарная нуль-последовательность. Рассмотрим модуль отклонения $|c_n - 0| = |c_n|$ n-го члена $\{c_n\}$ от n-го члена $\{0\}$ и неравенство $|c_n| < \tau$ ($\tau > 0$). Пусть $H_\tau = \{n : |c_n| < \tau, n \in \mathbf{N}\}$ – множество решений неравенства $|c_n| < \tau$ относительно n на множестве натуральных чисел $\mathbf{N}$, где индекс τ в обозначении H_ε означает зависимость H от τ. Очевидно, что $[H_\tau = K] \vee [H_\tau = N_m]$, где K – пустое или конечное множество, $N_m = \{m + 1, m + 2, ...\}$ – множество всех натуральных чисел, последующих за числом $m \in Z_0 = \{0, 1, 2, ...\}$. В частности, $N_m = \mathbf{N}$, если $m = 0$. Если же $m > 0$, то $N_m \subset \mathbf{N}$.

Определение 1. Если для каждого $\tau > 0$ существует число $m \in Z_0$, такое, что $H_\tau = N_m$, то $\{c_n\}$ называется бесконечно малой последовательностью (БМП).

Если множество БМП обозначить заглавной греческой буквой Θ, то определение 1 и его отрицание запишутся в виде

$$\{c_n\} \in \Theta \overset{def}{\Leftrightarrow} \forall \varepsilon > 0 \; \exists m \in Z_0 \left[\{n : |c_n| < \varepsilon, n \in \mathbf{N}\} = N_m \right],$$

$$\left[\{c_n\} \notin \Theta \right] \overset{def}{\Leftrightarrow} \left[\exists \varepsilon > 0 \; \forall m \in Z_0 \left[\{n : |c_n| < \varepsilon, n \in \mathbf{N}\} = K \right] \right].$$

Следствие из определения 1. БМП есть ограниченная последовательность.

Определение 2. Если существует стационарная последовательность $\{c\}$ такая, что $\{c_n - c\}$ есть БМП, то $\{c_n\}$ называется последовательностью, сходящейся к последовательности $\{c\}$, иначе – расходящейся последовательностью.

При этом $\{c\}$ называется предельной последовательностью для $\{c_n\}$ или пределом $\{c_n\}$. Тот факт, что $\{c_n\}$ есть сходящаяся к $\{c\}$ последовательность, в дальнейшем будет обозначаться $\lim\limits_{n\to\infty}\{c_n\} = \{c\}$, или $\lim\{c_n\} = \{c\}$. Это обозначение представляется нам более логич-

ным против существующего $\lim\limits_{n\to\infty} c_n = c$, так как пределом последовательности может быть только стационарная последовательность, а не число.

Итак, по определению

$$\left[\lim\{c_n\}=\{c\}\right] \overset{def}{\Leftrightarrow} \left[\exists\{c\}\left[\{c_n-c\}\in\Theta\right]\right]. \quad (1)$$

С учетом определений разности двух последовательностей и БМП определение (1) можно записать в двух равносильных формах:

$$\lim\{c_n\}=\{c\} \overset{def}{\Leftrightarrow} \exists c\in\mathbf{R}\ \exists\{\alpha_n\}\in\Theta\ \forall n\in\mathbf{N}\left[c_n=c+\alpha_n\right], \quad (2)$$

$$\lim\{c_n\}=\{c\} \overset{def}{\Leftrightarrow} \exists c\in\mathbf{R}\ \forall\tau>0\ \exists m\in\mathrm{Z}_0\left[\{n:|c_n-c|<\tau, n\in\mathbf{N}\}=\mathrm{N}_m\right]. \quad (3)$$

Если буквой Ψ обозначить множество сходящихся последовательностей, то путем отрицания из (1), (2) и (3) получим определение расходящейся последовательности в трех равносильных формах:

$$\{c_n\}\notin\Psi \overset{def}{\Leftrightarrow} \forall\{c\}\left[\{c_n-c\}\notin\Theta\right],$$

$$\{c_n\}\notin\Psi \overset{def}{\Leftrightarrow} \forall c\in\mathbf{R}\ \forall\{\alpha_n\}\in\Theta\ \exists n\in\mathbf{N}\left[c_n\neq c+\alpha_n\right],$$

$$\{c_n\}\notin\Psi \overset{def}{\Leftrightarrow} \forall c\in\mathbf{R}\ \exists\tau>0\ \forall m\in Z_0\left[\{n:|c_n-c|<\tau, n\in\mathbf{N}\}=\mathrm{K}\right]. \quad (4)$$

Определение (3) предела последовательности назовем τ-определением в отличие от классического определения предела последовательности по Коши, называемое также "$\varepsilon - m$"-определением.

Сравнение τ-определения предела последовательности с определением по Коши

Приведем определение сходимости по Коши [Зорич В.А. 2019]:

$$\lim\{c_n\}=\{c\} \overset{def}{\Leftrightarrow} \forall\varepsilon>0\ \exists m\in\mathbf{N}\ \forall n>m\left[|c_n-c|<\varepsilon\right], \quad (5)$$

а затем его отрицаем:

$$\lim\{c_n\}\neq\{c\} \overset{def}{\Leftrightarrow} \exists\varepsilon>0\ \forall m\in\mathbf{N}\ \exists n>m\left[|c_n-c|\geq\varepsilon\right]. \quad (6)$$

1. В (3) в правую часть знака эквивалентности включен предел c под знаком квантора существования, благодаря чему после отрицания (3) получается определение расходимости (4), включающее в себя предел c под знаком квантора общности, что может оказаться весьма кстати при доказательстве расходимости по определению. Однако в (5) в правой части знака эквивалентности предел c отсутствует, соответственно в (6) в правой части знака эквивалентности предел c также отсутствует. Поэтому на первый взгляд кажется, что в (5) и (6) буква c одна и та же, но на самом деле в этих определениях буква c имеет диаметрально противоположный смысл. Так что с логической точки зрения определение (3) оказалось более точным и полным, нежели определение (5).

2. В (3) запись $n : |c_n - c| < \tau$, $n \in \mathbf{N}$ явно указывает на то, что неравенство $|c_n - c| < \tau$ решается на множестве натуральных чисел. В то время как (5) не содержит такой информации.

3. В (5) параметр m принимает натуральные значения. В (3) же – неотрицательные целые значения, что может оказаться более адекватным решаемой задаче (задача 1).

4. Геометрическая интерпретация τ-определения на плоскости Oxy позволяет лучше понять смысл предела последовательности.

5. Иногда τ-определение может быть использовано как метод вычисления пределов по определению (задача 2).

За исключением описанных выше замечаний, определения (3) и (5) эквивалентны, т. е. из сходимости $\{c_n\}$ по τ-определению следует сходимость $\{c_n\}$ по "$\varepsilon - m$"-определению, и наоборот.

С учетом перечисленных выше аргументов и дальнейших применений τ-определение может рассматриваться как альтернативное определение предела последовательности.

Отметим некоторые следствия, вытекающие из определений.

Следствие 1 (инвариантность сходимости $\{c_n\}$ относительно обозначения индекса n). Если $\lim\{c_n\} = \{c\}$, то для любых натуральных индексов $i, j, \ldots k$ справедливы равносильности $[\lim\{c_j\} = \{c\}] \Leftrightarrow [\lim\{c_j\} = \{c\}] \Leftrightarrow \ldots \Leftrightarrow [\lim\{c_j\} = \{c\}]$.

Следствие 2 (инвариантность расходимости $\{c_n\}$ относительно обозначения индекса n). Если $\{c_n\} \notin \Psi$, то для любых натуральных индексов $i, j, \ldots, k$ справедливы равносильности $[\{c_n\} \notin \Psi] \Leftrightarrow [\{c_j\} \notin \Psi] \Leftrightarrow \ldots \Leftrightarrow [\{c_k\} \notin \Psi]$.

Задача 1. По определению (3) доказать, что $\lim\left\{\dfrac{3n-2}{n+3}\right\} = \{3\}$.

Решение. Составим и решим неравенство $\{n: |c_n - c| < \tau, n \in \mathbf{N}\}$.

$$\left[\left|\frac{3n-2}{n+3}-3\right|<\tau\right]\Leftrightarrow\left[\frac{-11}{n+3}<\tau\right]\Leftrightarrow\left[n>-3-\frac{11}{\tau}\right]\Rightarrow\left[m=E\left[-3-\frac{11}{\tau}\right]\right].$$

Очевидно, что за m следует взять число $0 \in Z_0$, так что $\{n: |c_n - c| < \tau, n \in \mathbf{N}\} = \mathbf{N}$. Согласно же (5), за m можно взять какое-либо число $m = \tilde{m} \in \mathbf{N}$, и неравенство в определении (5) $\forall n > m[|c_n - c| < \varepsilon]$ будет верно, но при этом останется неоднозначность с выбором m.

Задача 2. $\{c_n\}: c_n = \dfrac{a_0 + a_1 n + a_2 n^2 + ... + a_m n^m}{b_0 + b_1 n + b_2 n^2 + ... + b_m n^m}$, где $m \in$, $b_m \neq 0$.

По определению 2 доказать, что $\lim\{c_n\} = \left\{\dfrac{a_m}{b_m}\right\}$.

Решение. Составим разность $c_n - c$ и преобразуем ее, где c пока неизвестно.

$$\frac{a_0+...+a_{m-1}n^{m-1}+a_m n^m}{b_0+...+b_{m-1}n^{m-1}+b_m n^m}-c=\frac{(a_0-cb_0)n^{-m}+...+(a_{m-1}-cb_{m-1})n^{-1}+(a_m-cb_m)}{b_0 n^{-m}+...+b_{m-1}n^{-1}+b_m}=$$

$$=\frac{a_m-cb_m}{b_0 n^{-m}+...+b_{m-1}n^{-1}+b_m}+\frac{(a_0-cb_0)n^{-m}+...+(a_{m-1}-cb_{m-1})n^{-1}}{b_0 n^{-m}+...+b_{m-1}n^{-1}+b_m}.$$

Так как $\dfrac{(a_0-cb_0)n^{-m}+...+(a_{m-1}-cb_{m-1})n^{-1}}{b_0 n^{-m}+...+b_{m-1}n^{-1}+b_m} \in \Theta$, то стационарная последовательность $\{c\}$ будет предельной для данной, если $a_m - cb_m = 0$, т. е. $\left\{c_n - \dfrac{a_m}{b_m}\right\} \in \Theta$.

Теорема 1. Если последовательность $\{c_n\}$ сходится, то она имеет только один предел: $[\{c_n\} \in \Psi] \Rightarrow [\exists! c \in \mathbf{R}[\lim c_n = c]]$.

Одно из традиционных доказательств данной теоремы состоит из следующих шагов [Архипов 2004][1].

1. Предполагается существование двух пределов c_1 и c_2 $(c_1 \neq c_2)$.
2. Показывается, что $c_1 = c_2$.
3. Утверждается, что теорема 1 доказана, так как $c_1 = c_2$ противоречит предположению $c_1 \neq c_2$.

Новое доказательство. Допустим, что $\{c_n\}$ имеет, по крайней мере, два предела $\{c_1\}$ и $\{c_2\}$ $(c_1 \neq c_2)$. Пусть $\{c\} = \{c_1 - c_2\}$. Тогда, согласно (2), $\forall n \in \mathbf{N}\left[[c_n = c_1 + \alpha_n] \wedge [c_n = c_2 + \beta_n]\right]$ и $\left[\{\alpha_n\} - \{\beta_n\} = \{c\} \notin \Theta\right] \Rightarrow \left[\{\alpha_n - \beta_n\} \notin \Theta\right]$. Но это противоречит свойству бесконечно малых. Теорема 1 доказана.

[1] *Лисин Б.В.* Пределы. Непрерывность функции (Электронное методическое пособие). Нижний Новгород, 2010.

Сравнение традиционного и нового доказательств. Традиционный способ доказательства единственности теорем вида $U \Rightarrow V$ основан на формальной эквивалентности $[U \Rightarrow V] \Leftrightarrow \big[[U \wedge \neg V] \Rightarrow V\big]$, где U, V – высказывания. Предполагается, что V : *false*. Из истинности условия и ложности предположения V выводится V : *true*. После утверждается, что полученное противоречие завершает доказательство теоремы $U \Rightarrow V$. Возникает вопрос: можно ли назвать доказательством то, что приводит к высказыванию, противоречащему нашему же предположению? Однако, во-первых, наше предположение всего лишь предположение, истинность или ложность которого пока неизвестны. Во-вторых, импликация $U \Rightarrow V$ не эквивалентна теореме, а является всего лишь ее моделью. И, в-третьих, если V содержит квантор общности $\forall$, например по переменной χ, то в конъюнкции $U \wedge \neg V$ этот квантор перейдет в квантор существования $\exists$. В результате вместо того, чтобы показать истинность для всех допустимых x, в лучшем случае получим истинность для некоторых допустимых x. Что касается нового доказательства, то оно завершилось только после получения противоречия относительно ранее установленного факта: разность двух БМП есть БМП. Поэтому новое доказательство можно считать логически безупречным.

Теорема 2. Если последовательность $\{c_n\}$ сходится, то она ограниченна.

Новое доказательство. Допустим, что $\{c_n\}$ не ограниченна: $\forall \mu > 0 \;\; \exists l \in \quad \big[|c_l| > \mu\big]$. По условию и по допущению имеем

$$\begin{cases} \forall n \in \mathbf{N}\big[c_n = c + \alpha_n\big], \\ \forall \mu > 0 \; \exists l \in \square \; \big[|c_l| > \mu\big] \end{cases} \overset{n=l}{\Rightarrow} \begin{cases} c_l = c + \alpha_l, \\ \forall \mu > 0 \; \exists l \in \square \; \big[|c_l| > \mu\big] \end{cases} \Rightarrow \forall \mu > 0 \; \exists l \in \square \; \big[|c + \alpha_l| > \mu\big],$$

из чего следует, что $\{\alpha_n\}$ – неограниченная последовательность, что противоречит следствию из определения 1. Теорема 2 доказана.

Теорема 3 (критерий бесконечной малости).

$\big[\{c_n\} \in \Theta\big] \Leftrightarrow \big[\lim\{c_n\} = \{0\}\big]$.

Необходимость. По аксиоматике вещественных чисел $\exists !0 \in \mathbf{R}$. Согласно τ-определению,

$$\forall \tau > 0 \; \exists m \in Z_0 \; \big[\{n : |c_n| < \tau, \, n \in \mathbf{N}\} = \mathrm{N}_m\big] \Leftrightarrow$$

$$\Leftrightarrow \big[\exists !0 \in \mathbf{R} \; \forall \tau > 0 \; \exists m \in Z_0[\{n : |c_n - 0| < \tau, \; n \in \mathbf{N}\} = \mathrm{N}_m]\big] \overset{(3)}{\Leftrightarrow} \big[\lim\{c_n\} = \{0\}\big].$$

Достаточность. Принимая во внимание (3), имеем

$\big[\exists !0 \in \mathbf{R} \; \forall \tau > 0 \; \exists m \in Z_0[\{n : |c_n - 0| < \tau, \, n \in \mathbf{N}\} = \mathrm{N}_m]\big] \Leftrightarrow$

$\Leftrightarrow \big[\forall \tau > 0 \; \exists m \in Z_0[\{n : |c_n| < \tau, \, n \in \mathbf{N}\} = \mathrm{N}_m]\big] \Leftrightarrow [\{c_n\} \in \Theta]$.

Теорема 3 доказана.

Следствие. Нуль – последовательность $\{0\}$ является предельной как для самой себя, так и для всех бесконечно малых последовательностей.

Понятие фундаментальной последовательности

Рассмотрим частный случай линейной однородной последовательности $\{ac_n + bc_m\}$, составленной из одной и той же последовательности $\{c_k\}$, где $a, b \in \mathbf{R}$ $(ab \neq 0)$, n и m – натуральные индексы, пробегающие множество $\mathbf{N}$ независимо друг от друга. Последовательность $\{ac_n + bc_m\}$ представляет особый случай при $a = 1$ и $b = -1$. А именно в этом случае можно дать новое определение фундаментальной последовательности и новое доказательство критерия сходимости.

Определение 3. Если линейная однородная последовательность $\{c_m - c_n\}$ является бесконечно малой, то $\{c_k\}$ называется фундаментальной, иначе – нефундаментальной последовательностью.

Множество фундаментальных последовательностей обозначим заглавной греческой буквой Φ.

Теорема 4 (критерий сходимости). Для сходимости последовательности $\{c_k\}$ необходимо и достаточно фундаментальность $\{c_k\}$: $[\{c_k\} \in \Psi] \Rightarrow [\{c_k\} \in \Phi]$.

Необходимость. $[\{c_k\} \in \Psi] \Rightarrow [\{c_k\} \in \Phi]$. Пусть $\lim\{c_k\} = \{c\}$. Тогда по свойству сходящихся последовательностей $\lim\{c_m\} = \{c\}$ и $\lim\{c_n\} = \{c\}$. Имеем $\lim\{c_m - c_n\} = \lim\{c_m\} - \lim\{c_n\} = \{c\} - \{c\} = \{0\}$, из чего по теореме 3 следует, что $\{c_m - c_n\} \in \Theta$. Тогда по определению 3 $\{c_k\} \in \Phi$.

Достаточность. $[\{c_k\} \in \Phi] \Rightarrow [\{c_k\} \in \Psi]$. По условию $\{c_k\} \in \Phi$, что означает $\{c_m - c_n\} \in \Theta$. Предварительно покажем, что если последовательности $\{c_m\}$ и $\{c_n\}$ не имеют общего предела, то их разность не может быть БМП. В самом деле, пусть $\lim\{c_m\} = \{c_1\}$, $\lim\{c_n\} = \{c_2\}$, где $c_1 \neq c_2$. И пусть $c = c_1 - c_2 \neq 0$. Имеем $\{c_m - c_n\} = \{c\} + \{\alpha_m - \beta_n\} \notin \Theta$. Так что $\{c_m - c_n\} \notin \Theta$. Теперь допустим, что $\{c_k\} \notin \Psi$. Тогда по свойству расходящейся последовательности $[\{c_m\} \notin \Psi]$, $[\{c_n\} \notin \Psi]$, а для расходящихся последовательностей $\{c_m\}$ и $\{c_n\}$ их общий предел не существует. И, согласно только что доказанному, $\{c_m - c_n\} \notin \Theta$ и по определению 3 $\{c_k\} \notin \Phi$, что противоречит условию. Теорема 4 доказана.

Следствие (критерий расходимости). Нефундаментальность $\{c_k\}$ есть необходимое и достаточное условие для расходимости последовательности $\{c_k\}$.

◄ К теореме 4 применить закон противоположности. ►

Следствие из необходимости. $[\{c_k\} \in \Theta] \Rightarrow [\{c_k\} \in \Phi]$.

Рассмотрим знакопеременную последовательность $\{c_n\}$ и $\{|c_n|\}$.

Определение 4. Последовательность $\{c_n\}$ называется абсолютно сходящейся, если сходится последовательность $\{|c_n|\}$.

Теорема 5. $[\{c_n\} \in \Psi] \Rightarrow [\{|c_n|\} \in \Psi]$.

Доказательство. По условию $\{c_n\} \in \Psi$.

Случай 1. $\forall n \in \mathbf{N}[c_n \geqslant 0]$. Тогда $\forall n \in \mathbf{N}[|c_n| = c_n]$ и $\{|c_n|\} \in \Psi$.

Случай 2. $\forall n \in \mathbf{N}[c_n < 0]$. Тогда $\forall n \in \mathbf{N}[|c_n| = -c_n = (-1) \cdot c_n]$ и $\{|c_n|\} \in \Psi$.

Случай 3. Пусть $\{c_n\}$ – знакопеременная последовательность. Тогда $\forall n \in \mathbf{N}\ [|c_n| \geqslant 0]$. Так как $\{c_n\} \in \Psi$, то по теореме 2 $\exists \mu > 0$ $\forall n \in \mathbf{N}\ [|c_n| \leqslant \mu]$. Следовательно, $\{|c_n|\} \in \Psi$ как неубывающая и ограниченная сверху числом μ последовательность. Теорема 5 доказана.

Следствие. $[\{|c_n|\} \notin \Psi] \Rightarrow [\{c_n\} \notin \Psi]$.

Доказательство. К теореме 5 применить закон контрапозиции.

Теорема 5 необратима, что видно из примера $\{c_n\} : c_n = (-1)^{n+1}$.

Согласно следствию из теоремы 5, для знакопеременных последовательностей понятие условной сходимости не имеет смысла, в то время как для знакопеременных числовых рядов это понятие существует.

Таким образом, сравнивая знакопеременные последовательности со знакопеременными числовыми рядами, можно сделать следующий антисимметричный вывод:

1) всякая сходящаяся последовательность сходится абсолютно, но не всякая абсолютно сходящаяся последовательность сходится;
2) всякий абсолютно сходящийся числовой ряд сходится, но не всякий сходящийся числовой ряд сходится абсолютно.

Рассмотрим последовательности $\{u_n\}$, $\{v_n\}$, $\{w_n\} : \forall n \in \mathbf{N}\ [u_n \geqslant 0, v_n \geqslant 0, w_n \geqslant 0]$.

Введем последовательности сумм

$$\{U_n\} : U_n = \sum_{k=1}^{n} u_k,\ \{V_n\} : V_n = \sum_{k=1}^{n} v_k,\ \{W_n\} : W_n = \sum_{k=1}^{n} w_k.$$

Теорема 6 (признаки сравнения для неотрицательных последовательностей сумм). Если $\forall n \in \mathbf{N}\ [u_n \leqslant v_n \leqslant w_n]$, то

1) из сходимости последовательности $\{V_n\}$ следует сходимость $\{U_n\}$;
2) из расходимости последовательности $\{V_n\}$ следует расходимость $\{W_n\}$.

Доказательство. Из 1) следует ограниченность последовательности $\{V_n\}$. Так как $\{u_n\}$ – неотрицательная последовательность, то $\{U_n\}$ не убывает, а в силу условия $\forall n \in \mathbf{N}\,[u_n \leqslant v_n]$ и $\forall n \in \mathbf{N}\,[U_n \leqslant V_n]$, $\{U_n\}$ ограниченна. Так что последовательность $\{U_n\}$ не убывает и ограниченна сверху. Поэтому она сходится. Допустим, что $\{W_n\}$ сходится. Тогда, согласно условию $\forall n \in \mathbf{N}\,[v_n \leqslant w_n]$ и только что доказанному, последовательность $\{V_n\}$ должна сходиться. Однако это противоречит условию. Теорема 6 доказана.

В заключение перечислим основные результаты работы.

1. Дано новое определение бесконечно малой последовательности.

2. Дано новое определение предела числовой последовательности, названное τ-определением.

3. Дано новое доказательство единственности предела сходящейся числовой последовательности и показана логическая уязвимость одного из традиционных доказательств единственности предела.

4. Дано новое определение фундаментальной последовательности и предложено альтернативное доказательство эквивалентности сходимости и фундаментальности числовой последовательности.

Представленные в статье результаты используются автором на лекционных и практических занятиях по математическому анализу на физико-математическом факультете Государственного гуманитарно-технологического университета.

Литература

Архипов 2004 – Лекции по математическому анализу: Учеб. для вузов / Архипов Г.И., Садовничий В.А., Чубариков В.Н.; под ред. В.А. Садовничего. М.: Дрофа, 2004.

Галканов 2011 – *Галканов А.Г.* Метод от противоположного и его применения к доказательству теорем: Монография. М.: МГУЛ, 2011.

Галканов 2019 – *Галканов А.Г.* Инновационные методы в преподавании математики в вузе: о базисных понятиях дифференциальных уравнений первого порядка // Вестник Государственного гуманитарно-технологического университета. 2019. № 3. С. 5–14.

Галканов 2020 – *Галканов А.Г.* Инновационные методы в преподавании математики в вузе: о методе от противоположного (МОП) // Вестник Государственного гуманитарно-технологического университета. 2020. № 1. С. 11–17.

Галканов 2022 – *Галканов А.Г.* О некоторых понятиях и теоремах математического анализа // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 2. С. 48–58. DOI: 10.28995/2686-679X-2022-2-48-58.

Зорич 2019 – *Зорич В.А.* Математический анализ. Часть 1. 10-е изд., испр. М.: МЦНМО, 2019.

References

Arkhipov, G.I., Sadovnichiy, V.A. and Chubarikov, V.N. (2004), *Lektsii po matematicheskomu analizu: Uchebnik dlya vuzov* [Lectures on mathematical analysis. Textbook for universities], in Sadovnichiy, V.A (ed.), Drofa, Moscow, Russia.

Galkanov, A.G. (2011), *Metod ot protivopolozhnogo i yego primeneniya k Dokazatel'stvu teorem: Monografiya* [Method from the opposite and its application to the proof of theorems. Monograph], MGUL, Moscow, Russia.

Galkanov, A.G. (2019), "Innovative Methods in Teaching Mathematics at Higher Educational Institutions. On the Basic Concepts of First-Order Differential Equations", *Bulletin of the State Humanitarian and Technological University*, vol. 3. pp. 5–14.

Galkanov, A.G. (2020), "Innovative methods in teaching mathematics in higher educational institution. About the method from the opposite (MFO)", *Bulletin of the State Humanitarian and Technological University*, vol. 1. pp. 11–17.

Galkanov, A.G. (2022), "About some concepts and theorems in mathematical analysis", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 48–58, DOI: 10.28995/2686- 679X-2022-2-48-58.

Zorich, V.A. (2019), *Matematicheckiy analiz. Chast'* 1 [Mathematical analysis. Part 1], MCCME, Moscow, Russia

Информация об авторе

Аллаберди Г. Галканов, кандидат технических наук, доцент, Государственный гуманитарно-технологический университет, Орехово-Зуево, Московская обл., Россия; 142600, Россия, Московская обл., Орехово-Зуево, ул. Зеленая, д. 22; agalkanov@yandex.ru

Information about the author

Allaberdi G. Galkanov, Cand. of Sci. (Technical Engineering), associate professor, State Humanitarian-Technological University, Orekhovo-Zuevo, Moscow Region, Russia; bld. 22, Zelenaya Str., Moscow Region, Orekhovo-Zuevo, Russia, 142600; agalkanov@yandex.ru

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 4
2023

Дизайн обложки
Е.В. Амосова

Корректор
Н.В. Москвина

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, Москва, Миусская пл., 6

Свидетельство о регистрации СМИ
ПИ № ФС77-72977 от 25.05.2018 г.
Периодичность 4 раза в год

Подписано в печать 19.12.2023
Выход в свет 26.12.2023
Формат 60×90 1/16.
Уч.-изд. л. 7,0. Усл. печ. л. 7,5
Тираж 1050 экз. Свободная цена
Заказ № 1869

Отпечатано в типографии Издательского центра
Российского государственного гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru