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

3
2025

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 (physical and mathematical sciences)

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

2.3.8. Informatics and information processes (technical science)

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: 6-6, 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 (физико-математические науки)

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

2.3.8. Информатика и информационные процессы (технические науки)

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., д. 6, стр. 6

Электронный адрес: grnat@rambler.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

Н.В. Гришина, кандидат технических наук, доцент,
Российский государственный гуманитарный университет (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 519.689
DOI: 10.28995/ 2686-679X-2025-3-8-20

Перспективы применения моделей, основанных на архитектуре трансформеров, в задачах обработки естественного языка

Андрей П. Титов
МИРЭА – Российский технологический университет, Москва, Россия, titov_and@mail.ru

Наталия В. Гришина
Российский государственный гуманитарный университет, Москва, Россия;
Московский государственный лингвистический университет, Москва, Россия, grnat@rambler.ru

Дарья Н. Титова
Образовательный центр «Протон», Москва, Россия, decestoeva@gmail.com

Аннотация. В статье рассматриваются архитектуры, принципы работы и особенности моделей T5 (Text-to-Text Transfer Transformer) и BART (Bidirectional and Auto-Regressive Transformers). Разобрано применение этих моделей в различных задачах по обработке естественного языка (NLP-задачах). Модели на основе трансформеров T5 и BART за последнее время сильно эволюционировали в области NLP. Модели представляют собой инструменты для решения широкого списка задач, в том числе: перевод, суммирование и классификацию.

Модель T5 преобразует все задачи NLP в формат «входной текст – выходной текст» и является наиболее универсальной. Значительное упрощение процесса обучения и адаптации модели возможно за счет использования одной и той же архитектуры для различных задач. Она обучается на большом наборе данных, что позволяет обрабатывать текстовые данные.

Модель BART имеет в своем составе авторегрессивные элементы и элементы двунаправленных моделей. Она обучается на задаче восстановления текста. Это позволяет ей эффективно справляться с задачами, связанными с генерацией и преобразованием текста. BART успешно

справляется с задачами выборки и перевода благодаря своей способности учитывать контекст и структуру текста.

В статье рассматриваются преимущества и недостатки обеих моделей, изучено их влияние на развитие NLP. Рассмотрены перспективы дальнейших исследований. Универсальность и эффективность делают их важными инструментами для исследователей и практиков, работающих в этой быстро развивающейся области.

Статья исследует основные принципы работы этих моделей и применение в различных задачах. На конкретных примерах демонстрируется, как T5 и BART преодолевают ограничения предыдущих подходов, характерные для традиционных рекуррентных нейронных сетей и других методов обработки текста. Исследование несет в себе углубленный анализ масштабируемости трансформеров, а также показывает их вклад в развитие современных систем искусственного интеллекта. Авторы подчеркивают, что дальнейшее развитие трансформеров расширит возможности машинного обучения и обработки естественного языка.

Ключевые слова: модель T5, модель BART, задачи по обработке естественного языка, рекуррентные нейронные сети

Для цитирования: Титов А.П., Гришина Н.В., Титова Д.Н. Перспективы применения моделей, основанных на архитектуре трансформеров, в задачах обработки естественного языка // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 8–20. DOI: 10.28995/ 2686-679X-2025-3-8-20

The prospects of using transformer-based models in natural language processing tasks

Andrei P. Titov
MIREA – Russian Technological University, Moscow, Russia, titov_and@mail.ru

Nataliya V. Grishina
Russian State University for the Humanities, Moscow, Russia; Moscow State Linguistic University, Moscow, Russia, grnat@rambler.ru

Dar'ya N. Titova
Proton Educational Center, Moscow, Russia, decestoeva@gmail.com

Abstract. The article considers the architecture, operating principles and key features of T5 and BART, as well as their use in various NLP tasks. In recent years, models based on the T5 (Text-to-Text Transfer Transformer) and

BART (Bidirectional and Auto-Regressive Transformers) transformers have evolved significantly in the field of natural language processing (NLP). Models are powerful tools for solving a wide range of tasks, including text generation, translation, summation, and classification.

The T5 model is a universal one that converts all NLP tasks into the input text-output text format. That allows using the same architecture for different tasks, which greatly simplifies the process of learning and adapting the model. It is trained on a large dataset, which allows processing text data.

The BART model combines elements of both auto – regressive and bidirectional models. It is trained on the task of text recovery. That allows it to effectively handle tasks related to text generation and conversion. BART demonstrates outstanding results in sampling and translating tasks due to its ability to take into account the context and structure of the text.

The article goes into the advantages and disadvantages of both models and their impact on NLP development. It also considers prospects for further research. Their versatility and effectiveness make them important tools for researchers and practitioners working in that rapidly evolving field.

The article studies the basic principles of operation of these models and their use in various tasks. Concrete examples demonstrate how T5 and BART overcome the limitations of previous approaches typical of traditional recurrent neural networks and other text processing methods. The study provides an in-depth analysis of the effectiveness and scalability of transformers, and also shows their contribution to the development of modern artificial intelligence systems. The authors emphasize that further improvements in the field of transformers can significantly expand the horizons of machine learning and natural language processing.

Keywords: T5 model, BART model, natural language processing tasks, recurrent neural networks

For citation: Titov A.P., Grishina N.V. and Titova, D.N. (2025), “The prospects of using transformer-based models in natural language processing tasks”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series*, no. 3, pp. 8–20, DOI: 10.28995/ 2686-679X-2025-3-8-20

По мере развития средств искусственного интеллекта (ИИ) модели-трансформеры стали эффективным инструментом для автоматизации процесса обработки текста. Модели на основе трансформеров, такие как T5 и BART, оказывают значительное влияние на развитие обработки естественного языка. Модели показывают высокие результаты в задачах генерации, перевода и суммирования текста. Универсальность и адаптивность T5 и BART позволяют решать широкий спектр задач с использованием одной архитектуры,

что делает их особенно ценными для исследователей и практиков. Понимание их принципов работы и применения является ключевым для дальнейших инноваций в области NLP.

Статья направлена на исследование и анализ перспектив применения моделей, основанных на архитектуре трансформеров, в задачах обработки естественного языка. Рассмотрены основные достижения и преимущества трансформеров, таких как их способность к контекстному пониманию и генерации текста. Это делает их эффективными для различных приложений – от машинного перевода до создания диалоговых систем. В статье рассматриваются ограничения, с которыми сталкиваются исследователи. Обсуждаются пути развития трансформеров, включая их адаптацию к новым задачам, направленным на улучшение производительности в реальных условиях.

Модель T5 благодаря своей универсальной архитектуре позволяет решать широкий спектр задач. Это особенно полезно для исследователей и разработчиков, стремящихся к созданию многофункциональных приложений в области NLP. Модель BART сочетает в себе преимущества двунаправленного и авторегрессивного обучения. Это позволяет ему эффективно справляться с задачами, связанными с восстановлением и преобразованием текста, такими как суммирование и перевод [Билал 2024].

Необходимость в таких моделях также обусловлена их способностью адаптироваться к различным контекстам и задачам, что делает их идеальными для применения в реальных сценариях, таких как чат-боты, системы рекомендаций и автоматизированные инструменты для анализа данных. Модели T5 и BART являются ключевыми инструментами для достижения высоких результатов в области обработки естественного языка, что подчеркивает их актуальность и необходимость в современных исследованиях [Гаврилова 2024].

Модель T5 (Text-to-Text Transfer Transformer) – это один из методов обработки естественного языка, разработанный Google Research. Основная идея T5 состоит в том, что она рассматривает все задачи, связанные с текстом, как задачи преобразования текста в текст. Это подход, который позволяет использовать одну архитектуру для решения самых разных задач – от перевода и суммирования до классификации и генерации текста.

В T5 используется архитектура трансформера, которая основана на механизме, позволяющем модели фокусироваться на разных частях входного текста без ограничения на последовательность, что делает ее особенно эффективной для обработки длинных текстов.

Каждая задача формулируется в формате «входной текст → выходной текст». Любой текст, который подается на вход модели, предварительно обрабатывается, чтобы соответствовать требованиям конкретной задачи. Например, для задачи перевода текст может выглядеть так: «перевести на французский: Hello, how are you?», и модель будет генерировать: “Bonjour, comment ça va?”. Технология T5 включает в себя несколько ключевых этапов, таких как подготовку данных, обучение и предсказание.

Подготовка данных – на этом этапе модель получает большой объем текстов, которые подвергаются предварительной обработке. Все входные данные преобразуются в текстовые пары: входной текст и соответствующий выходной текст. Это означает, что для каждой задачи формируется набор пар (вход, выход), который закодируется в числовые представления с использованием процесса разделения текста на токены, которые могут быть словами, частями слов или символами, что позволяет модели обрабатывать текст в числовом формате (токенизации) [Fishcheva 2022].

Обучение модели T5 происходит в два этапа. Сначала проходит предобучение на большом наборе текстовых данных, где задача состоит в том, чтобы угадать пропущенные слова (masked language modeling) или завершить текст (text completion). Для этого модель использует специальные маскированные токены, которые указывают на пропуски в тексте. Затем модель дообучается на конкретных задачах с использованием ранее подготовленных пар (вход, выход) для вывода результата. Такой двухступенчатый подход позволяет модели эффективно адаптироваться к различным типам задач, что делает ее универсальной.

Механизм внимания, лежащий в основе трансформеров, включает в себя три основных компонента: запросы (query), ключи (key) и значения (value). Модель вычисляет взвешенные суммы значений на основе соответствия между запросами и ключами. Это позволяет ей динамически фокусироваться на самых релевантных частях входного текста. Модель имеет возможность справляться со сложной структурой и контекстом предложения, учитывая взаимосвязи между словами независимо от их положения.

После завершения процесса обучения модель готова к предсказанию. На этом этапе ей передается новая задача, которая снова превращается в текст в формате «вход → выход». Модель оценивает этот текст, использует механизмы внимания для выявления значимой информации и производит предсказания, которые затем декодируются обратно в текст [Лезгян 2023].

Важно отметить, что T5 использует подход декодирования поиском и выборки, чтобы сформировать окончательный текст.

Это значит, что на каждом шаге предсказания она может выбирать наиболее вероятный следующий токен на основании предшествующих, что позволяет генерировать связные и логичные ответы.

Модель T5 была спроектирована с использованием масштабируемой архитектуры, что позволяет ей применяться в различных контекстах, от мобильных приложений до больших облачных вычислений. Возможности T5, заключающиеся в том, что она может успешно справляться с разнообразными задачами обработки естественного языка, объясняют ее популярность и широкое использование в последние годы [Васильев 2023].

Рассмотрим концепцию математических элементов, лежащих в основе модели A5 с архитектурой трансформеров. Слова и токены представляются в виде векторов в высокоразмерном пространстве, что позволяет модели захватывать семантические отношения между ними. Основным компонентом трансформеров является механизм внимания, который позволяет модели фокусироваться на различных частях входной последовательности. Он вычисляется следующим образом [Йылдырым 2022]:

$$Attention\ (Q,\ K,\ V) = \text{softmax}\left(\frac{QK^{\top}}{\sqrt{d}}\right)V,$$

где Q – матрица запросов, K – матрица ключей, V – матрица значений, а d – размерность ключей.

Трансформеры не имеют встроенной информации о порядке токенов, поэтому используется позиционное кодирование, чтобы добавить информацию о позиции токенов в последовательности. Обычно это делается с помощью тригонометрических функций [Йылдырым 2022]:

$$PE_{(pos,2i)} = \sin\left(\frac{pos}{10000^{2i/d_{model}}}\right)$$

$$PE_{(pos,2i+1)} = \cos\left(\frac{pos}{10000^{2i/d_{model}}}\right).$$

Модель обучается с использованием функции потерь, которая минимизирует разницу между предсказанными и истинными значениями. Обычно используется кросс-энтропийная потеря:

$$\mathcal{L} = -\sum_{i=1}^{N} y_i \log(\hat{y}_i),$$

где y_i – истинное значение, а $\hat{y}_i$ – предсказанное значение.

Модель A5 может использовать различные стратегии декодирования, включая декодирование и выбор, что позволяет генерировать

текст на основе предыдущих токенов. Эти математические концепции позволяют модели A5 обрабатывать и генерировать текст, учитывая его контекстуальную и последовательную структуру.

T5 представляет собой модель, способную решать широкий спектр задач на основе единой текстовой формулировки, что делает ее важным шагом в эволюции технологий обработки естественного языка [Калинина 2023].

Рассмотрим данную модель более детально. На языке Python реализуем его с помощью встроенных библиотек и библиотеки Transformers.

```
from transformers import T5Tokenizer, T5ForConditionalGeneration
# Загрузка модели и токенизатора T5
model_name = «t5-small»
tokenizer = T5Tokenizer.from_pretrained(model_name)
model = T5ForConditionalGeneration.from_pretrained(model_name)

# Пример текста для обработки
input_text = «translate English to French: How are you?»
# Токенизация входного текста
input_tokens = tokenizer.encode(input_text, return_tensors=»pt»)
# Генерация текста
output_tokens = model.generate(input_tokens)
# Декодирование сгенерированных токенов в текст
output_text = tokenizer.decode(output_tokens[0], skip_special_tokens=
True)
# Вывод результата
print(“Сгенерированный текст:”, output_text)
```

Загружаем предобученную модель T5 и соответствующий токенизатор. В данном случае используем t5-small модель, но можно выбрать и другие версии. Далее в качестве примера ставим задачу перевода текста с английского языка на французский. Входной текст конвертируется в токены, которые могут быть обработаны моделью. С помощью метода *generate* мы получаем сгенерированные токены. Преобразуем эти токены обратно в текст, игнорируя специальные токены, и выводим сгенерированный текст.

Модель BART (Bidirectional and Auto-Regressive Transformers) представляет собой передовую архитектуру для обработки естественного языка, разработанную для решения задач, таких как суммирование текста, машинный перевод и генерация текста. BART сочетает в себе элементы bidirectional и auto-regressive подходов, что делает его весьма уникальным и эффективным. В связи с тем,

что BART является комбинацией двух разных типов трансформеров, рассмотрим более детально ее основные компоненты [Носкина 2024].

BART основывается на архитектуре трансформера и включает в себя два основных этапа: кодирования и декодирования. Двухсторонняя структура в модели позволяет эффективно создавать из предложения последовательности, извлекать и обрабатывать контекстные зависимости. Используя слои самообучения (self-attention) и полносвязные слои, кодировщик BART обрабатывает входной текст через строительство контекстного представления каждого токена на основе всех токенов в предложении. Это позволяет захватывать как местные, так и глобальные зависимости в тексте. Декодировщик модели BART использует авторегрессию, то есть происходит генерация последовательности токен за токеном. Это основано не только на кодировочных представлениях, но и на ранее предсказанных токенах. Что позволяет декодировщику учитывать контекст уже сгенерированного текста [Глазкова 2023].

```
import torch
from transformers import
BartTokenizer, BartForConditionalGeneration
model_name = “facebook/bart-large-cnn” # Вы можете использовать другие версии модификации BART
tokenizer = BartTokenizer.from_pretrained(model_name)
model = BartForConditionalGeneration.from_pretrained(model_name)
input_text =
    (“The BART model is a transformer-based model that is particularly effective for text generation tasks”.
    “It combines the benefits of bidirectional context, as in BERT, and the autoregressive nature of GPT”.
    “BART can be used for a variety of tasks including text summarization, machine translation, and more”).
input_tokens = tokenizer.encode(input_text, return_tensors=”pt”, max_length=1024, truncation=True)
summary_ids = model.generate(input_tokens, max_length=100, min_length=30,
                    length_penalty=2.0, num_beams=4, early_stopping=True)
summary_text = tokenizer.decode(summary_ids[0], skip_special_tokens=True)
print(«Сумма текста:», summary_text)
```

– подходит для множества задач, включая перевод, суммирование, классификацию и т. д.;

– позволяет легко адаптировать модель к новым задачам, просто меняя формат ввода;
– показывает отличные результаты на многих benchmark-тестах.

Недостаток модели T5 – достаточно тяжелая, что может быть проблемой для обучения и развертывания.

BART – модель, соединяющая двунаправленный подход (как у BERT) и авторегрессионный подход (как у GPT). Разработанная Facebook, BART становится особенно полезной для задач, связанных с генерацией текста.

Отметим достоинства модели BART:
– хорошо справляется с задачами суммирования и редактирования текста;
– модель понимает контекст благодаря двунаправленному обучению на больших корпусах.

Недостаток модели BART – требует значительных вычислительных ресурсов.

GPT – серия моделей, оптимизированная для генерации текста. Она использует авторегрессионный подход и хорошо подходит для создания диалоговых систем.

Достоинства модели GPT:
– обеспечивает естественный и связный разговорный стиль, эффективно поддерживая диалоги;
– модель способна создавать разнообразный текст без заданного шаблона, что делает ее полезной для креативных задач;
– может адаптироваться к различным контекстам, что делает ее хорошим выбором для личных ассистентов и чат-ботов.

Недостаток модели GPT – не так хорошо справляется с задачами, требующими четко заданного формата вывода, как T5 и BART.

При генерации текстов с использованием искусственного интеллекта существуют риски, связанные с недопониманием контекста или созданием нежелательного контента. Они могут быть вызваны, например, тем, что искусственный интеллект интерпретирует вводимые данные не так, как ожидал пользователь, что приводит к неуместным или ошибочным ответам; кроме того, если в обучающем наборе данных содержится предвзятая, оскорбительная или недостоверная информация, это также может сказаться на качестве генерируемых текстов. Например, даже простая замена слов или изменение порядка слов может привести к совершенно другим результатам [Титов 2023].

Чтобы минимизировать эти риски, разработчики и исследователи постоянно работают над улучшением алгоритмов и повышением качества обучающих данных. Создаются механизмы контроля за содержанием, а также разрабатываются методы, поз-

воляющие пользователям лучше понимать границы возможностей ИИ, являющегося инструментом, использование которого требует ответственности как от разработчиков, так и от пользователей.

Каждая из упомянутых моделей обладает уникальными сильными и слабыми сторонами, поэтому выбор наиболее подходящей модели зависит от специфики задачи. T5 демонстрирует высокую адаптивность, что делает его более подходящим для разнообразных задач обработки текста. В то же время BART показывает выдающиеся результаты в редактировании и создании связного текста, а GPT превосходит другие модели в области диалогового взаимодействия и креативной текстовой генерации.

Кроме того, обе модели обладают высокой способностью к адаптации и дополнительному обучению на специализированных наборах данных, что позволяет значительно повышать их эффективность в узкоспециализированных задачах. Это открывает новые горизонты для применения T5 и BART в таких областях, как медицина, юриспруденция и образование, где критически важны точность и надежность результатов.

Однако существуют и определенные ограничения. Например, обе модели требуют значительных вычислительных ресурсов во время обучения, что может стать серьезной проблемой для мелких организаций или исследовательских групп. Кроме того, если модели обучены на данных низкого качества, существует риск генерации предвзятых или некорректных результатов.

Таким образом, модели T5 и BART представляют собой перспективные инструменты для решения задач обработки естественного языка. Их дальнейшее развитие будет способствовать улучшению качества взаимодействия человека с машинами, открывая новые горизонты для исследований и практического применения в различных сферах. В будущем стоит ожидать дальнейших улучшений в архитектуре и алгоритмах, что позволит повысить доступность таких моделей.

Литература

Билал 2024 – *Билал С.* Адаптация двунаправленных и авторегрессивных трансформеров для суммаризации текстов на арабском языке // Современные исследования: теория, практика, результаты: Сб. мат-лов IV Международной научно-практической конференции, Москва, 15 февраля 2024 года. М.: АНО ДПО «ЦРОН», 2024. С. 80–88.

Васильев 2023 – *Васильев Д.Д., Пятаева А.В.* Использование языковых моделей T5 для задачи упрощения текста // Программные продукты и системы. 2023. № 2. С. 228–236.

Гаврилова 2024 – *Гаврилова А.Е., Вагарина Н.С.* Обзор и оценка моделей-трансформеров для автоматического реферирования текстов // Проблемы управления в социально-экономических и технических системах: Материалы XX Международной научно-практической конференции: Сборник научных статей, Саратов, 17–18 апреля 2024 года. Саратов: Издательский центр «Наука», 2024. С. 371–374.

Глазкова 2023 – *Глазкова А.В., Морозов Д.А.* Многозадачное дообучение для генерации ключевых слов к научным текстам // Информационные технологии и нанотехнологии (ИТНТ-2023): Сб. тр. по мат-лам IX Международной конференции и молодежной школы: В 6 т. Самара, 17–23 апреля 2023 г. Т. 4. Самара: Самарский национальный исследовательский университет имени академика С.П. Королева, 2023. С. 40872.

Йылдырым 2022 – *Йылдырым С., Асгари-Ченаглу М.* Осваиваем архитектуру Transformer. Разработка современных моделей с помощью передовых методов обработки естественного языка. М.: ДМК-Пресс, 2022. 320 с.

Калинина 2023 – *Калинина А.Ю., Киреев В.С.* Визуализация корпуса документов с помощью извлечения сущностей и связей предметной области на основе нейросетевой модели глубокого обучения T5 // XXV Международная научно-техническая конференция «НЕЙРОИНФОРМАТИКА-2023»: Сб. науч. тр., Москва, 23–27 октября 2023 г. М.: МИФИ, 2023. С. 312–320.

Лезгян 2023 – *Лезгян А.С.* Автоматическое реферирование текстов: классификация, архитектуры, современные подходы и проблемы // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2023. № 1. С. 19–27.

Носкина 2024 – *Носкина А.В., Мельничук Д.В.* Сравнение NLP-моделей на задаче суммаризации академических текстов на русском языке // Компьютерная лингвистика и вычислительные онтологии. 2024. № 7. С. 54–59. DOI: 10.17586/2541-9781-2024-7-54-59.

Титов 2023 – *Титов А.П.* Анализ моделей адаптивных нейро-нечетких систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 21–35.

Fishcheva 2022 – *Fishcheva I.N., Osadchiy D., Bochenina K.O., Kotelnikov E.V.* Argumentative Text Generation in Economic Domain // Computational Linguistics and Intellectual Technologies: Papers from the Annual International Conference “Dialogue” (2022). Vol. 21. Moscow, 15–18 June 2022. Moscow: RSUH, 2022. P. 211–222.

References

Bilal, S. (2024), “Adaptation of bidirectional and autoregressive transformers for the summarization of texts in Arabic”, *Modern research: theory, practice, results: Proceedings of the 4th Scientific and Practical International Conference*, Moscow, February 15, 2024, ANO DPO “TSRON”, Moscow, Russia, pp. 80–88.

Fischeva, I.N., Osadchy, D., Bochenina, K.O. and Kotelnikova, E.V. (2022), "Argumentative Text Generation in Economic Domain", *Computational Linguistics and Intellectual Technologies.*

Papers from the Annual International Conference "Dialogue" (2022), Moscow, June 15–18, Issue 21, RSUH, Moscow, Russia, pp. 211–222.

Gavrilova, A.E. and Vagarina, N.S. (2024), "Review and evaluation of transformer models for automatic text abstraction", *Management issues in socio-economic and technical systems. Proceedings of the 20th Scientific and Practical International Conference. Coll. of articles*, Saratov, April 17–18, Izdat. tsentr "Nauka", Saratov, Russia, pp. 371–374.

Glazkova, A.V. and Morozov, D.A. (2023), "Multitasking retraining for generating keywords for scientific texts", *Information technologies and nano-technologies (ITNT-2023). Sat. Art. by the Proceedings of the 9th International Conference and Youth School in 6 vols.*, Samara, April 17–23, vol. 4, Samara National Research University, Samara, Russia, p. 40872.

Iyldyrym S.,and Asgari-Chenaglu M. (2022), *Osvaivaem arkhitekturu Transformer. Razrabotka sovremennykh modelei s pomoshch'yu peredovykh metodov obrabotki estestvennogo yazyka* [Mastering Transformer architecture. Developing modern models using advanced natural language processing methods], DMK-Press, Moscow, Russia, 320 pp.

Kalinina, A.Y. and Kireev, V.S. (2023), "Visualization of the documents corpus by extracting entities and domain connections based on the deep learning neural network model T5", *25th Scientific and Technical International Conference "NEUROINFORMATICS-2023". Coll. of scientific papers*, Moscow, October 23-27, 2023, National Research Nuclear University MEPhI, Moscow, Russia, pp. 312–320.

Lezgian, A.S. (2023), "Automatic text abstraction. Classification, architecture, modern approaches and issues", *Mathematical modeling, computer and field experiment in natural sciences*, no. 1, pp. 19–27.

Noskina, A.V. and Melnichuk, D.V. (2024), "Mastering NLP methods for the purpose of summarizing academic texts in Russian", *Computer Network-System and Computing technologies*, no. 7, pp. 54–59.

Titov, A.P. (2024), "Analysis of models of adaptive neuro-fuzzy systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1. pp. 21–35.

Vasil'ev, D.D. and Pyataeva, A.V. (2023), "Using the T5 language models for the text simplification task", *Software products and Systems*, no. 2, pp. 228–236.

Информация об авторах

Андрей П. Титов, кандидат технических наук, доцент, МИРЭА – Российский технологический университет, Москва, Россия; 119454, Россия, Москва, пр. Вернадского, д. 78; titov_and@mail.ru

Наталия В. Гришина, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6, стр. 6;

Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38 стр. 1; grnat@ rambler.ru

Дарья Н. Титова, Образовательный центр «Протон», Москва, Россия; 121309, Россия, Москва, ул. Барклая, д. 15, корп. 3; decestoeva@gmail.com

Information about the authors

Andrei P. Titov, Cand. of Sci. (Computer Science), associate professor, MIREA – Russian Technological University, Moscow, Russia; bld. 78, Vernadskii Lane, Moscow, 119454, Russia; titov_and@mail.ru

Nataliya V. Grishina, Cand. of Sci. (Computer Science), associate professor, Russian State University for the Humanities, Moscow, Russia; 6-6, Miusskaya Sq., Moscow, 125047, Russia;

Moscow State Linguistic University, Moscow, Russia; 38-1, Ostozhenka St., Moscow, 119034, Russia; grnat@ rambler.ru

Dar'ya N. Titova, Proton Educational Center, Moscow, Russia; 15-3, Barklaya St., Moscow, 121309, Russia; decestoeva@gmail.com

УДК 004.491.22
DOI: 10.28995/ 2686-679X-2025-3-21-35

Шифрование и дешифрование файлов с помощью алгоритма AES в режиме CBC на Python

Марьяна А. Георгиева
Кабардино-Балкарский государственный университет, Нальчик, Россия, maryana.g@list.ru

Алим З. Кашежев
Кабардино-Балкарский государственный университет, Нальчик, Россия, alim.kashezhev562@gmail.com

Аннотация. В данной работе рассматривается реализация алгоритма шифрования AES (Advanced Encryption Standard) в режиме CBC (Cipher Block Chaining) с использованием языка программирования Python. Актуальность темы обусловлена возрастающими рисками утечки и несанкционированного доступа к данным в условиях роста объема передаваемой и хранимой информации. AES является одним из наиболее надежных и широко применяемых алгоритмов симметричного шифрования, поддерживающего ключи длиной 128, 192 и 256 бит, что позволяет гибко настраивать уровень безопасности в зависимости от требований задачи. Цель работы – разработка программы для шифрования и дешифрования файлов с использованием AES в режиме CBC. Программа реализована с использованием библиотек PyQt6 для создания графического интерфейса и Crypto, а также hashlib для выполнения криптографических операций. В приложении предусмотрены два режима работы: автоматический (с фиксированным паролем) и ручной (с вводом пароля пользователем). Основные этапы работы алгоритма включают генерацию ключа и вектора инициализации на основе пароля, шифрование и дешифрование данных с использованием режима CBC, а также обработку ошибок для обеспечения устойчивости программы. Результатом работы стало создание надежного и удобного инструмента для защиты конфиденциальных данных, который демонстрирует практическую применимость AES в реальных сценариях. Приложение обеспечивает высокий уровень безопасности благодаря использованию AES и режима CBC, что делает его устойчивым к современным криптографическим атакам. Разработанное решение может быть использовано для защиты личных и корпоративных данных, а также для изучения принципов работы криптографических алгоритмов.

Ключевые слова: симметричное шифрование, криптостойкие ключи, защита данных, PBKDF2 алгоритм

Для цитирования: *Георгиева М.А., Кашежев А.З.* Шифрование и дешифрование файлов с помощью алгоритма AES в режиме CBC на Python // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 21–35. DOI: 10.28995/ 2686-679X-2025-3-21-35

File encryption and decryption using the AES algorithm in CBC mode with Python

Mar'yana A. Georgieva
Kabardino-Balkarian State University, Nalchik, Russia, maryana.g@list.ru

Alim Z. Kashezhev
Kabardino-Balkarian State University, Nalchik, Russia, alim.kashezhev562@gmail.com

Abstract. The article considers the implementation of the AES (Advanced Encryption Standard) encryption algorithm in CBC (Cipher Block Chaining) mode using the Python programming language. The relevance of the topic stems from growing risks of data leakage and unauthorized access amid increasing volumes of transmitted and stored information. AES is one of the most secure and widely adopted symmetric encryption algorithms, supporting 128-, 192-, and 256-bit keys, enabling flexible adjustment of security levels based on task requirements. The goal of the work is to develop a program for file encryption and decryption using AES in CBC mode. The program is implemented with the PyQt6 libraries for creating a graphical user interface and Crypto and also hashlib for cryptographic operations. The application features two modes: automatic (with a fixed password) and manual (with user-defined password input). The main stages of the algorithm include password-based key and initialization vector generation based on the password, CBC-mode encryption/decryption, and error handling to ensure program stability. The result is a reliable and user-friendly tool for protecting confidential data, demonstrating the practical applicability of AES in real-world scenarios. The application provides a high level of security through AES and CBC mode, making it resistant to modern cryptographic attacks. The developed solution can be used to safeguard personal and corporate data, as well as to study the principles of cryptographic algorithms.

Keywords: symmetric encryption, cryptographically secure keys, data protection, PBKDF2 algorithm

For citation: Georgieva, M.A. and Kashezhev A.Z. (2025), “File encryption and decryption using the AES algorithm in CBC mode with Python”, *RSUH/RGGU Bulletin. “Information Science. Information security. Mathematics” Series*, no. 3, pp. 21–35, DOI: 10.28995/ 2686-679X-2025-3-21-35

Введение

С развитием интернета, облачных технологий и цифровых коммуникаций объем передаваемой и хранимой информации увеличивается экспоненциально, что чревато увеличением рисков, которые связаны с утечкой, кражей или несанкционированным доступом к защищаемым данным [Александрова 2024]. Несмотря на то, что алгоритм AES в режиме CBC широко применяется, многие существующие реализации сталкиваются с рядом ограничений. В первую очередь, инструменты шифрования чаще всего ориентированы на технически подготовленных пользователей, от которых требуется работа через командную строку или же использование сложных настроек, что затрудняет их использование в повседневных сценариях [Назаровская 2024]. Помимо этого, в некоторых решениях применяются устаревшие методы генерации ключа, такие как хэширование MD5, которое уязвимо к коллизиям и не соответствует современным стандартам криптографической стойкости [Хаширова 2019]. Кроме того, отсутствие гибких режимов работы ограничивает адаптивность таких программ под различные требования безопасности. В связи с этим одной из важнейших задач в данном вопросе выступает обеспечение безопасности данных с использованием алгоритма AES. Среди множества алгоритмов шифрования Advanced Encryption Standart (AES) можно рассматривать как один из наиболее надежных и широко применяемых методов.

Разработанное программное обеспечение позволяет устранить описанные проблемы благодаря внедрению в него новых возможностей. Так, во-первых, интеграция современного графического интерфейса на базе PyQt6, который делает процесс шифрования и дешифрования доступным для пользователей без глубоких технических знаний, а также использование двух режимов – автоматического и ручного – обеспечивает гибкость в выборе степени контроля над процессом. Во-вторых, улучшена генерация ключей: вместо MD5 используется более доработанная реализация алгоритма PBKDF2 с SHA-256 для формирования ключа и вектора инициализации, благодаря чему повышается устойчивость к атакам перебора, так как PBKDF2 реализует механизм так называемого растяжения ключа с тысячами итераций, что значительно усложняет подбор

пароля злоумышленником[1]. В-третьих, выполнение комплексной обработки ошибок, включая проверку целостности пароля и обработку исключений при работе с файлами, что не только повышает надежность программы, но и делает ее более дружелюбной для конечного пользователя [Гавриленко 2021]. В-четвертых, использование режима CBC, который дополнен механизмом автоматического добавления и удаления padding'а, что позволяет исключить ошибки при шифровании файлов произвольного размера.

Целью данного исследования является исследование процесса шифрования и дешифрования файлов с использованием языка программирования Python. В рамках данной работы будут рассмотрены основные этапы реализации алгоритма AES, включая генерацию ключей, шифрование и дешифрование данных.

Алгоритм AES, в свою очередь, относится к классу симметричных блочных шифров, что означает использование одного и того же ключа как для шифрования, так и для дешифрования данных [Русецкая 2021]. Данный алгоритм поддерживает три длины ключа: 128, 192 и 256 бит, благодаря чему появляется возможность гибко настраивать уровень безопасности в зависимости от требований той или иной задачи[2]. За счет многократного применения операций замещения, перестановки, смешивания и добавления ключа обеспечивается высокая криптостойкость алгоритма AES [Вепрев 2025]. Эти операции выполняются в несколько раундов, а именно: 10 раундов для 128-битного ключа, 12 раундов для 192-битного и 14 раундов для 256-битного ключа.

Актуальность выбранной темы обусловлена несколькими факторами. Во-первых, Python благодаря своей простоте, гибкости и наличию мощных библиотек для работы с криптографией является если не самым, то одним из наиболее популярных языков программирования, на котором многие создают свои программные продукты. Во-вторых, AES широко применяется в реальных приложениях, и понимание его реализации на Python позволяет разработчикам создавать безопасные решения для защиты данных. И в-третьих, изучение практических аспектов шифрования на Python способствует более глубокому понимаю принципов работы криптографических алгоритмов и их применения в современных системах.

---

[1] *Boppreh P.* Pure Python implementation of AES, with optional cipher modes. URL: https://github.com/boppreh/aes (дата обращения 10.02.2025).

[2] *Diego V.V.* Implementation of AES CBC and CTR modes. URL: https://github.com/diegodvv/AES-CBC-CTR-implementation (дата обращения 10.02.25).

В соответствии с поставленной задачей была разработана программа на языке программирования Python, позволяющая как шифровать, так и дешифровать хранимые файлы.

При создании приложения был реализован графический интерфейс (GUI) для удобного взаимодействия с пользователем при шифровании и дешифровании файлов с использованием AES алгоритма. В свою очередь, программа была разработана с использованием таких библиотек, как PyQt6 для создания интерфейса и pycryptodome для реализации криптографических операций. Таким образом, программа включает в себя следующие компоненты:

1. Графический интерфейс, содержащий окно приложения с элементами управления для выбора файла, ввода пароля, выбора режима шифрования «Автоматический» и «Ручной» для выполнения операций шифрования и дешифрования.

2. Логика шифрования и дешифрования, заключающаяся в реализации алгоритма AES с использованием режима сцепления блоков шифротекста (CBC) для обеспечения безопасности данных.

3. Обработка ошибок, включающая в себя механизмы обработки ошибок, такие как проверка корректности пароля и обработка исключений при операциях с файлами.

Поскольку алгоритм AES является симметричным блочным шифром, работающим с блоками данных фиксированного размера – 128 бит, в приложении требуется использование режима CBC, который предполагает наличие вектора инициализации (IV) для обеспечения уникальности шифрования каждого блока данных.

В первую очередь стоит начать с генерации ключа и вектора инициализации. В данной программе ключ и вектор инициализации генерируются на основе пароля, который ввел пользователь или же был автоматически введен программой, реализуемой с помощью функции под названием “derive_key_and_init_vector”. Эта функция использует хэширование PBKDF2-SHA256, взятое из встроенной в Python библиотеки под названием “hashlib” для создания последовательности байтов, которая затем делится на ключ и вектор инициализации и представлена в коде следующим образом:

```
from hashlib import pbkdf2_hmac
def derive_key_and_init_vector(self, password, salt, key_length=32,
init_vect_length=16, iterations=100000):
    derived_key = pbkdf2_hmac(
        sha256’,
        password.encode(‘utf-8’),
```

```
    salt,
    iterations,
    dklen=key_length + init_vect_length
)
return derived_key[:key_length], derived_key[key_length:key_
length+init_vect_length]
```

Вместе с тем стоит отметить, что salt (или соль) здесь играет роль случайной последовательности байтов, которая добавляется к паролю для увеличения сложности атаки методом перебора [Арванова 2024].

Теперь рассмотрим сам процесс шифрования данных, состоящий из нескольких этапов. В первую очередь происходит генерация ранее описанного salt с помощью функции get_random_bytes, которая возвращает случайные байты и получение ключа вместе с вектором инициализации.

После этого происходит инициализация шифра AES в режиме CBC. Данный режим означает, что каждый блок данных перед шифрованием выполняется в виде XOR с результатом шифрования предыдущего блока. Благодаря этому обеспечивается зависимость между блоками, что делает шифрование более устойчивым к атакам.

На следующем этапе происходит чтение данных из файла блоками, размер которых кратен размеру блока AES, а именно 16 байт, что необходимо для корректной работы алгоритма, после чего происходит их шифрование.

Далее выполняется добавление дополнений (padding) к последнему блоку данных для соответствия размеру блока AES с помощью вычисления количества байт, которые необходимо добавить. Однако стоит отметить, что дополнение добавляется в том случае, когда размер последнего блока данных меньше 16 байт, чтобы выровнять размер блока, потому как алгоритм AES работает с блоками фиксированного размера, а именно 16 байт [Свейгарт 2020].

И наконец после шифрования всех блоков данных, включая последний блок с PKCS7 padding, начинается последний этап, в котором зашифрованные данные записываются в выходной файл. Данный этап проходит в два действия:

1. В начале файла записывается salt, который необходим, как было отмечено ранее, для генерации ключа и вектора инициализации при дешифровании.

2. Зашифрованные данные записываются в файл блоками, в результате чего получается файл, который содержит salt и зашифрованные данные:

```
from Crypto.Util.Padding import pad
from Crypto.Random import get_random_bytes
def encrypt(self, inp_file, outp_file, password, key_length=32):
    block_size = AES.block_size
    salt = get_random_bytes(block_size) # Генерация криптостойкой соли
    key, init_vect = self.derive_key_and_init_vector(password, salt, key_
    length, block_size)
    cipher = AES.new(key, AES.MODE_CBC, init_vect)
    outp_file.write(salt)
    while True:
        chunk = inp_file.read(1024 * block_size) # Чтение блоками по 16 КБ
        if not chunk:
            break
        if len(chunk) % block_size != 0 or len(chunk) == 0:
            chunk = pad(chunk, block_size)
        outp_file.write(cipher.encrypt(chunk))
```

Далее рассмотрим, как происходит процесс дешифрования. Сперва происходит чтение salt из зашифрованного файла. Однако, как было отмечено ранее, при шифровании salt записывается в начало зашифрованного файла, а значит, ее можно извлечь без повторной генерации, что упрощает дешифровку файла.

Затем происходит повторная генерация ключа и вектора инициализации с помощью ранее упомянутой функции derive_key_and_init_vector. Однако здесь теперь salt передается из зашифрованного файла.

Далее, как и в случае с шифрованием данных, формируется объект шифра AES в режиме CBC.

После этого зашифрованные данные читаются из файлов блоками по 1024 * block_size байт (обычно 16 КБ) и затем каждый блок дешифруется с использованием объекта шифра AES.

И окончательный этап дешифрования – удаление дополнений (padding) из последнего блока данных. На данном этапе после дешифрования последнего блока данных проверяется значение последнего байта, которое указывает на количество добавленных байтов дополнения, затем эти байты удаляются из данных:

```
from Crypto.Util.Padding import unpad
from Crypto.Cipher import AES
def decrypt(self, input_file, password, key_length=32):
    block_size = AES.block_size
    salt = input_file.read(block_size)
```

```
key, init_vector = self.derive_key_and_init_vector(password, salt,
key_length, block_size)
cipher = AES.new(key, AES.MODE_CBC, init_vector)
decrypted_data = b''
buffer = b''
try:
    while True:
        chunk = input_file.read(1024 * block_size)
        if not chunk:
            break
        buffer += cipher.decrypt(chunk)
    decrypted_data = unpad(buffer, block_size)
except (ValueError, KeyError) as e:
    raise ValueError("Ошибка дешифрования: неверный пароль или
поврежденные данные") from e
return decrypted_data
```

Изучив принцип работы шифрования и дешифрования файлов в режиме CBC, стоит рассмотреть работоспособность самой программы. Сперва пользователя приветствует окно приложения, на котором пользователь может выбрать один из режимов работы приложения для шифрования и дешифрования файлов, а именно: «Автоматический» и «Ручной». В автоматическом режиме пользователю не нужно вводить пароль для шифрования файла, он фиксированный, задается программой в виде случайного набора символов, однако при желании можно посмотреть введенный пароль. В этом случае пользователю нужно лишь выбрать файл, который необходимо зашифровать, нажав на кнопку «Зашифровать файл». После этого, если пользователю нужно будет дешифровать данный файл, он должен, не закрывая программу, нажать на кнопку «Дешифровать файл». Во втором режиме принцип действий практически идентичен первому, однако здесь уже пользователь сам задает в соответствующем текстовом поле пароль, для того чтобы зашифровать или дешифровать файл, и, как было описано ранее, пользователь может посмотреть введенный им пароль. Результат реализации соответствующего программного продукта с графическим интерфейсом представлен на рис. 1.

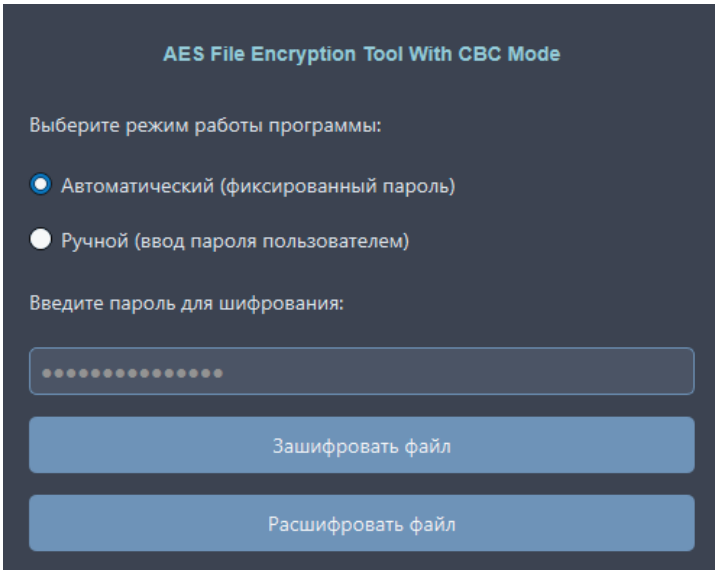
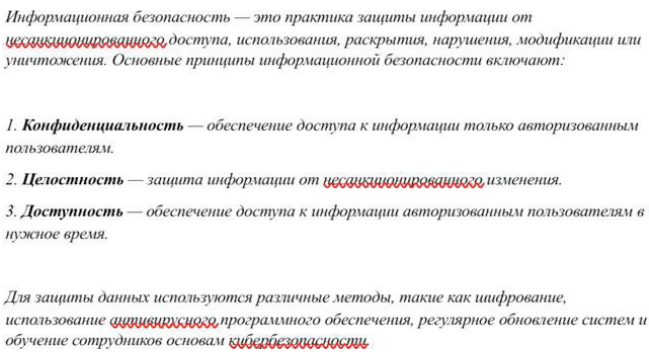


Рис. 1. Графический интерфейс программы

Теперь, в качестве примера, попробуем зашифровать исходный файл под названием “input_file” в формате “.docx” со следующим содержанием, представленным на рис. 2:


Информационная безопасность — это практика защиты информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Основные принципы информационной безопасности включают:

*1. **Конфиденциальность** — обеспечение доступа к информации только авторизованным пользователям.*

*2. **Целостность** — защита информации от несанкционированного изменения.*

*3. **Доступность** — обеспечение доступа к информации авторизованным пользователям в нужное время.*

Для защиты данных используются различные методы, такие как шифрование, использование антивирусного программного обеспечения, регулярное обновление систем и обучение сотрудников основам кибербезопасности.

Рис. 2. Содержимое файла input_file.docx

Далее выбирается ручной режим работы для демонстрации работоспособности пользовательского ввода. Для примера в качестве пароля будет выступать набор символов A34_k@1%d4/, который отображен на рис. 3.

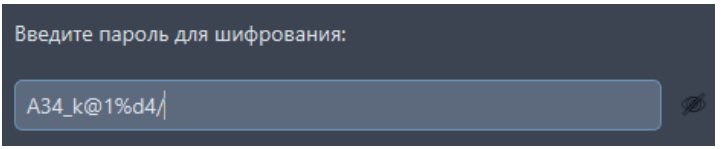


Рис. 3. Пользовательский ввод пароля в ручном режиме

Затем выбирается файл, который необходимо зашифровать (в данном случае это файл “input_file.docx”). В результате выполнения данных действий появляется всплывающее окно, приведенное на рис. 4, которое сообщает пользователю об успешном завершении шифрования файла:

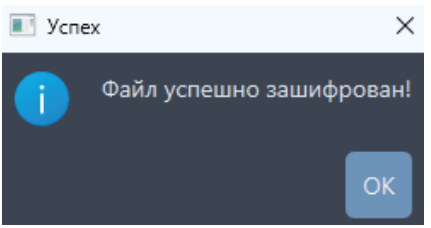


Рис. 4. Всплывающее окно об успешном выполнении операции

И теперь в корневой папке пользователь может увидеть файл под названием “output_file_encrypted.docx”, представляющий собой зашифрованный файл, который отображен на рис. 5.

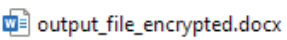


Рис. 5. Зашифрованный файл

На данном этапе, когда пользователь пытается открыть полученный файл в соответствующей программе, он сталкивается с проблемой, которая не позволяет просмотреть содержимое. Это, в свою очередь, указывает на то, что файл был модифицирован, как видно из рис. 6.

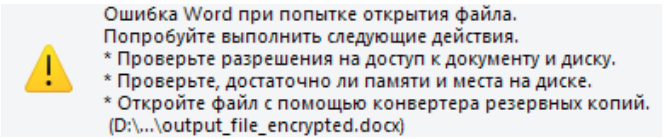


Рис. 6. Ошибка при попытке открытия зашифрованного файла

Разобравшись с шифрованием файла, стоит перейти к его дешифровке. Для проведения данной операции необходимо выбрать зашифрованный файл, использовав тот же пароль, что и при шифровании. После того как был выбран нужный файл, программа экспортирует дешифрованный файл, но уже под названием “output_file_decrypted.docx”, который пользователь может открыть без каких-либо проблем и убедиться в том, что получившийся результат соответствует содержимому input_file, содержание которого представлено на рис. 7.

Информационная безопасность — это практика защиты информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Основные принципы информационной безопасности включают:

*1. **Конфиденциальность** — обеспечение доступа к информации только авторизованным пользователям.*

*2. **Целостность** — защита информации от несанкционированного изменения.*

*3. **Доступность** — обеспечение доступа к информации авторизованным пользователям в нужное время.*

Для защиты данных используются различные методы, такие как шифрование, использование антивирусного программного обеспечения, регулярное обновление систем и обучение сотрудников основам кибербезопасности.

Рис. 7. Содержимое файла output_file_decrypted.docx

Однако, если же пользователь введет неправильный пароль для дешифрования, то увидит всплывающее окно с сообщением о том, что пароль неверный, как показано на рис. 8.

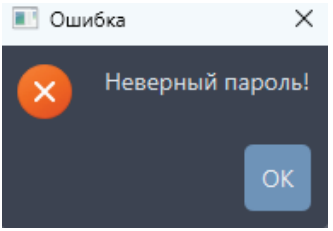


Рис. 8. Ошибка при вводе неправильного пароля

Выводы

Разработанный программный продукт позволяет не только устранить недостатки существующих решений, но и расширить сферу применения программы. Использование PBKDF2 с SHA-256 вместо MD5, интеграция интуитивного GUI и поддержка гибридных режимов работы обеспечивают актуальность приложения как для защиты персональных данных, так и для образовательных целей, демонстрируя современные подходы к реализации криптографических алгоритмов, что подчеркивает новизну разработки и ее соответствие нынешним требованиям информационной безопасности.

AES с учетом режима CBC обеспечивает высокий уровень безопасности, что делает его наиболее предпочтительным выбором для защиты конфиденциальных данных. Режим CBC, используемый в данной работе, добавляет дополнительный уровень защиты за счет использования вектора инициализации (IV), который гарантирует, что даже идентичные блоки данных будут зашифрованы по-разному. Это предотвращает возможность анализа зашифрованных данных на основе повторяющихся шаблонов, что особенно важно при работе с большими объемами информации или файлами, содержащими повторяющиеся структуры [Васильева 2025]. Благодаря использованию данного алгоритма удалось создать надежное и эффективное приложение с высокой криптографической стойкостью для шифрования и дешифрования файлов. Это делает алгоритм устойчивым к современным атакам, включая атаки методом полного перебора (brute force), что особенно важно в условиях роста вычислительных мощностей и появления новых методов криптоанализа.

Кроме того, AES оптимизирован для работы на современных процессорах, что позволяет эффективно шифровать и дешифро-

вать данные даже на устройствах с ограниченными ресурсами[3]. Разработанное приложение демонстрирует не только надежность алгоритма AES, но и его практическую применимость в реальных сценариях. Как было сказано ранее, благодаря интуитивно понятному графическому интерфейсу пользователи могут легко шифровать и дешифровать файлы, не обладая глубокими знаниями в области криптографии. И вместе с этим поддержка двух режимов работы – автоматического (с фиксированным паролем) и ручного (с вводом пароля пользователем) – позволяет адаптировать приложение под различные задачи и требования безопасности.

Литература

Александрова 2024 – *Александрова П.С., Червинчук А.С., Резниченко С.А.* Проверка соответствия банковской системы требованиям к защите информации в платежной системе // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 39–55.

Арванова 2024 – *Арванова С.М.* Перспективы применения высокоскоростных генераторов случайных чисел для аутентификации доступа и распределения ключей // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки». 2024. № 8. С. 67–70.

Васильева 2025 – *Васильева И.Н.* Криптографические методы защиты информации: учебник и практикум для вузов. М.: Юрайт, 2025. 310 с.

Вепрев 2025 – *Вепрев С.Б., Нестерович С.А., Макаров А.В.* Анализ уязвимостей в операционных системах и прикладных программных продуктах // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 1. С. 95–105.

Гавриленко 2021 – *Гавриленко А.В.* Дистанционное обучение и информационная безопасность // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 1. С. 51–65. DOI: 10.28995/2686-679X-2021-1-51-65.

Назаровская 2024 – *Назаровская В.С., Баранников Д.Н., Русецкая И.А.* Информационная безопасность библиотечных систем предприятий // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 87–103.

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

[3] Examples in PythonEncryptionAES. Decryption // Practical Cryptography for Developers. https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/content/symmetric-key-ciphers/aes-encrypt-decrypt-examples.html (дата обращения 10.02.2025).

Свейгарт 2020 – *Свейгарт Э.* Криптография и взлом шифров на Python / Пер. с англ. А.Г. Гузикевич; ред. В.Р. Гинзбург. М.; СПб.: Диалектика, 2020. 512 с.

Хаширова 2019 – *Хаширова Т.Ю.* Модель обобщенной оценки защищенности информации в интегрированных системах безопасности // Университетский научный сборник № 3: Сб. науч. тр. национальной университетской научно-практической конференции, приуроченной к 85-летию со дня основания Кабардино-Балкарского государственного университета, Нальчик, 20–25 сентября 2019 г. / Ред. Т.Ю. Хаширова, И.И. Мамучиев, М.И. Мамучиева, Е.К. Эдгулова. Нальчик: Кабардино-Балкарский государственный университет им. Х.М. Бербекова, 2019. Т. 1. С. 155–161.

References

Aleksandrova, P.S., Chervinchuk, A.S. and Reznichenko, S.A. (2024), "Checking the compliance of the banking system with the requirements for the protection of information in the payment system", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 39–55.

Arvanova, S.M. (2024), "Prospects for application of high-speed random number generators for access authentication and key distribution", *Modern Science: actual problems of theory and practice. Series: Natural and technical sciences*, no. 8, pp. 67–70.

Gavrilenko, A.V. (2021), "Distance learning and information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 51–65.

Khashirova, T.Y. (2019), "Model of generalized assessment of information security in integrated security systems", in Khashirova, T.Y., Mamuchiev, I.I., Mamuchieva, M.I. and Edgulova, E.K. (ed.), *University Scientific Collection No. 3: Coll. of scientific papers of the National University Scientific-Practical Conference Commemorating the 85th anniversary of Kabardino-Balkarian State University*, Nalchik, September 20–25, 2019, vol. 1. Kabardino-Balkarian State University named after K.M. Berbekov. Nalchik, Russia, pp. 155–161.

Nazarovskaya, V.S., Barannikov, D.N. and Rusetskaya, I.A. (2024), "Information security of enterprise library systems", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 87–103.

Rusetskaya, I.A. (2021), "Cryptography. From the past to the future", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 47–57.

Sweigart, E. (2020), *Kriptografiya i vzlom shifrov na Python* [Cryptography and cipher cracking in Python], Dialectics-Williams, Moscow, Russia, 592 p.

Vasil'eva, I.N. (2025), *Kriptograficheskie metody zashchity informatsii: uchebnik i praktikum dlya vuzov* [Cryptographic Methods of Information Protection. Textbook and Workshop for Universities], Yurait, Moscow, Russia, 310 p.

Veprev, S.B., Nesterovich, S.A. and Makarov, A.V. (2025), “Vulnerability analysis in operating systems and application software products”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series*, no. 1, pp. 95–105.

Информация об авторах

Марьяна А. Георгиева, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; maryana.g@list.ru

Алим З. Кашежев, студент, Кабардино-Балкарский государственный университет, Нальчик, Россия; 360004, Россия, Нальчик, ул. Чернышевского, д. 173; alim.kashezhev562@gmail.com

Information about the authors

Mar’yana A. Georgieva, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevskogo Str., Nalchik, 360004, Russia; maryana.g@list.ru.

Alim Z. Kashezhev, student, Kabardino-Balkarian State University, Nalchik, Russia; bld. 173, Chernyshevskogo Str., Nalchik, 360004, Russia; alim.kashezhev562@gmail.com

УДК 347.734:004.056
DOI: 10.28995/ 2686-679X-2025-3-36-53

Организационно-правовые особенности аудита информационной безопасности в кредитных организациях Российской Федерации

Егор О. Павлов
Финансовый университет при Правительстве РФ,
Москва, Россия, epavlov466@gmail.com

Сергей А. Резниченко
Финансовый университет при Правительстве РФ,
Москва, Россия;
Национальный исследовательский ядерный университет «МИФИ»,
Москва, Россия;
Российский государственный гуманитарный университет,
Москва, Россия, rsa_5@bk.ru

Аннотация. В современных условиях динамичная модернизация, эскалация и экстраполяция состояния информационно-цифровой среды банковского сектора порождает возникновение актуальных проблематик, тесно связанных с национальной безопасностью, и в частности с информационной безопасностью. Актуальной проблемой остается несовершенство информационных банковских и платежных систем, требующих постоянного контроля посредством аудита информационной безопасности. В данной научной работе рассматриваются вопросы совершенствования системы контроля, мониторинга и проверки информационной безопасности в кредитных организациях на основе аудита. Методологическая основа исследования включает анализ и систематизацию существующих подходов к аудиту информационной безопасности. В ходе работы выявлено несовершенство действующей законодательной базы и системы отчетности, а также установлено отсутствие в составе аудиторного отдела кредитных организаций штатного квалифицированного специалиста, отвечающего за аудит информационной безопасности. В рамках исследовательской работы разработаны рекомендации по систематизации нормативных документов Банка России, регламентирующих проведение аудита, улучшению внутренней документации банков, введению в штат аудиторских подразделений специалистов по информационной безопасности и включению результатов аудита в информационный ресурс Банка России. Практическая значимость полученных результатов заключается

в возможности применения их при проведении аудита информационной безопасности в банковском секторе. Результаты исследования могут быть использованы для модернизации структуры аудита информационной безопасности в кредитных организациях, повышения уровня защиты банковских и платежных систем и минимизации рисков, связанных с их эксплуатацией.

Ключевые слова: аудит информационной безопасности, кредитные организации, стандартизация требований, подразделение аудита

Для цитирования: Павлов Е.О., Резниченко С.А. Организационно-правовые особенности аудита информационной безопасности в кредитных организациях Российской Федерации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 36–53. DOI: 10.28995/ 2686-679X-2025-3-36-53

Organizational and legal peculiarities of information security audit in credit organizations Russian Federation

Egor O. Pavlov
Financial University under the Government of the Russian Federation, Moscow, Russia, epavlov466@gmail.com

Sergei A. Reznichenko
Financial University under the Government of the Russian Federation, Moscow, Russia;
National Research Nuclear University MEPhI, Moscow, Russia;
Russian State University for the Humanities, Moscow, Russia,
rsa_5@bk.ru

Abstract. In modern conditions, dynamic modernization, escalation and extrapolation of the state of the information and digital environment in the banking sector gives rise to the emergence of topical issues closely related to national security, and in particular, to information security. The imperfection of information banking and payment systems, which require constant control through information security audit, remains an urgent challenge. The research paper considers the issues of improving the system of control, monitoring and verification of information security in credit organizations based on audit. The methodological basis for the research includes the analysis and systematization of existing approaches to information security audit. The work reveals the imperfection of the current legislative framework and reporting system, as well as establishes the absence of a full–time qualified specialist responsible for information security au-

dit in the audit department of credit organizations. As part of the research work, recommendations were developed to systematize the Bank of Russia's regulatory documents governing the audit, to improve banks' internal documentation, to introduce information security specialists into the staff of audit departments and to include audit results in the Bank of Russia's information resource. The practical significance of the results obtained lies in the possibility of their applying when conducting information security audits in the banking sector. The results of the study can be used to modernize the structure of information security audit in credit institutions, to increase the level of protection of banking and payment systems and minimize the risks associated with their operation.

Keywords: information security audit, credit organizations, standardization of requirements, audit department

For citation: Pavlov, E.O. and Reznichenko, S.A. (2025), "Organizational and legal features of information security audit in credit organizations of the Russian Federation", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 36–53, DOI: 10.28995/ 2686-679X-2025-3-36-53

Введение

В условиях стремительной цифровизации банковского сектора и интеграции новейших информационно-коммуникационных технологий возрастают требования к обеспечению информационной безопасности, являющейся неотъемлемой частью национальной безопасности государства [Александрова, Червинчук, Резниченко 2024]. Современные тенденции цифровой трансформации, сопровождающиеся экспоненциальным ростом объемов обрабатываемых данных, увеличением числа онлайн-операций и активным развитием финансовых технологий, создают предпосылки для возникновения новых угроз и уязвимостей в информационной среде кредитных организаций [Бочкарева, Вороненко 2022]. В связи с этим актуализируется необходимость совершенствования механизмов контроля, мониторинга и аудита информационной безопасности в банковском секторе.

Одним из ключевых аспектов обеспечения надежности банковских и платежных систем является их регулярная проверка на предмет соответствия установленным требованиям информационной безопасности [Гильманова, Ахметшина 2022]. Однако анализ существующих подходов к аудиту информационной безопасности демонстрирует наличие ряда существенных проблем, включая несовершенство нормативно-правовой базы, отсутствие стандартизиро-

ванных методик проведения аудита, недостаточную квалификацию персонала, отвечающего за обеспечение защиты информационных ресурсов, а также слабую интеграцию результатов аудита в систему управленческих решений.

Настоящая научная работа направлена на исследование и разработку подходов к совершенствованию системы аудита информационной безопасности в кредитных организациях, что позволит повысить уровень защиты информационных активов банков и снизить риски, связанные с их эксплуатацией. В ходе исследования проводится комплексный анализ действующей системы регулирования информационной безопасности в банковском секторе, рассматриваются существующие практики проведения аудита и выявляются их основные недостатки. Особое внимание уделяется вопросам систематизации нормативных документов Банка России, регламентирующих проведение аудита, а также внедрению в штат аудиторских подразделений банков квалифицированных специалистов по информационной безопасности.

Методологическая основа исследования включает системный и сравнительный анализ, позволяющий выявить закономерности и тенденции в развитии механизмов аудита информационной безопасности. В качестве ключевых направлений совершенствования предложены рекомендации по унификации отчетности, формированию комплексного подхода к контролю за состоянием информационной безопасности, а также включению результатов аудиторских проверок в информационные ресурсы Банка России.

Практическая значимость проведенного исследования заключается в разработке рекомендаций, способствующих повышению эффективности аудита информационной безопасности в банковском секторе. Полученные результаты могут быть использованы как в процессе совершенствования нормативно-правовой базы в области информационной безопасности, так и при разработке внутренних регламентов кредитных организаций, что, в свою очередь, позволит минимизировать риски, связанные с утечками данных, кибератаками и несанкционированным доступом к финансовой информации.

Проблематика организационных и правовых аспектов в области аудита информационной безопасности в банковской сфере

Аудит информационной безопасности в кредитных организациях Российской Федерации играет ключевую роль в обеспечении надежной защиты финансовых и персональных данных, предот-

вращении угроз и соблюдении требований регуляторов. Современные вызовы в сфере информационной безопасности требуют системного подхода к организации аудита [Гришина 2022]. Однако действующая практика аудита информационной безопасности в банковском секторе сталкивается с рядом проблем, которые требуют детального анализа и проработки на нормативном и организационном уровнях[1].

Одной из наиболее актуальных проблем является отсутствие единого свода нормативных требований к проведению аудита информационной безопасности в кредитных организациях. В настоящее время банки руководствуются различными регламентирующими документами Банка России, в точности, совокупностью документов СТО БР ИББС. На текущий момент отсутствует детально проработанный унифицированный подход к аудиту информационной безопасности, это приводит к возникновению разночтений в ходе планирования и проведения аудиторских мероприятий. Более того, отсутствие систематизированных требований к проведению аудита информационной безопасности приводит к разночтениям в толковании нормативных положений, снижает эффективность аудиторской деятельности и ее отчетности.

Так, еще одной существенной проблемой в области аудита информационной безопасности в банковском секторе является недостаточная регламентация процесса ведения внутренней документации, сопровождающей подготовку и проведение аудиторских мероприятий. В настоящее время кредитные организации разрабатывают внутреннюю документацию в соответствии со своими корпоративными стандартами, что приводит к существенным различиям в структуре, объеме и содержании отчетных материалов. Отсутствие унифицированного подхода к формированию документации существенно усложняет процесс взаимодействия с регулирующими органами, поскольку каждая организация использует индивидуальные методологии, критерии оценки и формы представления информации. Это, в свою очередь, затрудняет проведение сравнительного анализа аудиторских проверок в разных финансовых учреждениях, снижает эффективность надзорной деятельности и делает невозможным формирование объективных отраслевых показателей информационной безопасности. Кроме того, отсутствие стандартизированных требований к ведению внутренней документации затрудняет обмен передовым опытом и

[1] *Сердюк В.Д.* Аудит информационной безопасности (ИБ) // «ИТ Аналитика». URL: https://bytemag.ru/aydiit-iinformaciionnoji-bezopasnostii-1089/ (дата обращения 03.03.2025).

внедрение передовых методик обеспечения информационной безопасности в банковском секторе.

Кроме того, особого внимания заслуживает организационный аспект проведения аудита информационной безопасности в кредитных организациях. Согласно Положению Банка России № 242–П от 16.12.2003 г.[2], функции внутреннего контроля в банковских структурах возлагаются на службу внутреннего аудита, а также на иные подразделения внутреннего контроля. Однако в современных условиях, характеризующихся высокой степенью угроз и усложнением нормативных требований, возникает необходимость во введении в штат аудиторских подразделений банков квалифицированного специалиста, ответственного за вопросы информационной безопасности. Отсутствие должного уровня компетенций у руководителя отдела внутреннего аудита информационной безопасности приводит к недостаточному анализу состояния защищенности информационных активов, некомпетентному подходу к проведению аудита в области информационной безопасности и, как следствие, к выявлению неполного перечня потенциальных угроз и уязвимостей.

Наконец, одной из ключевых проблем аудита информационной безопасности в банковском секторе остается недостаточная прозрачность результатов аудиторских проверок. В настоящее время на информационном ресурсе Банка России[3] публикуются данные по финансовой отчетности, однако информация о выходных характеристиках аудита информационной безопасности в этой системе отсутствует. Это создает ситуацию, при которой уровень информационной безопасности остается непрозрачным для клиентов, партнеров и национальных регуляторов. В результате заинтересованные стороны не могут объективно оценить надежность банков с точки зрения их устойчивости к информационным угрозам, что негативно сказывается на общем уровне доверия к финансовой системе. Закрытость информации о результатах аудита информационной безопасности также ограничивает возможности для анализа динамики угроз и эффективности применяемых мер защиты, что препятствует формированию комплексной стратегии повышения уровня информационной безопасности в банковском секторе [Кочаева, Йоллыев 2024].

---

[2] Положение Банка России № 242-П от 16.12.2003 // Информационно-правовой портал ГАРАНТ.РУ. URL: https://base.garant.ru/584330/ (дата обращения 10.03.2025).

[3] Информационный ресурс Банка России о результатах аудита отчетности кредитных организаций и банковских групп. URL: https://cbr.ru/statistics/audit_report/ (дата обращения 10.03.2025).

Выработка предложений по совершенствованию организационных и правовых аспектов в области аудита информационной безопасности в банковской сфере

Совершенствование системы аудита информационной безопасности в кредитных организациях требует комплексного подхода, включающего разработку унифицированного свода нормативных требований и методик их практического применения [Симакова 2024]. В связи с этим необходимо разработать и внедрить унифицированные требования к аудиту информационной безопасности в банковском секторе, которые позволят обеспечить единообразие аудиторских процедур, повысить уровень защиты информационных активов и снизить вероятность возникновения инцидентов, связанных с безопасностью. В табл. 1 представлены унифицированные и систематизированные аудиторские требования, изложенные в действующих нормативных актах Центрального Банка Российской Федерации. Именно эти сведения обеспечивают единообразие подходов к оценке соответствия кредитных организаций установленным нормативам в области информационной безопасности.

Введение обязательного свода единых требований, основанного на стандартах СТО БР ИББС и РС БР ИББС, создаст прозрачную систему контроля за состоянием информационной безопасности в кредитных организациях и повысит доверие к результатам аудита [Минаков, Эриашвили 2024]. Дополнительно следует внедрить механизм регулярного пересмотра и актуализации свода нормативных требований в соответствии с меняющимися угрозами и технологическими реалиями. Это может быть реализовано путем создания специализированной рабочей группы при Банке России, включающей представителей кредитных организаций, экспертов в области информационной безопасности и независимых аудиторов. Такой подход обеспечит своевременную адаптацию методик аудита к новым вызовам и угрозам, а также повысит общий уровень защищенности банковской системы.

Таблица 1

Систематизированные требования,
изложенные в действующих нормативных актах Банка России

№ п/п	Категория требований	Нормативное обоснование	Методика оценки	Формат отчетности	Требования к квалификации аудиторов
1	Общие требования к обеспечению ИБ	СТО БР ИББС-1.0-2014	Проверка соответствия организации базовым требованиям ИБ	Отчет с анализом выполнения обязательных и рекомендованных мер	Опыт работы в области ИБ, знание нормативных документов ИББС
2	Основные требования к аудиту ИБ	СТО БР ИББС-1.1-2007	Анализ подходов к аудиту, проверка методологий проведения аудиторских мероприятий	Унифицированный отчет с рекомендациями по устранению выявленных недостатков	Опыт в проведении аудита ИБ, сертификация CISA или аналогичные
3	Оценка соответствия требованиям ИБ	СТО БР ИББС-1.2-2014	Самооценка организации, аудит отчетности и проверка выполнения требований	Таблица соответствия требованиям с указанием выявленных несоответствий	Сертификация по стандартам ИБ (CISA, ISO 27001 Lead Auditor)
4	Сбор и анализ технических данных при расследовании инцидентов	СТО БР ИББС-1.3-2016	Проверка методов сбора и анализа технической информации при инцидентах	Раздел в отчете, содержащий описание инцидентов и технический анализ	Опыт работы в сфере компьютерной криминалистики, сертификация GIAC

Окончание табл. 1

№ п/п	Категория требований	Нормативное обоснование	Методика оценки	Формат отчетности	Требования к квалификации аудиторов
5	Управление рисками ИБ при аутсорсинге	СТО БР ИББС-1.4-2018	Анализ договоров с подрядчиками, проверка механизмов защиты данных	Раздел в отчете с оценкой рисков аутсорсинга и рекомендациями по их снижению	Опыт работы в области управления аутсорсингом, знание нормативных требований
6	Менеджмент инцидентов, связанных с информационными угрозами	СТО БР БФБО-1.5-2023	Проверка процессов выявления, регистрации и расследования инцидентов	Детализированный отчет по выявленным инцидентам и их анализу	Опыт работы в сфере управления инцидентами, сертификация GCFA
7	Документирование процессов ИБ	РС БР ИББС-2.0-2007	Анализ внутренней документации организации по ИБ	Перечень существующих документов с анализом их полноты	Опыт в разработке нормативных документов, знание ISO 27001
8	Руководство по самооценке соответствия ИБ	РС БР ИББС-2.1-2007	Анализ методик самооценки организации, проверка документации	Отчет с рекомендациями по улучшению процессов самооценки	Опыт проведения внутренних аудитов, сертификация CISA
9	Методика оценки рисков нарушения ИБ	РС БР ИББС-2.2-2009	Анализ и оценка угроз, потенциальных уязвимостей и последствий их реализации	Раздел в отчете, включающий перечень идентифицированных рисков и меры их снижения	Опыт управления рисками, наличие сертификации CRISC, ISO 27005

10	Менеджмент инцидентов ИБ	РС БР ИББС-2.5-2014	Проверка процесса управления инцидентами, анализ инцидентов прошлого периода	Отчет о выявленных проблемах и предложениях по оптимизации	Опыт работы с SIEM-системами, сертификация CISSP
11	Обеспечение ИБ на стадиях жизненного цикла АБС	РС БР ИББС-2.6-2014	Проверка мер безопасности при проектировании и эксплуатации АБС	Раздел в отчете, анализ уязвимостей, рекомендации по их устранению	Опыт работы в безопасной разработке ПО (DevSecOps, Secure SDLC)
12	Ресурсное обеспечение ИБ	РС БР ИББС-2.7-2015	Анализ кадрового, технического и финансового обеспечения ИБ	Отчет с оценкой текущего состояния ресурсного обеспечения	Опыт управления ресурсами ИБ, знание best practices в сфере ITSM
13	Обеспечение ИБ при использовании технологии виртуализации	РС БР ИББС-2.8-2015	Проверка механизмов защиты виртуализированных сред и облачных сервисов	Раздел в отчете, содержащий анализ рисков виртуализации и рекомендации	Знание технологий виртуализации (VMware, Hyper-V, KVM), сертификация VCP
14	Предотвращение утечек информации	РС БР ИББС-2.9-2016	Анализ политик контроля доступа, проверка работы DLP-систем	Отчет с оценкой угроз утечек и предложениями по их минимизации	Опыт работы с системами предотвращения утечек данных, знание нормативных требований

Для устранения проблемы недостаточной регламентации процесса ведения внутренней документации при подготовке и проведении аудита информационной безопасности в кредитных организациях Российской Федерации необходимо унифицировать требования, а также нормативно закрепить стандарты и внедрить централизованные методические рекомендации.

Прежде всего Банку России нужно разработать и утвердить единые требования к ведению внутренней документации, сопровождающей аудиторские мероприятия в сфере информационной безопасности. В целях стандартизации данный нормативный акт должен учитывать положения существующих отраслевых стандартов и других регламентов, обеспечивающих оценку защищенности информационных систем кредитных организаций.

В рамках унифицированного подхода к ведению внутренней документации должны быть детализированы следующие аспекты:

– структура и содержание отчетных материалов: определение обязательных элементов аудиторской документации, включая план аудита, протоколы промежуточных проверок, перечень выявленных уязвимостей, заключения по результатам аудиторских мероприятий и рекомендации по устранению недостатков. Внедрение стандартизированных форм и шаблонов отчетов, что позволит унифицировать представление данных, повысить их сопоставимость и упростить взаимодействие с регулирующими органами;
– методология ведения документации: определение четких критериев оценки соответствия информационной безопасности требованиям регулятора. Установление единого формата анализа рисков и выявленных инцидентов с классификацией угроз и уязвимостей в соответствии с положениями национальных регуляторов и международными стандартами. Регламентация требований к использованию автоматизированных систем ведения документации и хранения результатов аудиторских проверок в защищенных средах;
– правила взаимодействия с регуляторными органами: введение обязательной процедуры представления отчетности в Банк России в формате, обеспечивающем единообразие информации и возможность централизованного анализа состояния информационной безопасности в банковском секторе. Определение порядка корректировки и доработки документации по замечаниям регулирующих органов, а также регламентация процедуры согласования мер по устранению выявленных нарушений;

– подготовка кадров и ответственность за ведение документации: введение требований к квалификации специалистов, ответственных за ведение внутренней документации по аудиту информационной безопасности, с обязательной сертификацией по стандартам CISA, ISO 27001 Lead Auditor и аналогичным программам. Установление персональной ответственности руководителей подразделений информационной безопасности за достоверность предоставляемых данных и соблюдение требований к ведению документации.

Реализация предложенного подхода потребует издания соответствующего нормативного акта Банка России, закрепляющего единые требования к ведению внутренней документации в кредитных организациях. Кроме того, необходимо разработать методические рекомендации по внедрению новых стандартов и обеспечить их адаптацию с учетом специфики деятельности различных финансовых организаций.

Таким образом, введение единой системы ведения внутренней документации по аудиту информационной безопасности повысит прозрачность аудиторских процессов, упростит надзорную деятельность регулятора и обеспечит возможность объективного сравнительного анализа уровня информационной безопасности в кредитных организациях Российской Федерации.

Для повышения эффективности аудита информационной безопасности в кредитных организациях Российской Федерации критически важно наличие в структуре банковского внутреннего аудита квалифицированного специалиста, обладающего глубокими знаниями в области обеспечения информационной безопасности. Одним из ключевых решений данной проблемы является введение в штат кредитных организаций должности специализированного аудитора по вопросам информационной безопасности. Данный специалист должен выполнять функции координации и методологического обеспечения аудиторских мероприятий в сфере ИБ, а также обеспечивать непрерывный мониторинг и оценку соответствия действующим требованиям, установленным Банком России, международными стандартами и внутренними регламентами кредитной организации.

Главным и исполнительным лицом такого подразделения должен быть назначен обученный специалист-аудитор, обладающий соответствующей сертификацией и опытом работы в области управления информационной безопасностью и аудита. Данный сотрудник будет отвечать за разработку и реализацию методологии аудита информационной безопасности, а также за формирование системы внутреннего контроля и управления рисками, связанными с защитой информационных активов.

Кроме того, необходимо нормативное закрепление требований к квалификации и профессиональной подготовке специалистов, осуществляющих внутренний аудит в данной сфере. Для этого рекомендуется издание внутреннего положения о системе тренингов и программ повышения квалификации сотрудников аудиторских подразделений кредитных организаций.

Таким образом, внедрение должности специализированного аудитора по информационной безопасности, а также разработка системы постоянного обучения и сертификации персонала внутреннего аудита, позволит значительно повысить качество и глубину проводимых проверок, улучшить контроль за состоянием защищенности информационных систем кредитных организаций, а также повысить их соответствие требованиям регуляторов.

Для повышения прозрачности аудита информационной безопасности в банковском секторе необходимо внедрение механизма открытого опубликования результатов аудиторских проверок в рамках автоматизированной системы Банка России, обеспечивающей доступ к отчетности кредитных организаций и банковских групп. В настоящее время финансовая отчетность кредитных организаций представляется на данном ресурсе в соответствии с установленными нормативными требованиями, однако сведения о результатах аудита информационной безопасности отсутствуют, что существенно снижает уровень осведомленности клиентов, партнеров и регуляторов о состоянии защиты информационных активов банков.

Для решения данной проблемы необходимо разработать и внедрить специализированный модуль в автоматизированной системе отчетности Банка России, содержащий агрегированные данные по результатам аудита информационной безопасности кредитных организаций. Этот модуль должен обеспечивать публикацию ключевых групповых и частных показателей аудита, включающих степень соответствия требованиям СТО БР ИББС и иным нормативным актам Банка России, количество выявленных критических, высоких и средних уязвимостей, динамику устранения нарушений, а также общий индекс защищенности информационных активов, рассчитанный на основе унифицированных методик. Важным элементом такого модуля должно стать автоматизированное формирование обобщенной аналитики по отрасли, позволяющее регуляторам и участникам финансового рынка оценивать динамику изменений уровня информационной безопасности, выявлять наиболее распространенные угрозы и анализировать эффективность применяемых в банковской сфере защитных механизмов. Кроме того, информация о результатах аудита должна быть доступна

заинтересованным сторонам с учетом уровня их компетенций и потребностей. Государственные регуляторы и надзорные органы должны получать полный доступ к детализированным отчетам аудиторских проверок, кредитные организации должны иметь возможность анализировать собственные показатели в сравнении с отраслевыми средними значениями, а клиенты и партнеры банков должны иметь доступ к обобщенным данным об уровне защищенности конкретных финансовых учреждений без раскрытия конфиденциальной информации.

Дополнительно для обеспечения наглядного представления результатов аудита предлагается внедрение механизма визуализации данных в виде круговой диаграммы для каждого банка, прошедшего аудит информационной безопасности, что позволит отобразить уровень соответствия требованиям СТО БР ИББС-1.0-2014[4] по 34-м групповым показателям, установленным в приложении А СТО БР ИББС-1.2-2014[5]. Данный инструмент, интегрированный в информационный ресурс Банка России, обеспечит детализированное представление степени соблюдения нормативных требований каждой кредитной организацией, повысит прозрачность мониторинга информационной безопасности в банковской системе Российской Федерации и предоставит возможность для сравнительного анализа динамики изменений показателей в разрезе отдельных организаций и отрасли в целом. Пример оформления круговой диаграммы на ресурсе Банка России представлен на рис. 1.

Также необходимо внедрение механизма обязательного раскрытия информации о результатах аудита информационной безопасности в унифицированной форме, обеспечивающей сопоставимость данных между различными организациями. Введение стандартизированных отчетных форм позволит избежать разночтений при интерпретации данных и упростит процедуру анализа результатов аудита. Реализация данного подхода обеспечит повышение уровня доверия к банковской системе за счет увеличения прозрачности процессов аудита информационной безопасности [Резниченко, Сиротский 2021]. Внедрение механизма централизованного сбора и анализа данных о состоянии защищенности информационных активов банков позволит не только улучшить контроль

[4] Стандарт Банка России СТО БР ИББС-1.0-2014 от 17.05.2014 // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/70567254/ (дата обращения 12.03.2025).

[5] Стандарт Банка России СТО БР ИББС-1.2-2014 от 17.05.2014 // Информационно-правовой портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/70567284/ (дата обращения 12.03.2025).

за исполнением требований регуляторов, но и создать основу для совершенствования национальной стратегии кибербезопасности в финансовом секторе [Синявская, Синявский 2022].

Круговая диаграмма для отображения результатов оценивания

Заключение

Современное состояние системы аудита информационной безопасности в кредитных организациях Российской Федерации демонстрирует ряд проблем, связанных с фрагментарностью нормативно-правового регулирования, отсутствием единых методологических подходов, недостаточной квалификацией специалистов и низкой прозрачностью результатов аудиторских проверок. В условиях активного развития цифровых технологий и увеличения числа угроз эти недостатки снижают эффективность обеспечения защиты финансовых активов и персональных данных клиентов. Проведенное исследование позволило выявить ключевые направления совершенствования организационных и правовых аспектов аудита информационной безопасности, включающие унификацию нормативных требований, регламентацию внутренней документации, введение специализированной аудиторской позиции в банковских структурах и повышение

прозрачности отчетности. Введение единого свода требований к аудиту на основе стандартов Банка России создаст единообразную систему оценки защищенности кредитных организаций, что позволит повысить качество аудита и упростить контроль со стороны регуляторов. Более того, разработка и утверждение централизованных методических рекомендаций по ведению внутренней документации устранит существующие разночтения в отчетности и обеспечит сопоставимость данных между различными финансовыми институтами. Включение в штат банков квалифицированных аудиторов по информационной безопасности, обладающих соответствующей сертификацией и опытом, повысит уровень экспертизы при проведении проверок и позволит более эффективно выявлять уязвимости. Внедрение механизма публикации агрегированных данных о результатах аудита информационной безопасности на платформе Банка России повысит прозрачность деятельности кредитных организаций и обеспечит доступность информации для заинтересованных сторон, включая клиентов, партнеров и государственные органы. Таким образом, реализация предложенных мер будет способствовать формированию единого подхода к аудиту информационной безопасности, снижению рисков и повышению устойчивости финансовой системы Российской Федерации в условиях цифровой трансформации.

Литература

Александрова, Червинчук, Резниченко 2024 – *Александрова П.С., Червинчук А.С., Резниченко С.А.* Проверка соответствия банковской системы требованиям к защите информации в платежной системе // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 39–55.

Бочкарева, Вороненко 2022 – *Бочкарева Е.А., Вороненко Е.В.* Трансформация финансово-контрольных правоотношений в условиях цифровизации // Право и практика. 2022. № 1. С. 148–154.

Гильманова, Ахметшина 2022 – *Гильманова Э.А., Ахметшина Р.И.* Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры // Форум молодых ученых. 2022. № 2 (66). С. 29–31.

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Кочаева, Йоллыев 2024 – *Кочаева А.Р., Йоллыев А.Б.* Безопасность в банковской сфере: ключевые аспекты и роль кибербезопасности в эпоху цифровой экономики // Вестник науки. 2024. № 1 (70). С. 140–143.

Минаков, Эриашвили 2024 – *Минаков А.В., Эриашвили Н.Д.* Анализ рисков и безопасности системы электронных средств платежа // Образование. Наука. Научные кадры. 2024. № 1. С. 274–281.

Резниченко, Сиротский 2021 – *Резниченко С.А., Сиротский А.А.* Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий, 2021. № 2. С. 98–112.

Симакова 2024 – *Симакова В.С.* Современные технологии проведения аудита // Экономика и бизнес: теория и практика. 2024. № 2–2. С. 80–83.

Синявская, Синявский 2022 – *Синявская Е.Е., Синявский В.Д.* Цифровая трансформация банковского сектора // Транспортное дело России. 2022. № 2. С. 34–36.

References

Aleksandrova, P.S., Chervinchuk, A.S. and Reznichenko, S.A. (2024), “Checking the compliance of the banking system with the requirements for the protection of information in the payment system”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics”* Series, no. 3, pp. 39–55.

Bochkareva, E.A. and Voronenko, E.V. (2022), “Transformation of financial and control legal relations in the context of digitalization”, *Law and Practice*, no. 1, pp. 148–154.

Gil’manova, E.A. and Akhmetshina, R.I. (2022), “The role of information security audit in the life cycle of the information security system in critical information infrastructure facilities”, *Forum of young scientists*, no. 2 (66), pp. 29–31.

Grishina, N.V. (2022), “Analysis of the dynamics of personal data leakage in the context of the implementation of the program ‘Digital Economy of the Russian Federation’ ”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics”* Series, no. 4, pp. 34–43.

Kochaeva, A.R. and Iollyev, A.B. (2024), “Security in the banking sector. Key aspects and the role of cybersecurity in the era of the digital economy”, *Bulletin of Science*, no. 1 (70), pp. 140-143.

Minakov, A.V. and Eriashvili, N.D. (2024), “Risk and security analysis of the electronic payment system”, *Education. Science. Scientific staff*, vol. 1, pp. 274–281.

Reznichenko S.A. and Sirotskii A.A., (2021), “Formalized model of information security audit in organization on compliance with the requirements of the standards”, Safety of information technology, vol. 2, pp. 98–112.

Simakova, V.S. (2024), “Modern audit technologies”, *Economics and Business: theory and practice*, no. 2-2, pp. 80–83.

Sinyavskaya, E.E. and Sinyavskii, V.D. (2022), “Digital transformation of the banking sector”, *Transport business of Russia*, vol. 2, pp. 34–36.

Информация об авторах

Егор О. Павлов, студент, Финансовый университет при Правительстве РФ, Москва, Россия; 125993, Россия, Москва, Ленинградский пр-т, д. 49; epavlov466@gmail.com

Сергей А. Резниченко, кандидат технических наук, доцент, Финансовый университет при Правительстве РФ, Москва, Россия; 125993, Россия, Москва, Ленинградский пр-т, д. 49;

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия; 115409, Россия, Москва, Каширское ш., д. 31;

Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6, стр. 6; rsa_5@bk.ru

Information about the authors

Egor O. Pavlov, student, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49, Leningradskii Av., Moscow, 125993, Russia; epavlov466@gmail.com

Sergei A. Reznichenko, Cand. of Sci. (Computer Science), associate professor, Financial University under the Government of the Russian Federation, Moscow, Russia; bld. 49, Leningradskii Av., Moscow, 125993, Russia;

National Research Nuclear University *MEPhI*, Moscow, Russia; bld. 31, Kashirskoe Highway, Moscow, 115409, Russia;

Russian State University for the Humanities, Moscow, Russia; 6-6, Miusskaya Sq., Moscow, 125047, Russia; rsa_5@bk.ru

УДК 004
DOI: 10.28995/ 2686-679X-2025-3-54-69

Модель противодействия атакам претекстинга в социальных сетях на основе анализа структуры атаки социальной инженерии

Валерий К. Маркелов
Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия, v.a.l.e.m.a.r.k@yandex.ru

Александр Н. Привалов
Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия;
Тульский государственный педагогический университет им. Л.Н. Толстого, Тула, Россия, privalov.61@mail.ru

Аннотация. Доктрина информационной безопасности Российской Федерации относит компьютерное мошенничество к одной из ключевых киберугроз в цифровом пространстве. Социальные сети охватывают аудиторию численностью более 100 млн российских интернет-пользователей, тем самым являясь основным средством для общения россиян во Всемирной сети. Данный факт позволяет социальным сетям служить одной из наиболее привлекательных площадок для осуществления мошеннических действий, в том числе с применением атак социальной инженерии. Среди методов социальной инженерии, которые используются злоумышленниками, особое место занимает претекстинг.

Для противодействия социоинженерным атакам претекстинга в социальных сетях возникает необходимость создания моделей противодействия таким угрозам. Необходимость разработки такой модели обусловлена высоким уровнем популярности социальных сетей, ростом числа преступлений с использованием информационно-телекоммуникационных технологий, а также недостаточным количеством исследований, которые посвящены проблеме претекстинга в социальных сетях.

Цель статьи – описать авторскую модель противодействия социоинженерным атакам претекстинга в социальных сетях на базе типовой структуры атаки социальной инженерии и рассмотреть области ее применения в методике противодействия таким атакам. Модель, рассмотренная в статье, может использоваться для разработки методики противодействия социоинженерным атакам претекстинга в социальных сетях.

Ключевые слова: социальные сети, социальная инженерия, претекстинг, модель противодействия претекстингу, информационная безопасность

Для цитирования: Маркелов В.К., Привалов А.Н. Модель противодействия атакам претекстинга в социальных сетях на основе анализа структуры атаки социальной инженерии // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 54–69. DOI: 10.28995/ 2686-679X-2025-3-54-69

A model for countering pretexting attacks in social networks based on the analysis of the structure of social engineering attacks

Valerii K. Markelov
Ivanovo State University, Shuya branch,
Shuya, Ivanovo region, Russia, v.a.l.e.m.a.r.k@yandex.ru

Aleksandr N. Privalov
Ivanovo State University, Shuya branch,
Shuya, Ivanovo region, Russia;
Tula State Lev Tolstoy Pedagogical University,
Tula, Russia, privalov.61@mail.ru

Abstract. The Information Security Doctrine of the Russian Federation identifies computer fraud as a key cyber threat in the digital domain. With over 100 million Russian internet users actively engaged on social networks, these platforms have become the primary medium for online communication in the country. Social networks reach an audience of more than 100 million Russian internet users, thus becoming the main means of communication for Russians on the World Wide Web. It allows social networks to serve as one of the most attractive platforms for carrying out fraudulent activities, including using social engineering attacks. Among the social engineering methods used by attackers, pretexting stands out as a particularly prevalent.

To effectively mitigate pretexting-based social engineering attacks on social networks, there arises a need to create models for combatting such threats.

The urgency of this task stems from: the ubiquity of social media platforms, the rising incidence of cybercrimes leveraging information and communication technologies and the limited body of research focusing specifically on pretexting within social networking environments.

The article aims to describe the author's model for countering pretexting attacks in social networks, grounded in the typical structure of social engineering assaults and to consider fields of its potential applications within methodological frameworks for combating such threats. The proposed model serves as

a foundational tool for formulating targeted countermeasures against social engineering attacks of pretexting in social media contexts.

Keywords: social networks, social engineering, pretexting, model for countering pretexting, information security

For citation: Markelov, V.K. and Privalov, A.N. (2025), "A model for countering pretexting attacks in social networks based on the analysis of the structure of social engineering attacks", *RSUH/RGGU BULLETIN "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 54–69, DOI: 10.28995/ 2686-679X-2025-3-54-69

Введение

В соответствии с Доктриной информационной безопасности Российской Федерации, «одной из основных информационных угроз является возрастание масштабов компьютерной преступности»[1]. В частности, к таким преступлениям относится мошенничество в сети Интернет как одной из разновидностей мошенничества в сфере компьютерной информации.

«В сфере информационной безопасности в России особенное внимание в настоящее время уделяется сфере ответственности за нарушения, касающиеся защиты персональных данных» [Русецкая 2023, с. 72]. Одним из видов мошенничества является мошенничество в сфере компьютерной информации, «то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации (ст. 159.6 УК РФ)»[2]. Краткая характеристика состояния преступности в РФ за 2024 год показывает, что «40% преступлений были совершены с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 13,1% больше, чем в 2023 году, в том числе тяжких и особо тяжких составов – на 7,8%»[3].

---

[1] Указ Президента РФ № 646 от 05.12.2016 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Президент России. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 27.03.2025).

[2] Уголовный кодекс Российской Федерации // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (дата обращения 27.03.2025).

[3] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2024 г. // МВД России. URL: https://мвд.рф/reports/item/60248328/ (дата обращения 27.03. 2025).

В условиях цифровой трансформации общества социальные сети стали ключевым каналом коммуникации и информационного обмена в интернет-пространстве. Статистические данные аналитического отчета “Digital 2025: The Russian Federation” (март 2025) свидетельствуют о том, что «в Российской Федерации насчитывается 133 млн пользователей сети Интернет (92,2% населения страны), из которых 106 млн являются пользователями социальных сетей, что составляет 79,6% от всех российских пользователей (74,5% населения страны)»[4]. Широкое распространение социальных сетей не только привлекает большое количество людей, но и обусловливает их активную эксплуатацию злоумышленниками [Гришина 2022].

Обоснование необходимости разработки методики противодействия социоинженерным атакам с использованием претекстинга

Злоумышленники в социальных сетях активно применяют разнообразные социоинженерные методики для реализации мошеннических схем. «Социальная инженерия – это вид совершения компьютерных преступлений, направленный на несанкционированное получение информации путем использования слабых мест в психике человека» [Янгаева 2021, с. 135]. Также под социальной инженерией понимают «совокупность методов манипуляции действиями человека в целях получения необходимого доступа к информации» [Ломакин и др. 2021, с. 152].

Одним из таких методов является претекстинг. «Претекстинг – это метод социальной инженерии, при котором злоумышленник создает ложную историю или предлог для получения конфиденциальной информации от цели» [Самойлова 2019, с. 27]. Претекстинг в СА в основном используется в сочетании с другими методами, такими как фишинг (претексты с целью убедить жертву перейти на фишинговый сайт), байтинг (претексты с целью убедить жертву установить на свое устройство вредоносное программное обеспечение), вишинг (претексты с целью осуществления мошеннических действий посредством телефонных звонков через социальную сеть), что делает социоинженерные атаки претекстинга (САП) еще более опасными. Одна из основных особенностей претекстинга за-

[4] Digital 2025: The Russian Federation // DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2025-russian-federation (дата обращения 28.03.2025).

ключается в том, что он «требует от преступника тщательной подготовки к осуществлению личного контакта с жертвой, ему необходимы сведения о ее персональных данных, личном окружении, семье, потребительских предпочтениях и т. п.» [Зотина 2022, с. 96].

Проведенный анализ публикаций по проблемам противодействия САП в социальных сетях в авторской статье «Претекстинг в социальных сетях: актуальность проблемы и пути ее решения» показывает интерес ученых к соответствующим исследованиям, при этом «в последние годы наблюдается рост числа исследований, посвященных изучению претекстинга как метода социальной инженерии, однако количество исследований, посвященных проблеме претекстинга в социальных сетях, остается недостаточным» [Маркелов, Привалов, 2024, с. 82].

Таким образом, необходимость разработки методики противодействия САП обуславливают следующие факторы:

1) высокий уровень популярности социальных сетей, которые привлекают злоумышленников, использующих социальные сети в качестве площадки для совершения мошеннических действий;
2) рост числа преступлений с использованием информационно-телекоммуникационных технологий;
3) несмотря на увеличение исследований в области претекстинга как метода социальной инженерии в целом, специфика данного метода в социальных сетях остается малоисследованной областью в связи с недостаточным количеством исследований по соответствующей тематике.

Для противодействия САП в социальных сетях возникает необходимость создания моделей противодействия таким угрозам. Таким образом, цель статьи – описать авторскую модель противодействия социоинженерным атакам претекстинга (САП) в социальных сетях на базе типовой структуры социоинженерной атаки (СА) и рассмотреть области ее применения в методике противодействия таким атакам.

Анализ подходов к структуре социоинженерных атак в социальных сетях

Для описания модели противодействия САП рассмотрим различные подходы к структуре СА в социальных сетях.

В соответствии со структурой СА В.П. Шейнова, «выделяют следующие этапы атаки: формулирование цели воздействия на объект, сбор информации об объекте воздействия с использова-

нием различных источников информации, обнаружение наиболее удобных мишеней воздействия, аттракция, понуждение к нужному действию, нужный итог» [Халилаева и др. 2023, с. 55].

К.Д. Митник и В.Л. Саймон в своей книге «Искусство обмана» описывают следующую структуру СА: «исследование; создание взаимопонимания и доверия; эксплуатация доверия; применение информации» [Митник, Саймон 2004, с. 247].

Описание модели противодействия социоинженерным атакам претекстинга в социальных сетях на базе типовой структуры атаки социальной инженерии

На основе рассмотренных структур СА и анализа существующих подходов по противодействию СА была разработана модель противодействия СА в социальных сетях с использованием претекстинга на основе анализа структуры СА (рис. 1).

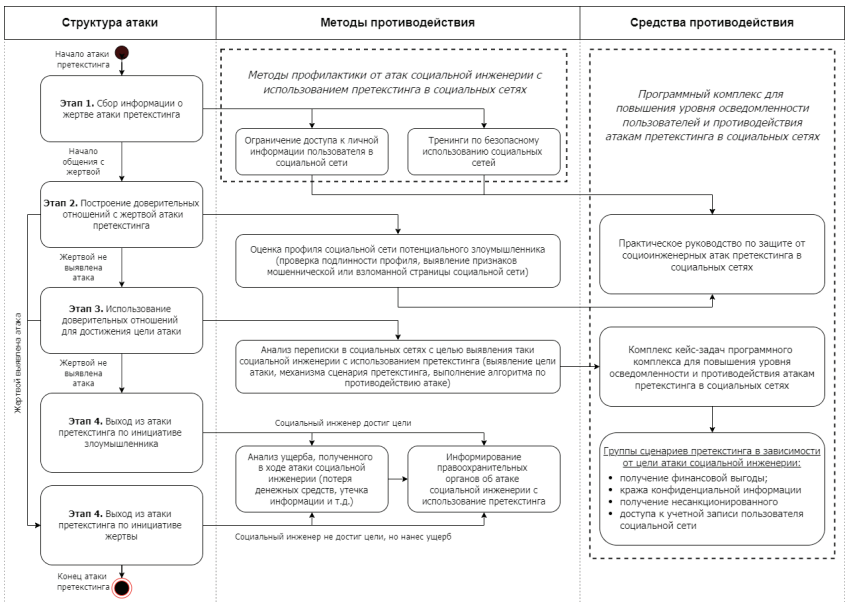


Рис. 1. Модель противодействия социоинженерным атакам претекстинга (САП) в социальных сетях

Рассмотрим модель противодействия САП в социальных сетях более подробно. Данная модель состоит из трех основных компонентов.

1. Структура САП, разработанная на основе структур атак социальной инженерии В.П. Шейнова, К.Д. Митника и В.Л. Саймона, включающая четыре основных этапа.

На начальном этапе социальный инженер тщательно изучает свою потенциальную жертву. Он анализирует публичную информацию в профиле пользователя социальной сети: фотографии, список друзей, группы, публикации и комментарии. Эти данные помогают ему составить психологический портрет человека, понять его интересы и слабые места, которые можно будет использовать в дальнейшем.

После сбора информации начинается этап построения отношений доверия. Социальный инженер инициирует контакт, подстраиваясь под интересы жертвы. Постепенно, используя собранные ранее сведения, он выстраивает доверительные отношения, которые становятся основой для атаки.

Когда доверие установлено, наступает этап использования доверительных отношений. Социальный инженер приводит в действие заранее подготовленный сценарий (претекст) для достижения своей цели атаки (получение финансовой выгоды, кража конфиденциальной информации, в том числе кража профиля социальной сети). Все его действия воспринимаются как достоверные благодаря тщательной подготовке на предыдущих этапах.

Завершающий этап (выход из атаки претекстинга) зависит от результата атаки. В случае успеха социальный инженер завершает общение с жертвой, минимизируя признаки манипуляции. При этом он может продолжить поддерживать видимость дружеских отношений с жертвой для возможных будущих манипуляций. Если жертва распознает обман, атака прекращается, но злоумышленник обычно уже успевает достичь части своих целей.

2. Методы противодействия САП в соответствии со структурой СА на каждом из ее этапов.

3. Средства противодействия САП. В частности, в качестве основного средства противодействия выступает программный комплекс «Безопасное общение в социальной сети» для повышения уровня осведомленности и противодействия САП в социальных сетях.

Первый этап САП в социальных сетях начинается со сбора информации о жертве СА для составления сценария (претекста). Для этого используется метод разведки OSINT, то есть «комплексная система поиска и анализа информации, доступной в открытом

доступе» [Мищиряков и др. 2024, с. 1415]. Поэтому с целью противодействия САП на данном этапе используются профилактические методы противодействия, затрудняющие злоумышленникам доступ к персональным данным пользователя социальной сети. К данным методам относятся:

– ограничение доступа к личной информации пользователя (закрытый профиль в социальной сети). Данный метод направлен на минимизацию объема данных, доступных потенциальным злоумышленникам, что затрудняет им сбор информации о жертве, необходимой для создания претекстов. Для этого пользователь может настроить параметры конфиденциальности в социальной сети, чтобы ограничить доступ к своей информации (ограничить видимость профиля (например, только для друзей), скрыть фотографии, публикации, поставить запрет на индексацию профиля социальной сети поисковыми системами). Также пользователь может удалить или скрыть информацию, которая не является необходимой для публичного доступа (место работы, адрес проживания, номер телефона, фотографии и публикации, содержащие личные данные), настроить доступ к своей информации только для доверенных лиц (например, для друзей или членов семьи), а также ограничить возможность других пользователей отмечать его на фотографиях или в публикациях. Возможности изменения параметров конфиденциальности напрямую зависят от наличия таких настроек в конкретной социальной сети;
– тренинги по безопасному использованию социальных сетей, направленные на снижение риска стать целью атаки претекстинга путем повышения уровня осведомленности пользователей и формирования навыков безопасного поведения. Задачами таких тренингов являются: развитие критического мышления для анализа «подозрительных» ситуаций общения; формирование навыков защиты личной и конфиденциальной информации; повышение осведомленности о правилах безопасного общения в социальной сети.

В качестве средства противодействия на первом этапе атаки претекстинга могут выступать практическое руководство по защите от САП в социальных сетях в рамках программного комплекса «Безопасное общение в социальной сети». В данном практическом руководстве раскрываются способы ограничения ограничение доступа к личной информации пользователя в популярных социальных сетях (ВКонтакте, Telegram), а также правила безопасного использования социальных сетей, направленные на снижение риска стать целью САП.

На втором этапе САП в социальных сетях злоумышленник начинает общение с жертвой с целью установления доверительных отношений. Для жертвы атаки на данном этапе наиболее важно выявить наличие САП, проводимой злоумышленником. С данной целью проводится оценка профиля потенциального злоумышленника:

1. Проверка даты создания профиля (новые профили могут быть подозрительными).

2. Анализ частоты и характера публикаций (отсутствие активности или шаблонные сообщения могут указывать на поддельный профиль).

3. Проверка фотографий (использование обратного поиска изображений для проверки, использование фотографий из других источников, размытые или стоковые изображения могут быть признаком поддельного профиля).

4. Анализ друзей (малое количество друзей в профиле социальной сети или отсутствие взаимных связей может указывать на поддельный профиль).

В качестве средства противодействия на втором этапе САП в социальных сетях могут использоваться практическое руководство программного комплекса «Безопасное общение в социальной сети», направленное на повышение уровня осведомленности и противодействия САП в социальных сетях, в котором раскрывается алгоритм оценки профиля социальной сети потенциального злоумышленника с целью выявления признаков мошеннической или взломанной страницы социальной сети.

На третьем этапе САП в социальных сетях злоумышленник использует доверительные отношения со своей жертвой для того, чтобы достичь цели САП (получение финансовой выгоды или кража конфиденциальной информации, в том числе кража профиля социальной сети жертвы). Для жертвы атаки на данном этапе важно не допустить достижения цели СА потенциальным злоумышленником и до окончания этапа выявить наличие САП. Для этого пользователи должны уметь распознавать признаки САП и принимать правильные решения по противодействию данной угрозе.

С этой целью проводится анализ переписки с потенциальным злоумышленником (анализ содержания сообщений, анализ контекста переписки, проверка подлинности собеседника с учетом оценки профиля социальной сети потенциального злоумышленника).

В качестве средства противодействия на третьем этапе САП может использоваться комплект кейс-задач программного комплекса, которые представляют собой ситуации сценариев САП в социаль-

ных сетях. Данные кейс-задачи способствуют повышению осведомленности пользователей об СА с использованием различных сценариев претекстинга, что позволяет пользователям анализировать переписку с потенциальным злоумышленником и выявлять претексты.

Каждая кейс-задача комплекта программного комплекса «Безопасное общение в социальной сети» включает в себя следующие элементы:

1) описание ситуации (пример переписки, имитирующей атаку претекстинга, например, сообщение от «друга» с просьбой перевести деньги);
2) вопросы для анализа ситуации сценария атаки претекстинга (Какие признаки указывают на атаку претекстинга? Как можно проверить подлинность профиля собеседника?);
3) выбор действия в рассматриваемой ситуации (проверка профиля собеседника; отказ от предоставления информации, требуемой собеседником; блокировка профиля собеседника и оповещение службы безопасности социальной сети о подозрительном профиле и т. д.).

В качестве примера рассмотрим общую структуру одной из кейс-задач программного комплекса «Безопасное общение в социальной сети».

Описание ситуации. Пользователь социальной сети ВКонтакте получает следующее сообщение от профиля, зарегистрированного под именем близкого друга. Сообщение имело следующее содержание:

Сообщение: «Привет! Это срочно! Я в больнице после ДТП, нужно срочно оплатить лечение. Моя карта заблокирована из-за подозрительных операций. Можешь перевести 25 000 рублей на карту Сбербанка 1234 **** **** 5678? Я все верну завтра, как только разберусь с банком. Не говори никому, мне очень стыдно за эту ситуацию».

Вопросы для анализа ситуации сценария атаки претекстинга.

1. Какие признаки указывают на атаку претекстинга?

- несоответствие активности (последний пост в профиле датирован 2 годами назад, тогда как реальный знакомый активно публикует новости (проверяется в ленте профиля);
- в списке друзей только 23 человека, тогда как у реального друга – более 400 друзей (проверяется в разделе «Друзья» профиля пользователя);
- признаки клонированного профиля (фотографии скопированы с основного профиля, но обрезаны по краям, что видно при увеличении);

- отсутствуют фотографии, опубликованные в последние 6 месяцев (проверяется в разделе «Фотографии» профиля пользователя);
- подозрительные метаданные (в разделе «О себе» профиля пользователя указан город, не совпадающий с местом жительства знакомого);
- дата регистрации профиля – менее месяца назад (проверяется при помощи сервисов для проверки даты регистрации профиля пользователя, например: https://regvk.com);
- особенности переписки (сообщение содержит требование конфиденциальности и сформулировано таким образом, чтобы оказать эмоциональное давление на собеседника, в сообщении предлагается конкретная сумма и реквизиты для перевода денежных средств).

2. Как можно проверить подлинность профиля собеседника?

- позвонить знакомому по номеру телефона, чтобы уточнить детали переписки (не используйте номер, который указан в профиле пользователя социальной сети, он может быть подменен на номер телефона злоумышленника);
- проверить наличие переписки с этим пользователем (отсутствие переписки может указывать на фальшивый профиль пользователя);
- посмотреть список общих друзей (в подозрительном профиле они будут отсутствовать);
- проверить, отображается ли профиль в поиске по основному номеру телефона знакомого.

3. Выбор действия в рассматриваемой ситуации:

- при подозрении на САП прекратить переписку с пользователем социальной сети;
- заблокировать подозрительный профиль;
- подать жалобу на пользователя социальной сети в поддержку ВКонтакте через официальную форму с жалобой на мошеннические действия;
- предупредить общих знакомых о возможной атаке претекстинга.

Данные кейс-задачи способствуют повышению осведомленности пользователей социальных сетей о САП в социальных сетях, развитию умения анализировать профиль потенциального злоумышленника на выявление признаков подлинной или мошеннической страницы, развивают умение анализировать переписку с потенциальным злоумышленником, а также формируют умение выбирать правильный алгоритм для противодействия сценариям претекстинга в социальных сетях.

На четвертом этапе, в случае выявления САП, жертва выходит из атаки по своей инициативе, в противном случае это происходит по инициативе злоумышленника. Если злоумышленником была достигнута цель атаки, злоумышленник старается «замести следы» проведенной атаки и оставить у своей жертвы ощущение, что она не подвергалась САП. На данном этапе проводится анализ ущерба, полученного в ходе проведения атаки (потеря денежных средств, утечка конфиденциальной информации, если они были переданы злоумышленнику до выявления атаки). При наличии ущерба от САП, связанного с потерей денежных средств, об этом информируются правоохранительные органы.

На основе рассмотренной модели противодействия САП в социальных сетях была построена функциональная модель в нотации IDEF0. На рис. 2 представлена контекстная диаграмма модели, а на рис. 3 – декомпозиция блока A0.

Рис. 2. Функциональная модель противодействия социоинженерным атакам претекстинга (САП) в социальных сетях в нотации IDEF0 (контекстная диаграмма)

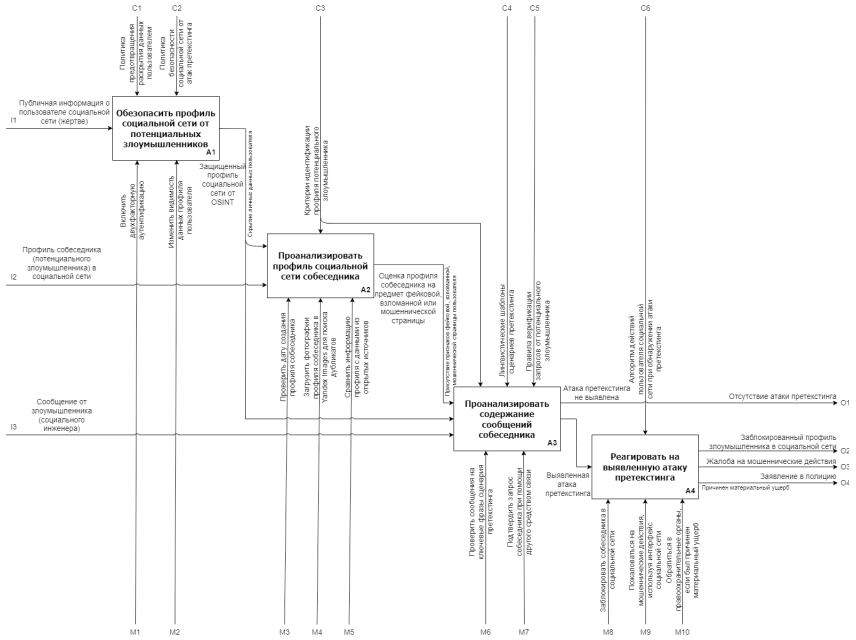


Рис. 3. Функциональная модель
противодействия социоинженерным атакам претекстинга (САП)
в социальных сетях в нотации IDEF0 (декомпозиция блока A0)

Таким образом, согласно функциональной модели противодействия САП в социальных сетях, с точки зрения пользователя социальной сети противодействие атаке претекстинга заключается в следующих шагах:

1) обеспечение защищенности профиля социальной сети;
2) анализ профиля социальной сети злоумышленника;
3) анализ содержания сообщения или группы сообщений злоумышленника, на основе которого формулируется вывод о том, является ли данный запрос на общение социоинженерной атакой претекстинга (САП);
4) реакция на выявленную атаку претекстинга.

Заключение

Рассмотренная модель противодействия социоинженерным атакам претекстинга (САП) в социальных сетях создает основу для разработки комплексной методики защиты пользователей от атак претекстинга. Перспективным направлением исследований в данной области является разработка программного комплекса для повышения уровня осведомленности и противодействия САП в социальных сетях, состоящего из следующих компонентов:

- практическое руководство по защите от САП в социальных сетях;
- комплекс кейс-задач, которые представляют собой ситуации сценариев САП в социальных сетях.

Данный программный комплекс может использоваться в качестве основного средства противодействия САП в социальных сетях.

Литература

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Зотина 2022 – *Зотина Е.В.* Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 4 (50). С. 93–99.

Ломакин и др. 2021 – *Ломакин А.Л., Хрусталев Е.Ю., Костюрин Г.А.* Социальная инженерия как угроза финансовой безопасности личности // Национальные интересы: приоритеты и безопасность. 2021. Т. 17, № 1 (394). С. 150–166.

Маркелов, Привалов 2024 – *Маркелов В.К., Привалов А.Н.* Претекстинг в социальных сетях: актуальность проблемы и пути ее решения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 71–86. DOI: 10.28995/2686-679X-2024-3-71-86.

Митник, Саймон 2004 – *Митник К.Д., Саймон В.Л.* Искусство обмана. М.: Компания АйТи, 2004. 359 с.

Мищиряков и др. 2024 – *Мищиряков И.В., Шевелев А.Д., Макарчук Д.В., Жданова М.М.* Исследование инструментов и методов для сбора и анализа открытой информации в сети интернет (OSINT) // Вестник науки. 2024. № 6 (75). С. 1414–1423.

Русецкая 2023 – *Русецкая И.А.* Комплаенс в области информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2023. № 2. С. 70–80.

Самойлова 2019 – *Самойлова А.А.* Методы социальной инженерии // Тенденции развития науки и образования. 2019. № 56-3. С. 25–28.

Халилаева и др. 2023 – *Халилаева Э.И., Маслова М.А., Герасимов В.М.* Система противодействия методам социальной инженерии в области информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2023. № 2 (48). С. 54–61.

Янгаева 2021 – *Янгаева М.О.* Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133–137.

References

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation'", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 34–43.

Khalilaeva, E.I., Maslova, M.A., Gerasimov, V.M. (2023), "System for counteracting social engineering methods in the field of information security", *Bulletin of the Ural Federal District. Security in the information sphere*, no. 2 (48), pp. 54–61.

Lomakin, A.L., Khrustalev, E.Yu. and Kostyurin, G.A. (2021), "Social engineering as a threat to the financial security of an individual", *National interests: priorities and security*, vol. 17, no. 1 (394), pp. 150–166.

Markelov, V.K. and Privalov, A.N. (2024), "Pretexting in social networks. Relevance of the issue and ways of its solution", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 3, pp. 71–86, DOI: 10.28995/2686-679X-2024-3-71-86.

Mitnik, K.D. and Simon, V.L. (2004), *Iskusstvo obmana* [The art of deception], IT Company, Moscow, Russia, 359 p.

Mishchiryakov, I.V., Shevelev, A.D., Makarchuk, D.V. and Zhdanova, M.M. (2024), "Research of tools and methods for collecting and analyzing open information on the Internet (OSINT)", *Science Bulletin*, no. 6 (75), pp. 1414–1423.

Rusetskaya, I.A. (2023), "Compliance in information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 70–80.

Samoilova, A.A. (2019), "Methods of social engineering", *Trends in the development of science and education*, no. 56-3, pp. 25-28.

Yangaeva, M.O. (2021), "Social engineering as a way to commit cybercrimes", *Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia*, no. 1 (42), pp. 133–137.

Zotina, E.V. (2022), "Pretexting as a social engineering technique used by telephone scammers. A criminological view of the issue", *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, vol. 13, no. 4 (50), p. 93–99.

Информация об авторах

Валерий К. Маркелов, аспирант, Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия; 155908, Россия, Ивановская область, Шуя, ул. Кооперативная, д. 24; v.a.l.e.m.a.r.k@yandex.ru

Александр Н. Привалов, доктор технических наук, профессор, Тульский государственный педагогический университет им. Л.Н. Толстого, Тула, Россия; 300026, Россия, Тула, пр-т Ленина, д. 125;

Ивановский государственный университет, Шуйский филиал, Шуя, Ивановская область, Россия; 155908, Россия, Ивановская область, Шуя, ул. Кооперативная, д. 24; privalov.61@mail.ru

Information about the authors

Valerii K. Markelov, postgraduate student, Ivanovo State University, Shuya branch, Shuya, Ivanovo region, Russia; 24, Kooperativnaya Str., Shuya, Ivanovo region, 155908, Russia; v.a.l.e.m.a.r.k@yandex.ru

Aleksandr N. Privalov, Dr. of Sci. (Mechanical Engineering), professor, Tula State Lev Tolstoy Pedagogical University, Tula, Russia; 125, Lenin Av., Tula, 300026, Russia;

Ivanovo State University, Shuya branch, Shuya, Ivanovo region, Russia; 24, Kooperativnaya Str., Shuya, Ivanovo region, 155908, Russia; privalov.61@mail.ru

УДК 51+533
DOI: 10.28995/ 2686-679X-2025-3-70-86

Математическая модель динамики вязкого газа в канале с волокнистым наполнителем

Дмитрий А. Тукмаков
Федеральный исследовательский центр «Казанский научный центр Российской академии наук», Казань, Россия, tukmakovda@imm.knc.ru

Аннотация. В работе представлена численная реализация математической модели течения газа в канале с волокнистым наполнителем. Динамика газа описывается двухмерным нестационарным уравнением Навье-Стокса. Математическая модель основана на континуальной методике моделирования динамики неоднородных сред – предполагалось, что для несущей и дисперсной фазы задаются объемные доли в общем объеме смеси. Объемное содержание дисперсной фазы является постоянной величиной. При моделировании динамики неоднородной среды для составляющих вектора скорости задавались однородные граничные условия Дирихле. Уравнения математической модели решались явным конечно-разностным методом Мак-Кормака второго порядка точности. Для подавление численных осцилляций применялась схема нелинейной коррекции сеточной функции. Исследована сеточная сходимость численной модели динамики газа в канале с волокнистым наполнителем. Проведено сопоставление результатов численных расчетов распространения ударной волны малой интенсивности в однородном газе и в неоднородных средах. В качестве неоднородных сред рассмотрены газовзвесь и канал, заполненный волокнистым наполнителем. Сопоставление демонстрирует, что при взаимодействии ударной волны малой интенсивности с газовзвесью скорость потока уменьшается, при этом взаимодействие потока газа с волокнистым наполнителем приводит к существенно большей потере кинетической энергии газа. Математическая модель динамики газа в волокнистом наполнителе может быть использована в расчетах подавления ударных волн.

Ключевые слова: математическая модель, численное моделирование, многофазные среды, газовзвеси, волокнистый наполнитель, межфазное взаимодействие, уравнение Навье-Стокса

Для цитирования: Тукмаков Д.А. Математическая модель динамики вязкого газа в канале с волокнистым наполнителем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 3. С. 70–86. DOI: 10.28995/ 2686-679X-2025-3-70-86

Mathematical model of viscous gas dynamics in a channel with fibrous filler

Dmitrii A. Tukmakov
Federal Research Center "Kazan Scientific Center of the Russian Academy of Sciences", Kazan, Russia, tukmakovda@imm.knc.ru

Abstract. The paper presents a numerical implementation of a mathematical model of gas flow in a channel with fibrous filler. Gas dynamics are described by a two-dimensional non-stationary Navier-Stokes equation. The mathematical model is based on the continuum technique of modeling the dynamics of inhomogeneous media – it was assumed that the volumetric fractions within the total volume of the mixture are specified for the carrier and dispersed phases. The volumetric content of the dispersed phase is a constant. When modeling the dynamics of an inhomogeneous medium, homogeneous Dirichlet boundary conditions were set for the velocity vector components. The equations of the mathematical model were solved by the explicit McCormack finite-difference method of the second order of accuracy. To suppress numerical oscillations, a nonlinear correction scheme of the grid function was used. The grid convergence of the numerical model of gas dynamics in a channel with a fibrous filler was investigated. The results of numerical calculations of the propagation of a low-intensity shock wave in a homogeneous gas and in inhomogeneous media were compared.

A gas suspension and a channel filled with a fibrous filler were considered as inhomogeneous media. The comparison demonstrates that when a low-intensity shock wave interacts with a gas suspension, the flow velocity decreases, while the interaction of the gas flow with the fibrous filler leads to a significantly greater loss of kinetic energy of the gas. The mathematical model of gas dynamics in a fibrous filler can be used in shock wave suppression calculations.

Keywords: mathematical model, numerical simulation, multiphase media, gas suspensions, fibrous filler, interphase interaction, Navier-Stokes equation

For citation: Tukmakov, D.A. (2025), "Mathematical model of viscous gas dynamics in a channel with fibrous filler", *RSUH/RGGU Bulletin. "Information Science. Information security. Mathematics" Series*, no. 3, pp. 70–86, DOI: 10.28995/ 2686-679X-2025-3-70-86

Введение

Одним из приложений математики является разработка математических моделей процессов механики жидкости и газа, интерес к таким исследованиям связан с различными практическими приложениями. В [Абдикаримов, Мансуров, Акбаров 2019] с помощью численного алгоритма решаются задачи аэроупругости – исследуются упругие колебания стержня (являющегося моделью крыла) в потоке газа с учетом нелинейных зависимостей изменения давления газа в процессе аэродинамического воздействия.

Отличием динамики неоднородных сред от классической гидро-газодинамики [Черный 1988; Овсянников 2003; Лоицянский 2003] является необходимость учитывать взаимодействие компонент в течениях смесей [Нигматулин 1978; Киселев, Руев, Трунев, Фомин, Шавалеев 1992; Кутушев 2003; Федоров, Фомин, Хмель 2015].

В [Фомин, Чен 2009] исследовалось воздействие термодинамических параметров дисперсных включений на подавление детонации. Недостаток методики математического моделирования, применяемой в работе, заключался в том, что пренебрегалось решением уравнений газовой динамики и решались только алгебраические уравнения химической физики. В [Тропин, Лаврук 2022] с помощью методологии гидродинамики многофазных сред исследовано взаимодействие детонационных волн в газодисперсных взвесях с облаком газокапельной взвеси. Математическая модель имеет одномерную геометрию и пренебрегает вязкостью. В [Huang, Zhang 2020] с помощью смешанного эйлерово-лагранжева подхода математически моделировалось воздействие ударных волн с газокапельной средой, с при учете испарения капельной дисперсной фазы. Математическая модель позволяла учесть взаимодействие газа и дисперсной фазы. Недостатком математической модели, примененной в работе, являлась одномерная геометрия течения.

В [Никитин, Тюренкова, Смирнова 2018] описана разработка физической концепции и реализующих ее математических моделей, позволяющих учесть эффект влияния многофазности горючего на условия зажигания и режимы распространения горения полидисперсных неоднородных смесей. Математические модели предполагались либо одномерными стационарными, либо нестационарными без учета пространственного изменения параметров математической модели. В [Матвиенко, Евтюшкин, Андропова 2015] представлены результаты развития траекторной концепции моделирования динамики неоднородных сред, предполагающей отсутствие взаимообратного взаимодействия компонент смеси –

уравнения динамики описывают только течение дисперсных частиц, гидродинамические поля несущей среды считаются заранее определенными. В статье предложены новые теоретические подходы разработки дифференциальных уравнений увлечения дисперсных частиц потоком несущей среды.

В обзоре литературы представлены публикации, посвященные исследованию ударноволновых процессов и течений в неоднородных средах. Исследования динамики неоднородных сред направлены, как правило, на изучение взаимодействия составных частей смеси, то есть частиц и газа.

Существует несколько методов математического моделирования динамики сложных гетерогенных течений. Траекторный подход [Матвиенко, Евтюшкин, Андропова 2015] не учитывает взаимодействие фаз смеси и поэтому не является физически достоверным для моделирования течений смесей с близкими массовыми долями компонентов. Равновесный метод математического моделирования динамики неоднородных сред [Нигматулин 1978] упрощает моделирование сложных течений за счет описания течений однородных газов и жидкостей с учетом коэффициентов дающих возможность учесть неоднородность течения. Однако такой подход не позволяет моделировать процессы, когда в расчетной области одновременно присутствуют участки с однородными и неоднородными средами, а также когда концентрация дисперсной фазы неодинакова. Математические модели течений неоднородных сред диффузионного типа [Нигматулин, 1978] применяются, как правило, в случае, когда компоненты смеси не отличаются агрегатным состоянием, поскольку не учитываются скоростную и температурную неравновесность компонент движущейся неоднородной среды. Учет взаимно обратных эффектов динамики смеси возможен с использованием метода континуального моделирования [Нигматулин 1978], который предполагает решение полной гидродинамической системы уравнений движения для каждого компонента. При этом системы уравнений движения компонентов смеси связаны функциями, описывающими взаимодействие компонент.

В данной работе на основе континуальной методики моделирования динамики неоднородных сред разработана математическая модель динамики газа в канале с волокнистым наполнителем. Модель предполагает расчет динамики газа с учетом сопротивления дисперсного каркаса и теплообмена между материалом дисперсного каркаса и движущемся газом.

Новизна работы заключается в том, что за счет модификации математической модели динамики газовзвесей, разработанной в рамках континуальной методики динамики неоднородных сред,

получена математическая модель, описывающая процесс течения газа в канале с волокнистым наполнителем.

Математическая модель

Для описания движения газовзвеси применяется континуальная математическая модель двухтемпературной двухскоростной смеси газа и дисперсных частиц, описанная в работах – [Тукмаков 2022; Тукмаков 2024a; Тукмаков 2024b; Тукмаков 2024c].

В континуальной методике моделирования динамики неоднородных сред изменение плотности несущей среды описывается с учетом изменения величины объемного содержания дисперсной фазы [Нигматулин 1978; Кутушев 2003; Федоров, Фомин, Хмель 2015], $\rho(t,x,y) = (1-\alpha(t,x,y))\rho_g(t,x,y)$, где $\rho_g(t,x,y)$ – функция плотности газа, $\alpha(t,x,y)$ – функция описывающая изменение объемного содержания частиц во времени и пространстве, определяемая из уравнений динамики дисперсной фазы. Таким образом уравнение неразрывности потока несущей среды имеет вид, аналогичный уравнению сохранения плотности сжимаемого газа [Черный 1988; Флетчер 1991; Лойцянский 2003; Овсянников 2003].

Математическая модель динамики газа в среде с волокнистым наполнителем описывается системой уравнений Навье-Стока, но имеет ряд отличий от системы уравнений динамики газовзвеси прежде всего за счет того, что объемное содержание дисперсной фазы постоянно $\alpha = \text{const}$ (1)–(3):

$$\frac{\partial \rho}{\partial t} + \frac{\partial (\rho u)}{\partial x} + \frac{\partial (\rho v)}{\partial y} = 0 \quad (1)$$

$$(1-\alpha)\left(\frac{\partial (\rho u)}{\partial t} + \frac{\partial (\rho u^2)}{\partial x} + \frac{\partial (\rho uv)}{\partial y} \right) + \frac{\partial (p - \tau_{xx})}{\partial x} - \frac{\partial (\tau_{xy})}{\partial y} = -F_{xfm} + \alpha \frac{\partial p}{\partial x} \quad (2)$$

$$(1-\alpha)\left(\frac{\partial (\rho v)}{\partial t} + \frac{\partial (\rho uv)}{\partial x} + \frac{\partial (\rho v^2)}{\partial y} \right) - \frac{\partial (\tau_{xy})}{\partial x} + \frac{\partial (p - \tau_{yy})}{\partial y} = -F_{yfm} + \alpha \frac{\partial p}{\partial y} \quad (3)$$

Вязкость газа определялась выражениями [Флетчер 1991]:

$$\tau_{xx} = \mu\left(2\frac{\partial u}{\partial x} - \frac{2}{3} D \right), \tau_{yy} = \mu\left(2\frac{\partial v}{\partial y} - \frac{2}{3} D \right), \tau_{xy} = \mu\left(\frac{\partial u}{\partial y} + \frac{\partial v}{\partial x} \right), D = \frac{\partial u}{\partial x} + \frac{\partial v}{\partial y}.$$

В систему уравнений динамики несущей среды входит уравнение сохранения энергии для динамики вязкого газа в канале с волокнистым наполнителем (4) и уравнение передачи тепла от газа к дисперсной фазе (5):

$$\frac{\partial(e)}{\partial t}+\frac{\partial\left(\left(e+p-\tau_{xx}\right)u-\tau_{xy}v+\lambda\,\partial T/\partial x\right)}{\partial}+\frac{\partial\left(\left(e+p-\tau_{yy}\right)v-\tau_{xy}u+\lambda\,\partial T/\partial x\right)}{\partial}=$$
$$=-\frac{6\alpha\lambda Nu_{fm}\left(T-T_1\right)}{d^2}-u\left|F_{xfm}\right|-v\left|F_{yfm}\right|+\alpha\frac{\partial p}{\partial x}+\alpha\frac{\partial p}{\partial y} \qquad (4)$$

$$\frac{\partial T_1}{\partial t}=\frac{6\lambda Nu_{fm}\left(T-T_1\right)}{\rho_{10}d^2C_{p1}}. \qquad (5)$$

Составляющие вектора межкомпонентного обмена импульсом для среды с волокнистым наполнителем составляют соответственно F_{xfm},F_{yfm}:

$$F_{xfm}=\frac{3\alpha}{4d}C_d\,\rho u\sqrt{u^2+v^2},F_{yfm}=\frac{3\alpha}{4d}C_d\,\rho v\sqrt{u^2+v^2}.$$

Здесь p, ρ, u, v – давление, плотность, декартовы составляющие скорости несущей среды в направлении осей x и y соответственно; T, e – температура и полная энергия газа; μ, λ – вязкость и теплопроводность газа. Температура газа – $T=(\gamma\text{-}1)\,(e/\rho\text{-}0.5(u^2+v^2)/R$, где R – газовая постоянная, давление газа $p=(\gamma\text{-}1)(e\text{-}0.5\rho(u^2+v^2))$. В уравнении (5) C_{p1} – удельная теплоемкость единицы массы вещества дисперсной фазы, Nu_{fm} – относительно число Нуссельта волокнистой среды, d – толщина нити волокна, ρ_{10} – плотность материала волокнистой среды. Используются следующие обозначения:

$$Re_1=\rho\left|\mathbf{V}-\mathbf{V}_1\right|d/\mu,Nu_1=2exp\left(-M_1\right)+0.459\,Re_1^{0.55}\,Pr^{0.33},M_1=\left|\mathbf{V}-\mathbf{V}_1\right|/c,Pr=C_p\mu\lambda^{-1},$$
$$M=\left|\mathbf{V}\right|/c,\;Re_{1fm}=\rho\left|\mathbf{V}\right|d/\mu,Nu_{fm}=2exp\left(-M\right)+0.459\,Re_1^{0.55}\,Pr^{0.33}.$$

Системы уравнений (1)–(5) интегрировались одной из разновидностей метода конечных разностей. Алгоритм численного метода рассмотрим на уравнении (6):

$$\frac{\partial f}{\partial t}+\frac{\partial a(f)}{\partial x}+\frac{\partial a(f)}{\partial y}=c(f) \qquad (6)$$

Явный конечно-разностный метод Мак-Кормака [Флетчер 1991] для скалярного нелинейного уравнения (6) имеет вид (7)–(8):

$$f^{*}_{j,k} = f^{n}_{j,k} - \frac{\Delta t}{\Delta x}\left(a^{n}_{j+1,k} - a^{n}_{j,k}\right) - \frac{\Delta t}{\Delta y}\left(b^{n}_{j,k+1} - b^{n}_{j,k}\right) + \Delta t c^{n}_{j,k} \quad (7)$$

$$f^{n+1}_{j,k} = 0.5\left(f^{n}_{j,k} + f^{*}_{j,k}\right) - 0.5\frac{\Delta t}{\Delta x}\left(a^{*}_{j,k} - a^{*}_{j-1,k}\right) - 0.5\frac{\Delta t}{\Delta y}\left(b^{*}_{j,k} - b^{*}_{j,k-1}\right) + 0.5\Delta t c^{*}_{j,k} \quad (8)$$

Здесь Δx, Δy – шаги по пространственному направлению, Δt – шаг по времени.

В расчетах применялась схема расщепления по пространственным переменным (9), состоящая из одномерных операторов – P_x, P_y, позволяющая построить решение на следующем временном слое [Ковеня, Тарнавский, Черный 1990]:

$$f^{n+1}_{j,k} = \mathbf{P}_x\left(\frac{\Delta t_x}{2}\right)\mathbf{P}_y\left(\frac{\Delta t_y}{2}\right)\mathbf{P}_y\left(\frac{\Delta t_y}{2}\right)\mathbf{P}_x\left(\frac{\Delta t_x}{2}\right)f^{n}_{j,k} \quad (9)$$

Временные шаги $Dt_x = Dt_y = Dt$. Переход со слоя t^n на слой t^{n+1} осуществляется следующим образом:

$$f^{(1)}_{j,k} = \mathbf{P}_x\left(\frac{\Delta t_x}{2}\right)f^{n}_{j,k}\ ,\ f^{(2)}_{j,k} = \mathbf{P}_y\left(\frac{\Delta t_y}{2}\right)f^{(1)}_{j,k}\ ,\ f^{(3)}_{j,k} = \mathbf{P}_y\left(\frac{\Delta t_y}{2}\right)f^{(2)}_{j,k}\ ,\ f^{n+1}_{j,k} = \mathbf{P}_x\left(\frac{\Delta t_x}{2}\right)f^{(3)}_{j,k}$$

Численные осцилляции подавлялись схемой нелинейной коррекции [Музафаров, Утюжников 1993; Тукмаков 2006].

Программный комплекс, реализующий численный алгоритм решения уравнений математической модели, состоит из нескольких подпрограмм: формирования граничных условий, построения сетки, подпрограмма описывающая взаимодействие компонент смеси, а также основная программа численного решения уравнений динамики неоднородной среды.

Результаты расчетов

Плотность частиц в газовзвеси или волокнистого наполнителя – $\rho_{10} = 2500$ кг/м^3, диаметр частиц или толщина волокон волокнистой среды – $d = 2$ мкм, начальное объемное содержание дисперсной фазы газовзвеси и волокнистой среды – $\alpha_0 = 0.001$. Длина канала – $L = 1$ м, ширина канала – $h = 0.1$ м. Сеточное разбиение области – $N_x = 200$ в направлении x и $N_y = 40$ в направлении y. Моделировалась работа так называемой «ударной трубы» [Черный 1988; Овсянников 2003; Лойцянский 2003; Кутушев 2003]. В области равновесного давления расположена неоднородная среда, тогда

как область повышенного давления заполнена однородным газом – рис. 1. Дисперсная фаза – либо газовзвесь (взвешенные в газе твердые частицы), либо волокна твердого материала. Повешенное давление газа составляет – p_2 = 123,2 кПа, тогда как равновесное давление газа – p_1 = 112 кПа. Компоненты смеси имеют начальную температуру – $T_0 = T_{10}$ =293 К. Начальная средняя плотность дисперсной компоненты: $\rho_1(x,y) = \alpha_0\rho_{10}$, $x > L/4$; $\rho_1(x,y) = 0$, $x \le L/4$.

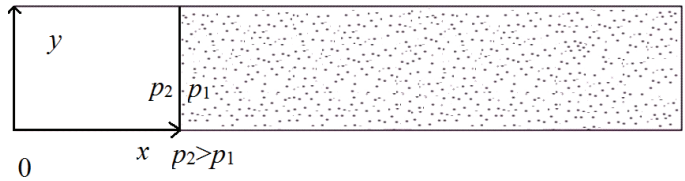


Рис. 1. Общая схема моделируемого процесса

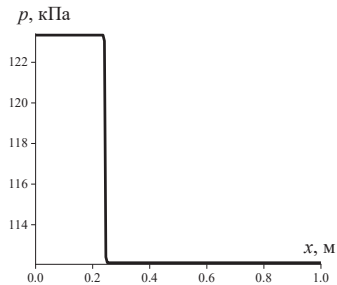


Рис. 2. Начальное распределение давления

На рис. 2 представлено распределение давления газа в продольном направлении в начальный момент времени, интенсивность начального перепада давления – p_2/p_1 = 1.1. В последующие моменты времени распад начального разрыва давления газа формирует одиночную ударную волну малой интенсивности.

Математическая модель, основанная на решении уравнения Навье-Стокса [Лойцянский 2003], позволяет учесть пристеночную вязкость в канале при движении несущей среды газовзвеси – рис. 3.

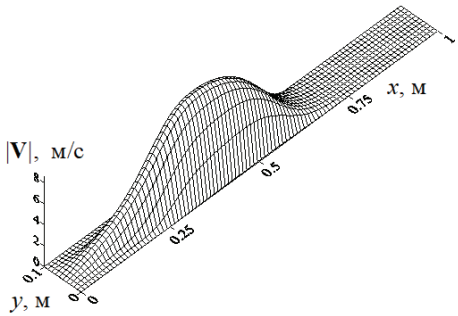
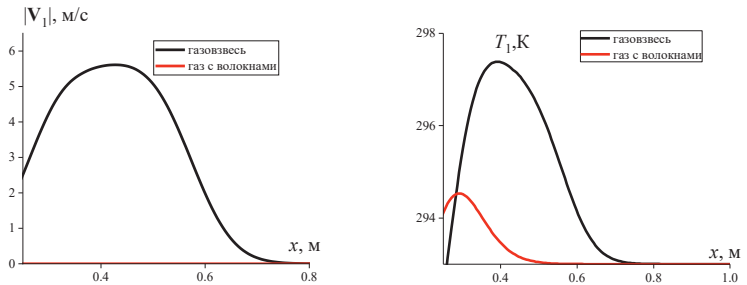


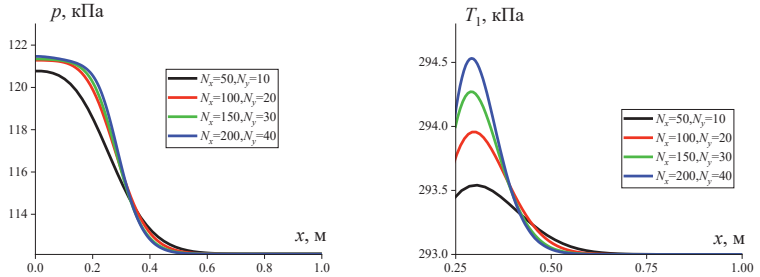
Рис. 3. Модуль скорости несущей среды газовзвеси



а *б*

Рис. 4. Пространственное распределение
модуля скорости рис. 4а и температуры – рис. 4б дисперсной фазы
для различных моделей неоднородных сред в продольном направлении

Особенностью математической модели газа с волокнами является то, что дисперсная компонента смеси неподвижна – рис. 4а. В модели газа с волокнами учитывается теплообмен между несущей средой и дисперсной фазой, в процессе движения ударной волны вдоль направления распространения ударной волны происходит изменение температуры волокнистой среды, при этом за счет отсутствия конвективных слагаемых в уравнении (13) интенсивность изменения температуры имеет меньшее значение, чем в газовзвеси – рис. 4б.



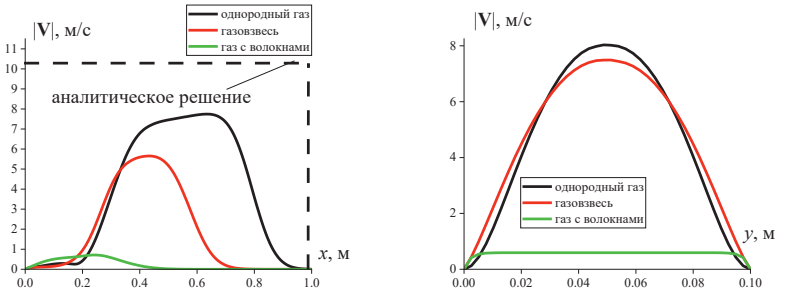
а *б*

Рис. 5. Пространственное распределение давления несущей среды – рис. 5а и температуры дисперсной фазы – рис. 5б дисперсной фазы, полученные расчетами в рамках модели газа с волокнами на последовательности конечно-разностных разбиений расчетной области

Исследование сеточной сходимости математической модели динамики газовзвеси (1)–(8), разработанной в рамках континуальной методики моделирования течений неоднородных сред, представлено в работе [Tukmakov 2024]. Для исследования сеточной сходимости модели динамики газа с волокнами были проведены численные расчеты на вложенной последовательности конечно-разностных разбиений физической области. Было определено, что при измельчении конечно-разностной сетки уменьшаются различия между рассчитанными параметрами динамики газа и дисперсной компоненты, в частности давления газа и температуры дисперсной фазы – рис. 5 а, б. Так, для конечно-разностных разбиений $\{N_x = 50, N_y = 10\}, \{N_x = 100, N_y = 20\}, \{N_x = 150, N_y = 30\}, \{N_x = 200, N_y = 40\}$ максимальные значения температуры дисперсной фазы в момент времени $t = 1.7$ мс составляют соответственно $T_{1max} = 293.5$ К, $T_{1max} = 293.95$ К, $T_{1max} = 293.25$ К, $T_{1max} = 294.5$ К.

Численные расчеты модуля скорости демонстрируют, что скорость несущей среды в подвижной газовзвеси и в газе с волокнистым наполнителем меньше, чем в однородном газе, при это численные решения имеют меньшие значения, чем аналитическое решение для одномерной линеаризованной модели течения невязкого газа [Лойцянский 2003] – рис. 6а. Как для однородного газа, так и для несущей среды газовзвеси профиль течения является параболическим, что согласуется из известными из литературы результатами моделирования течений вязких сред в каналах [Лойцянский 2003],

профиль течения газа с волокнами отличается от параболического профиля – рис. 6б. Максимальное значение модуля скорости несущей среды газовзвеси составляет 72% от максимального значения модуля скорости однородного вязкого газа, в газе с волокнами максимальное значение модуля скорости составляет 9% от максимального значения модуля скорости в однородном вязком газе.



а *б*

Рис. 6. Пространственное распределение модуля скорости для однородной среды и различных моделей неоднородных сред в продольном направлении ($y = h/2$) – рис. 6а, в поперечном сечении ($x = 0.3L$) – рис. 6б

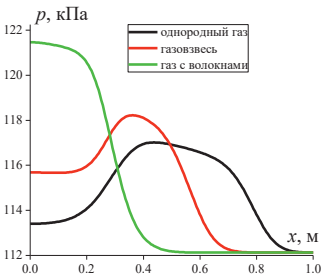


Рис. 7. Пространственное распределение давления газа для однородной среды и различных моделей неоднородных сред, $y = 0.5h$.

При распространении ударной волны по газовзвеси скорость движения ударной волны имеет меньшее значение, чем при движении ударной волны по однородному газу, в расчетах по модели ди-

намики газа с волокнами скорость распространения ударной волны меньше, чем при взаимодействии ударной волны с газовзвесью – рис. 7. Закономерность можно объяснить тем, что при замедлении течения несущей среды происходит переход кинетической энергии газа в потенциальную энергию.

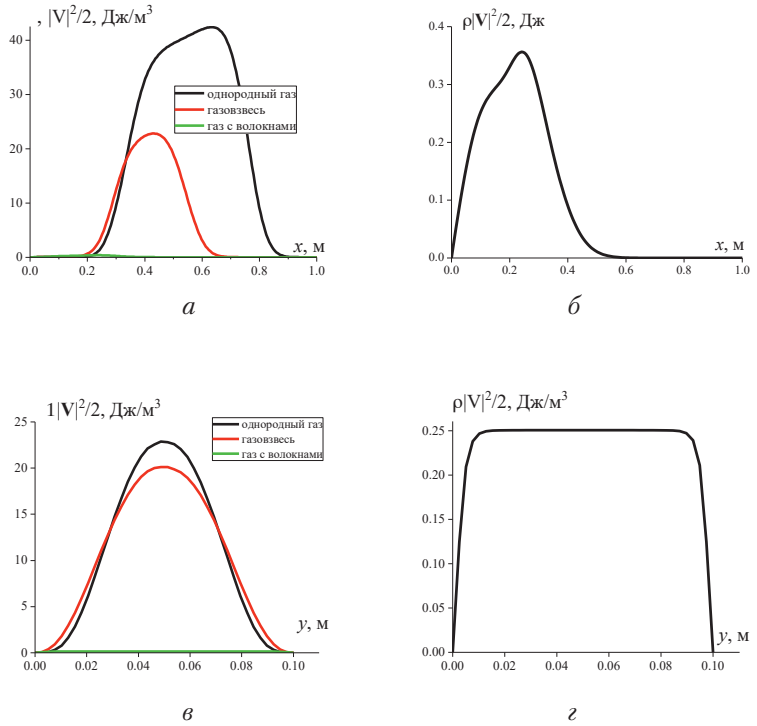


Рис. 8. Пространственное распределение кинетической энергии газа для однородной среды и различных моделей неоднородных сред в продольном ($y = h/2$) – рис. 8 а, б, поперечном ($x = 0.3L$) – рис. 8 в, г направлениях

Продольные и поперечные распределения кинетической энергии несущей среды газовзвеси демонстрируют, что в модели газа с волокнами кинетическая энергия существенно меньше, чем в континуальной модели динамики газовзвеси или в однородном газе – рис. 8 (а-г). Таким образом в случае течения газа в канале с волокнами за счет межфазного взаимодействия кинетическая

энергия несущей среды уменьшается примерно на два порядка относительно результатов расчетов для однородного газа. Поперечное распределение кинетической энергии газа для однородной среды и для газовзвеси согласуется с параболическим профилем, в то время как для модели течения газа в канале с волокнами для поперечного распределения кинетической энергии несущей среды наблюдается плоский профиль.

Выводы

В работе представлена математическая модель гидродинамики неоднородных сред. На основе континуальной методики моделирования неоднородных течений разработана математическая модель динамики газа в канале с волокнистым наполнителем. Подобного рода течения существенно отличаются не только от течений однородных газов в трубах и каналах, но и от неоднородных потоков с подвижной дисперсной фазой– течений запыленных и газокапельных сред и требуют разработки отдельного типа математических моделей. При этом разработанная в статье математическая модель применима к широкому классу течений неоднородных сред, в которых возможно пренебречь изменениями объемного содержания дисперсной фазы. Представленная математическая модель, несмотря на то, что реализуют континуальную методику динамики неоднородных сред, позволяет существенно снизить количество уравнений в частных производных, описывающих течение неоднородной среды. Полученные в работе результаты могут быть применены при разработке математических моделей технологий снижения интенсивности ударноволновых течений в трубах и каналах.

Благодарности

Работа выполнена при поддержке гранта Академии наук Республики Татарстан, предоставленного молодым кандидатам наук (постдокторантам) в рамках Государственной программы Республики Татарстан «Научно-технологическое развитие Республики Татарстан» (Соглашение № 84/2024-ПД от 16 декабря 2024 года).

Acknowledgements

The work was carried out with the support of a grant from the Academy of Sciences of the Republic of Tatarstan, provided to young candidates of science

(postdoctoral researchers) within the framework of the State Program of the Republic of Tatarstan “Scientific and Technological Development of the Republic of Tatarstan” (Agreement No. 84/2024-PD dated December 16, 2024).

Литература

Абдикаримов, Мансуров, Акбаров 2019 – *Абдикаримов Р.А., Мансуров М.М., Акбаров У.Й.* Численное исследование флаттера вязкоупругого жестко-защемленного стержня с учетом физической и аэродинамической нелинейностей // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2019. № 3. С. 94–107.

Киселев, Руев, Трунев, Фомин, Шавалеев 1992 – *Киселев С.П., Руев Г.А., Трунев А.П., Фомин В.М., Шавалеев М.Ш.* Ударно-волновые процессы в двухкомпонентлых и двухфазных средах. Новосибирск: Наука, 1992. 261 с.

Ковеня, Тарнавский, Черный 1990 – *Ковеня В.М., Тарнавский Г.А., Черный С.Г.* Применение метода расщепления в задачах аэродинамики. Новосибирск: Наука, 1990. 247 с.

Кутушев 2003 – *Кутушев А.Г.* Математическое моделирование волновых процессов в аэродисперсных и порошкообразных средах. СПб.: Недра, 2003. 284 с.

Лоицянский 2003 – *Лоицянский Л.Г.* Механика жидкости и газа. М.: Дрофа, 2003. 784 с.

Матвиенко, Евтюшкин, Андропова 2015 – *Матвиенко О.В., Евтюшкин Е.В., Андропова А.О.* Исследование применимости модели дрейфа частиц для моделирования переноса дисперсной фазы в потоке // Вестник Томского государственного университета. Математика и механика. 2015. № 5 (37). С. 76–83.

Музафаров, Утюжников 1993 – *Музафаров И.Ф., Утюжников С.В.* Применение компактных разностных схем к исследованию нестационарных течений сжимаемого газа. Математическое моделирование. 1993. Т. 5. № 3. С. 74–83.

Нигматулин 1978 – *Нигматулин Р.И.* Основы механики гетерогенных сред. М.: Наука, 1978. 336 с.

Никитин, Тюренкова, Смирнова 2018 – *Никитин В.Ф., Тюренкова В.В., Смирнова М.Н.* Разработка вычислительных комплексов предсказательного моделирования процессов горения многофракционных топлив в потоках окислителя // Вестник кибернетики. 2018. Т. 32. № 4. С. 38–51.

Овсянников 2003 – *Овсянников Л.В.* Лекции по основам газовой динамики. М.: Институт компьютерных исследований, 2003. 336 с.

Тропин, Лаврук 2022 – *Тропин Д.А., Лаврук С.А.* Физико-математическое моделирование ослабления гомогенных и гетерогенных детонационных волн облаками капель воды // Физика горения и взрыва. 2022. Т. 58. № 3. С. 80–90.

Тукмаков 2006 – *Тукмаков А.Л.* Численное моделирование акустических течений при резонансных колебаниях газа в закрытой трубе // Известия высших учебных заведений. Авиационная техника. 2006. № 4. С. 33–36.

Тукмаков 2022 – *Тукмаков Д.А.* Сопоставление численных моделей динамики электрически заряженных газовзвесей с массовой и поверхностной плотностями зарядов для различных дисперсностей частиц // Вестник МГТУ им. Н.Э. Баумана. Серия «Естественные науки». 2022. № 3. С. 43–56.

Тукмаков 2024a – *Тукмаков Д.А.* Численное исследование влияния граничных условий на расчеты динамики полидисперсной газовзвеси // Прикладная математика и механика. 2024. Т. 88. № 3. С. 422–433.

Тукмаков 2024b – *Тукмаков Д.А.* Исследование влияния граничных условий на динамику газовзвеси с вязкой несущей средой в канале // Вестник Воронежского государственного университета. Серия «Системный анализ и информационные технологии». 2024. № 2. С. 58–70.

Тукмаков 2024c – *Тукмаков А.Л., Тукмаков Д.А.* Численное исследование влияния коагуляции на динамику двухфракционной газовзвеси // Вестник ЮУрГУ. Серия «Математическое моделирование и программирование». 2024. Т. 17. № 4. С. 66–81.

Федоров, Фомин, Хмель 2015 – *Федоров А.В., Фомин В.М., Хмель Т.А.* Волновые процессы в газовзвесях частиц металлов. Новосибирск: Параллель, 2015. 301 с.

Флетчер 1991 – *Флетчер К.* Вычислительные методы в динамике жидкостей. Т. 2. М.: Мир, 1991. 552 с.

Фомин, Чен 2009 – *Фомин П.А., Чен Д.Р.* Влияние химически инертных частиц на параметры и подавление детонации в газах // Физика горения и взрыва. 2009. Т. 45. № 3. С. 77–88.

Черный 1988 – *Черный Г.Г.* Газовая динамика. М.: Наука, 1988. 424 с.

Huang, Zhang 2020 – *Huang Z., Zhang H.* On the interactions between a propagating shock wave and evaporating water droplets // Physics of Fluids. 2020. Vol. 32. No. 12.

Tukmakov 2024 – *Tukmakov D.A.* Investigation of the grid convergence of a finite-difference model of the dynamics of an electrically charged gas suspension // 2024 6th International Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russia, 29 February 2024 – 02 March 2024. New York, NY: IEEE, 2024. DOI: https://doi.org/10.1109/REEPE60449.2024.10479689.

References

Abdikarimov, R.A., Mansurov, M.M. and Akbarov, U.Yu. (2019), “Numerical study of flutter of a viscoelastic rigidly clamped rod taking into account physical and aerodynamic nonlinearities”, *RSUH/RGGU Bulletin. “Information Science. Information security. Mathematics” Series*. no. 3, pp. 94–107.

Chernyi, G.G. (1988), *Gazovaya dinamika*. [Gas dynamics], Nauka, Moscow, Russia, 424 p.

Fedorov, A.V., Fomin, V.M. and Khmel, T.A. (2015), *Volnovye processy v gazovzvesyakh chastits metallov* [Wave processes in gas suspensions of metal particles], Parallel, Novosibirsk, Russia, 2015, 301 p.

Fletcher, K. (1991), *Vychislitel'nye metody v dinamike zhidkostei* [Computational Methods in Fluid Dynamics], vol. 2, Mir, Moscow, Russia, 552 p.

Fomin, P.A. and Chen, J.R. (2009), "Effect of chemically inert particles on parameters and suppression of detonation in gases", *Combustion, Explosion, and Shock Waves*, vol. 45, no. (3), pp. 303–313.

Huang, Z. and Zhang, H. (2020), "On the interactions between a propagating shock wave and evaporating water droplets', *Physics of Fluids*, vol. 32, no. 12.

Kiselev, S.P., Ruev, G.A., Trunev, A.P., Fomin, V.M. and Shavaleev, M.Sh. (1992), *Udarno-volnovye processy v dvukhkomponentlykh i dvukhfaznykh sredakh* [Shock-wave processes in two-component and two-phase media], Nauka, Novosibirsk, Russia, 261 p.

Kovenya, V.M. Tarnavskii, G.A. and Chernyi, S.G. (1990), *Primenenie metoda rasshepleniya v zadachakh aerodinamiki* [Application of the splitting method in problems of aerodynamics], Nauka, Novosibirsk, Russia, 247 p.

Kutyshev, A.G. (2003), *Matematicheskoe modelirovanie volnovykh processov v aerodispersnykh i poroshkoobraznykh sredakh* [Mathematical modeling of wave processes in aerodispersed and powdery media], Nedra, St. Petersburg, Russia, 284 p.

Loitsyanskii, L.G. (2003), *Mekhanika zhidkosti i gaza* [Mechanics of liquid and gas], Drofa, Moscow, Russia, 784 p.

Matvienko, O.V., Evtyushkin, E.V. and Andropova, A.O. (2015), "Study of applicability of particle drift model for modeling dispersed phase transfer in flow", *Vestn. Tomsk. Gos. Univ. Mat. Mekh.*, no. 5, pp. 76–83.

Muzafarov, I.F. and Utyuzhnikov, S.V. (1993), "Application of compact difference schemes to study of unsteady flows of compressible gas", *Mathematical modeling*, vol. 5, no. 3, pp. 74–83.

Nigmatulin, R.I. (1978), *Osnovy mekhaniki geterogennykh sred* [Fundamentals of mechanics of heterogeneous media], Nauka, Moscow, Russia, 336 p.

Nikitin, V.F., Tyurenkova, V.V. and Smirnova, M.N. (2018), "Development of computing systems for predictive modeling of combustion processes of multi-fraction fuels in oxidizer flows", *Bulletin of Cybernetics*, vol. 32, no. 4, pp. 38–51.

Ovsyannikov, L.V. (2003), *Lektsii po osnovam gazovoi dinamiki* [Lectures on the fundamentals of gas dynamics], Institut komp'yuternykh issledovanii, Moscow, Russia, 336 p.

Tropin, D.A. and Lavruk, S.A. (2022), "Physicomathematical modeling of attenuation of homogeneous and heterogeneous detonation waves by clouds of water droplets", *Combustion, Explosion, and Shock Waves*, vol. 58, no. 3, pp. 327–336.

Tukmakov, A.L. (2006), "Numerical modeling of acoustic flows with resonant oscillations of gas in a closed pipe", *Bulletin of higher educational institutions. Aviation engineering*, no. 4, pp. 33–36.

Tukmakov, D.A. (2022), "Comparison of numerical models of the dynamics of electrically charged gas suspensions with mass and surface charge densities for different particle dispersions", *Bulletin of Bauman Moscow State Technical University. Series: Natural Sciences*, no. 3, pp. 43–56.

Tukmakov, D.A. (2024), “Numerical study of the influence of boundary conditions on the calculations of the dynamics of a polydisperse gas suspension”, *Applied Mathematics and Mechanics*, vol. 88, no. 3, pp. 422–433.

Tukmakov, D.A. (2024), “Study of the influence of boundary conditions on the dynamics of a gas suspension with a viscous carrier medium in a channel”, *Bulletin of the Voronezh State University. Series: System analysis and information technology*, no. 2, pp. 58–70.

Tukmakov, A.L. and Tukmakov, D.A. (2024), “Numerical study of the influence of coagulation on the dynamics of a two-fraction gas suspension”, *Bulletin of SUSU. Series: Mathematical modeling and programming*, vol. 17, no. 4, pp. 66–81.

Tukmakov, D.A. (2024), “Investigation of the grid convergence of a finite-difference model of the dynamics of an electrically charged gas suspension”, *2024 6th International Conference on Radio Electronics, Electrical and Power Engineering (REEPE)*, Moscow, Russia, 29 February 2024 – 02 March 2024, IEEE, New York, NY, DOI: https://doi.org/10.1109/REEPE60449.2024.10479689.

Информация об авторе

Дмитрий А. Тукмаков, кандидат физико-математических наук, Федеральный исследовательский центр «Казанский научный центр Российской академии наук», Казань, Россия; 420111, Россия, Казань, ул. Лобачевского, д. 2; tukmakovda@imm.knc.ru

Information about the author

Dmitrii A. Tukmakov, Cand. of Sci. (Physics and Mathematics), Federal Research Center “Kazan Scientific Center of the Russian Academy of Sciences”, Kazan, Russia; 2, Lobachevsky St., Kazan, 420111, Russia; tukmakovda@imm.knc.ru

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 3
2025

Дизайн обложки
Е.В. Амосова

Корректор
Ж.П. Григорьева

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, г. Москва, вн. тер. г. муниципальный округ Тверской,
Миусская пл., д. 6, стр. 6

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

Подписано в печать 25.08.2025
Выход в свет 29.08.2025
Формат 60×90 1/16
Уч.-изд. л. 5,0. Усл. печ. л. 5,5
Тираж 1050 экз. Свободная цена
Заказ № 2224

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