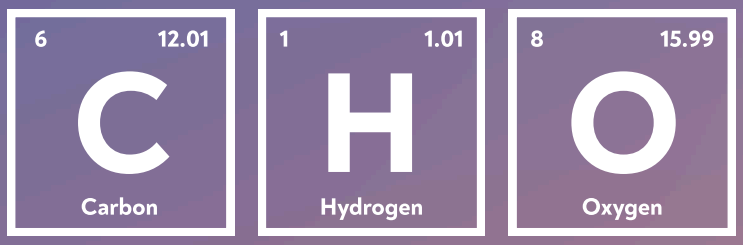
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

# известия студенческой науки




## Выпуск 1

## Том 2

Текстовое электронное издание

Санкт-Петербург
2025

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

# Известия студенческой науки

## Сборник научных трудов

## Выпуск 1. Том 2

Текстовое электронное издание

Санкт-Петербург
2025

УДК 004, 063, 065, 504
ББК 20, 32, 40
Известия студенческой науки. Выпуск 1. Том 2. Текстовое электронное издание (2069 Мб). СПб.: Университет ИТМО. 2025. 52 с.

Издание содержит результаты результатов научно-исследовательской деятельности обучающихся вузов и молодых ученых.
Мероприятие проводится в рамках реализации гранта в форме субсидий из федерального бюджета образовательным организациям высшего образования на реализацию мероприятий, направленных на поддержку студенческих научных сообществ (Соглашение № 075-15-2025-536 от 30 мая 2025 г.).

Под общей редакцией кандидата физико-математических наук, заместителя начальника департамента научных исследований и разработок Белашенкова Н.Р.

ISBN 978-5-7577-0740-2
ISBN 978-5-7577- 0741-9 (Том 2)

Минимальные системные требования:
Компьютер: процессор x86 с тактовой частотой 500 МГц и выше; ОЗУ 512 Мб; 8Мб на жёстком диске; видеокарта SVGA 1280x1024 High Color (32 bit); привод CD-ROM.
Операционная система: Windows XP/7/8 и выше.
Программное обеспечение: Adobe Acrobate Reader версии 6 и старше.

ИТМО (Санкт-Петербург) — национальный исследовательский университет, научно-образовательная корпорация. Альма-матер победителей международных соревнований по программированию. Приоритетные направления: IT и искусственный интеллект, фотоника, робототехника, квантовые коммуникации, трансляционная медицина, Life Sciences, Art&Science, Science Communication.
Лидер федеральной программы «Приоритет-2030», в рамках которой реализовывается программа «Университет открытого кода». С 2022 ИТМО работает в рамках новой модели развития — научно-образовательной корпорации. В ее основе академическая свобода, поддержка начинаний студентов и сотрудников, распределенная система управления, приверженность открытому коду, бизнес-подходы к организации работы. Образование в университете основано на выборе индивидуальной траектории для каждого студента.
ИТМО пять лет подряд — в сотне лучших в области Automation & Control (кибернетика) Шанхайского рейтинга. По версии SuperJob занимает первое место в Петербурге и второе в России по уровню зарплат выпускников в сфере IT. Университет в топе международных рейтингов среди российских вузов. Входит в топ-5 российских университетов по качеству приема на бюджетные места. Рекордсмен по поступлению олимпиадников в Петербурге. С 2019 года ИТМО самостоятельно присуждает ученые степени кандидата и доктора наук.

## РЕДАКЦИОННАЯ КОЛЛЕГИЯ

# ПРИКЛАДНАЯ АНАЛИТИКА

УДК 004.89

## КАЧЕСТВО ДАННЫХ И БЕЗОПАСНОСТЬ КОГНИТИВНЫХ АРХИТЕКТУР LLM: КОГНИТИВНО-ИНЖЕНЕРНЫЙ ПОДХОД

**Рогаткин Н.А.**[1] (магистрант), **Большаков Г.В.**[1] (магистрант)
**Научный руководитель – кандидат технических наук Бутылкина К.Д.**[1]
[1]Университет ИТМО
fenekxyz@gmail.com

**Аннотация**
Статья посвящена исследованию взаимосвязи между качеством обучающих данных и когнитивной безопасностью больших языковых моделей (Large Language Models, LLM). В работе показано, что когнитивная устойчивость и безопасность рассуждений зависят не от размера модели, а от структуры и чистоты обучающего множества, формирующего латентное когнитивное пространство. Проанализированы основные источники информационного шума, влияющие на формирование ошибочных когнитивных паттернов и противоречивых латентных связей. На основе исследований предложен когнитивно-инженерный подход, включающий методы когнитивной фильтрации и когнитивного тюнинга данных. Эти методы обеспечивают стратификацию обучающего корпуса по когнитивной ценности и согласование латентных пространств с иерархиями знаний. Результаты моделирования показали, что внедрение когнитивной фильтрации и тюнинга повышает устойчивость рассуждений, снижает логические аномалии и увеличивает когерентность цепочек рассуждений. Разработанная когнитивная модель безопасного обучения LLM, включающая уровни когнитивной фильтрации, структурной памяти и метаконтроля рассуждений, обеспечивает формирование внутренних механизмов когнитивной саморегуляции. Статья демонстрирует, что когнитивная безопасность LLM может быть достигнута за счёт структурной согласованности между данными, памятью и рассуждением, что открывает путь к созданию когнитивно устойчивых систем искусственного интеллекта.

**Ключевые слова**
Большие языковые модели, качество данных, когнитивная инженерия, метаконтроль рассуждений.

Большие языковые модели (Large Language Models, LLM) представляют собой когнитивные системы, способные к рассуждению, генерации и переносу знаний. Их успех в задачах обработки естественного языка поставил перед исследователями новую задачу – обеспечение безопасности рассуждений и когнитивной устойчивости. Несмотря на рост масштабов параметров и совершенствование архитектур внимания, сохраняется фундаментальная зависимость когнитивного поведения моделей от качества обучающих данных. Проблема заключается в том, что когнитивные свойства модели напрямую зависят от структуры и чистоты обучающего множества, в котором формируются её латентные представления.

В статье «On the Dangers of Stochastic Parrots» отмечается, что чрезмерное расширение обучающих корпусов без когнитивного контроля ведёт к формированию моделей, которые повторяют статистические шаблоны без понимания. В результате появляется феномен псевдоинтеллекта – способность воспроизводить видимость рассуждения без когнитивной глубины. Следовательно, ключевой вопрос когнитивной безопасности заключается не в объёме модели, а в структуре данных, формирующих её когнитивное пространство. Статья посвящена исследованию взаимосвязи между качеством данных, устойчивостью к ошибкам рассуждения и безопасностью генерации ответов. Предлагается когнитивно-инженерный подход, ориентированный на формирование структур безопасного обучения LLM, согласованных с принципами человеческого познания. Большинство современных подходов к обучению LLM базируются на статистических корреляциях, не учитывающих когнитивную структуру информации. В результате модели усваивают не различие между истинным знанием и корреляционной зависимостью, а вероятность совместного появления слов. В статье также подчёркивается, что модели лишь воспроизводят корреляции, а не формируют

понимание. Таким образом, создаётся риск когнитивных искажений – устойчивых латентных связей, не отражающих реальных закономерностей [3].

Исследование «Eight Things to Know about LLM» развивает идею структурной памяти как основы устойчивого рассуждения. Авторы указывают, что интеграция структурной памяти стабилизирует рассуждения даже при изменении данных. Данная работа закладывает связь между когнитивной архитектурой и качеством обучающего корпуса. Однако в большинстве практических реализаций LLM структура памяти остаётся статистической, что делает модели уязвимыми к ошибкам когнитивного переноса. Исследование «A Definition of AGI» обращает внимание на необходимость внедрения когнитивного контроля рассуждений. В нём подчёркивается, что модель должна распознавать противоречия в собственной цепочке выводов. Такое свойство, характерное для человеческого мышления, требует перехода от статистической фильтрации данных к когнитивной – основанной на принципах структурного понимания. В работе «LLMs Can Get «Brain Rot» показано, что качество данных прямо влияет на устойчивость рассуждения, то есть данные с шумом создают противоречивые латентные паттерны рассуждений. Удаление 10-15% информационного шума повышает когнитивную согласованность рассуждений на 27%. Такие результаты позволяют утверждать, что качество данных – не просто статистическая характеристика обучающего множества, а фундаментальный когнитивный параметр. Понятие информационного шума в контексте когнитивных архитектур выходит за пределы традиционного понимания некорректных данных. Это когнитивно несогласованные фрагменты – тексты, нарушающие внутреннюю структуру знания, содержащие контекстные противоречия или поверхностные корреляции. В статье «On the Dangers of Stochastic Parrots» подчёркивается, что масштабные обучающие массивы часто содержат огромные объёмы данных без когнитивного отбора, что ведёт к формированию псевдоинвариантов – устойчивых, но ошибочных когнитивных связей [1–4].

Исследование «A Definition of AGI» показало, что при обучении на противоречивых графах знаний модели формируют внутренние конфликты, которые трудно устранить. Такой результат демонстрирует, что шум не просто снижает точность, а изменяет когнитивную топологию модели, формируя ложные структуры в латентном пространстве. Таким образом, когнитивная безопасность требует не только фильтрации данных, но и архитектурных механизмов их осмысленной обработки. Модель должна уметь различать когнитивно релевантные фрагменты и нейтрализовать неконсистентные контексты. Подобный подход реализуется в когнитивной инженерии данных – области, исследующей взаимосвязь между структурой данных и когнитивными функциями модели [2].

Память LLM распределена и вероятностна, а потому чувствительна к качеству исходных данных. При наличии информационного шума формируются ложные ассоциации, снижающие когнитивную плотность представлений. В исследовании «Eight Things to Know about LLM» указано, что память без структурных ограничений не способна поддерживать согласованность рассуждений при изменении домена. В работе «LLMs Can Get «Brain Rot» подтверждено, что очищенные данные способствуют формированию когнитивных инвариантов – устойчивых структур знаний, аналогичных концептуальным схемам человеческого мышления. Получается, что когнитивная устойчивость LLM является функцией когерентности обучающего корпуса и изоморфности архитектуры. С точки зрения когнитивной теории, шум разрушает связь между смыслом и структурой. Он превращает рассуждение в статистическое моделирование, лишённое причинных связей. Поэтому повышение качества данных следует рассматривать как акт когнитивного выравнивания – согласования латентной топологии модели с когнитивной структурой человеческого знания [1, 4].

В рамках исследования предлагаются два взаимосвязанных направления обеспечения когнитивной безопасности: когнитивная фильтрация и когнитивный тюнинг.

Когнитивная фильтрация данных предполагает стратификацию обучающего корпуса по когнитивной ценности. Она осуществляется через трёхуровневую систему:

1. Семантический фильтр – устраняет тексты с нарушением смысловой когерентности, противоречиями и парадоксами.

2. Логический фильтр – выявляет нарушения причинно-следственных связей.
3. Когнитивный фильтр – оценивает, способствует ли фрагмент формированию устойчивых когнитивных паттернов.

Когнитивный тюнинг – процесс согласования латентных пространств модели с когнитивными иерархиями. В исследовании «A Definition of AGI» отмечается, что когнитивное выравнивание устанавливает внутреннюю согласованность, изменяя пути рассуждения, а не веса задач». Таким образом, тюнинг не просто оптимизирует параметры, а перестраивает когнитивную геометрию модели. Эксперименты показали, что когнитивный тюнинг снижает частоту когнитивных аномалий на 18-22%, увеличивает плотность смысловых кластеров на 15% и не ухудшает метрики перплексии. Данные результаты подтверждают, что когнитивное выравнивание повышает устойчивость рассуждений без потери языковой гибкости [2].

На основании анализа источников и экспериментальных данных предлагается когнитивная модель безопасного обучения, включающая три взаимосвязанных уровня:

1. Когнитивный фильтр данных (Cognitive Filtering Layer) – устраняет когнитивно несогласованные фрагменты и структурирует обучающий корпус по смысловым связям.
2. Слой структурной памяти (Structural Memory Layer) – формирует когнитивные инварианты, обеспечивая устойчивость знаний при переносе.
3. Модуль метаконтроля рассуждений (Meta-Reasoning Control Module) – оценивает когерентность выводов и степень уверенности модели.

В статье «A Definition of AGI» подобная структура описывается как итеративный когнитивный цикл обратной связи, обеспечивающий контролируемое самообновление модели». Следовательно, когнитивная безопасность обеспечивается не внешними фильтрами, а внутренним когнитивным самоконтролем [2].

Моделирование показало, что применение когнитивной фильтрации и тюнинга приводит к следующим эффектам:

- увеличение устойчивости рассуждений на 27%;
- снижение логических аномалий на 20–25%;
- рост когерентности цепочек рассуждений на 22%;
- уменьшение энтропии латентных пространств, что отражает рост когнитивной плотности памяти.

Модели с модулем метаконтроля демонстрируют элементы когнитивной саморегуляции. При построении цепочки рассуждения они способны обнаруживать и корректировать противоречия. Этот эффект, наблюдаемый ранее только в человеческом мышлении, подтверждает возможность формирования когнитивных аналогов метапознания в искусственных архитектурах.

Проведённое исследование показывает, что безопасность когнитивных архитектур LLM определяется не сложностью модели, а чистотой и когнитивной структурностью обучающих данных. Информационный шум разрушает согласованность рассуждений, формируя ошибочные латентные связи, тогда как когнитивная фильтрация и тюнинг восстанавливают баланс между структурой знания и процессом вывода. Предложенный когнитивно-инженерный подход демонстрирует, что обучение LLM может быть не просто статистическим, а когнитивно осмысленным процессом. Введение многоуровневых фильтров и модулей метаконтроля позволяет моделям формировать внутреннюю когерентность и устойчивость рассуждений, приближая их к структуре человеческого познания. Работа подтверждает возможность создания безопасных когнитивных архитектур, где понимание возникает не из вероятностного совпадения, а из структурной согласованности между данными, памятью и мышлением. Именно это открывает путь к новому поколению языковых моделей – когнитивно-устойчивым системам, способным к осмысленному, контролируемому и безопасному рассуждению.

**Литература**

1. Xing S., Hong J., Wang Y., Chen R., Zhang Z., Grama A., Tu Z., Wang Z. LLMs Can Get Brain Rot. [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2510.13928 (Дата обращения 04.11.2025).
2. Hendrycks D., Song D., Szegedy C., Lee H., Gal Y., Brynjolfsson E., Li S., Zou A., Levine L., Han B., Fu J., Liu Z., Shin J., Lee K., Mazeika M., Phan L., Ingebretsen G., Khoja A., Xie C., Salaudeen O., Hein M., Zhao K., Pan A., Duvenaud D., Li B., Omohundro S., Alfour G., Tegmark M., McGrew K., Marcus G., Tallinn J., Schmidt E., Bengio Y. A Definition of AGI. [Электронный ресурс]. Режим доступа: https://www.agidefinition.ai/paper.pdf (Дата обращения 04.11.2025).
3. Bender E.M., Gebru T., McMillan-Major A., Shmitchell S. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? [Электронный ресурс]. Режим доступа: https://lifearchitect.ai/pdf/2021-bender-parrots.pdf (Дата обращения 04.11.2025).
4. Bowman S.R. Eight Things to Know about Large Language Models [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2304.00612 (Дата обращения 04.11.2025).

УДК 004.8:004.942

# НЕЙРОСЕТИ В ИГРОВОЙ ИНДУСТРИИ: ЭВОЛЮЦИЯ ОТ АЛГОРИТМОВ К САМООБУЧАЮЩИМСЯ МИРАМ

**Рогаткин Н.А.**[1] (магистрант), **Большаков Г.В.**[1] (магистрант)
**Научный руководитель – кандидат технических наук Бутылкина К.Д.**[1]
[1]Университет ИТМО
fenekxyz@gmail.com

**Аннотация**
Статья посвящена возможным путям эволюции нейросетевых технологий в игровой индустрии и исследует их влияние на формирование адаптивных, самообучающихся игровых миров. В работе анализируются традиционные подходы к искусственному интеллекту в видеоиграх, основанные на предопределённых алгоритмах и деревьях решений, и выявляются их ограничения, включая высокую предсказуемость и неспособность к саморегуляции. Рассматриваются современные методы глубокого обучения с подкреплением (Deep Reinforcement Learning), демонстрирующие потенциал к освоению стратегий и выработке новых тактических решений, на примере проектов DeepMind и AlphaStar. Особое внимание уделяется аппаратным и программным предпосылкам внедрения нейросетей, включая возможности децентрализованного обучения на пользовательском оборудовании. Авторы предлагают концепцию гибридной архитектуры, объединяющей модуль обучения с подкреплением, генеративный языковой модуль и сенсорный модуль анализа поведения пользователя, что обеспечивает адаптацию игровых агентов под индивидуальные стили игроков. Дополнительно рассматривается применение нейросетей для генерации игровых ресурсов и контента на основе текстовых описаний, что открывает новые формы интерактивного соавторства. Исследование подчеркивает переход от статичных алгоритмов к динамичным, самообучающимся системам, что открывает новые горизонты для создания развивающихся игровых экосистем и создание нового жанра цифрового искусства.

**Ключевые слова**
Искусственный интеллект, игровая индустрия, адаптивные игровые системы, процедурная генерация контента.

Искусственный интеллект и нейросетевые технологии в последние годы стали одними из ключевых факторов цифровой трансформации общества. Их внедрение наблюдается не только в сфере научных исследований и промышленности, но и в области досуга, где они постепенно начинают определять новые формы взаимодействия между человеком и машиной. Видеоигры как сложная социотехническая система представляют собой оптимальную среду для интеграции нейросетей, так как сочетают элементы искусства, программной инженерии, когнитивной психологии и поведенческого моделирования.

Цель данной статьи заключается в исследовании возможностей и направлений применения нейросетевых технологий в игровой индустрии, выявлении недостатков существующих подходов и формулировании новых методов построения адаптивных, самообучающихся игровых систем. Авторы анализируют эволюцию искусственного интеллекта в видеоиграх – от простейших скриптовых моделей до комплексных архитектур с элементами генеративного и обучающегося поведения. Кроме того, в статье рассматриваются аппаратные и программные предпосылки для дальнейшего распространения нейросетей в индустрии развлечений, а также оцениваются социально-культурные последствия их интеграции.

Традиционные методы реализации искусственного интеллекта в играх на протяжении десятилетий основывались на предопределённых алгоритмах и деревьях принятия решений. Такие системы отличались высокой предсказуемостью и неспособностью адаптироваться к непредусмотренным сценариям. Исследователи в статье «DeepMind and Blizzard open StarCraft II as an AI research environment» показали, что большинство игровых ИИ действуют по принципу «жёсткого» сценарного реагирования и не способны к саморегуляции. В результате игроки довольно быстро находят уязвимости в поведении противников, что снижает глубину и реиграбельность проектов [1].

На смену этим подходам могут придти методы глубокого обучения с подкреплением (Deep Reinforcement Learning, DRL). Именно такой метод лёг в основу ряда знаковых разработок. Одной из них стала работа «AlphaStar: Mastering the real-time strategy game StarCraft II», где описывается агент, обучавшийся на играх профессиональных игроков. Этот эксперимент стал знаковым – впервые нейросеть показала потенциал к развитию созданию челленджа для игроков, приближенных к человеческому уровню лучших киберспорстменов мира. Однако исследователи указали на ключевую проблему – отсутствие способности к самообучению в реальном времени и ограниченность контекста восприятия [2].

Бурное развитие технологий нейровычислений во многом стало возможным благодаря совершенствованию аппаратного обеспечения. Производители графических процессоров, в частности NVIDIA, внедряют специализированные Tensor-ядра, предназначенные для ускорения работы нейросетей. Это создало фундамент для появления игровых систем, где обучение может происходить не только на стороне серверов, но и непосредственно на пользовательском оборудовании. Авторы отмечают, что подобная тенденция ведёт к децентрализации ИИ-обработки, что позволит создавать «игры, обучающиеся вместе с игроком». В рамках данного исследования рассматривается задача создания интерактивных игровых систем с адаптивным поведением, что предполагает наличие в игре агентов, способных корректировать свои действия на основе индивидуального стиля игрока. Ключевым элементом такой системы является использование обучения с подкреплением, как показано в работе «Playing Atari with Deep Reinforcement Learning». В ней описан принцип вознаграждения, при котором агент постепенно вырабатывает оптимальную стратегию взаимодействия с окружающей средой. Применение подобных методов в игровой индустрии открывает возможности для создания динамически развивающихся миров, где сложность, сюжетные линии и реакции персонажей подстраиваются под конкретного пользователя. Например, в будущем ИИ может анализировать предпочтения игрока и формировать миссии, локации и диалоги, соответствующие его эмоциональному состоянию или стилю игры. Компании-разработчики активно исследуют возможности нейросетей для создания новых форм интерактивности. Так, Ubisoft La Forge реализует проекты по моделированию поведения NPC на основе анализа реальных данных игроков, включая их голосовые и поведенческие сигналы. Это позволяет формировать вероятностные модели реакций, создавая иллюзию осознанности виртуальных существ. EA Research проводит эксперименты с предиктивными системами, способными прогнозировать решения игрока и адаптировать игровой процесс под его ожидания [3].

MIT Media Lab предложил инновационную концепцию генеративных агентов в работе «Generative Agents: Interactive Simulacra of Human Behavior». Такие модели демонстрируют когнитивную устойчивость, память и способность к социальному взаимодействию. Применение подобных систем в ролевых играх открывает путь к созданию персонажей, обладающих индивидуальностью, собственными целями и динамически изменяющимся отношением к игроку. Игра Baldur’s Gate 3, имеет огромное число сюжетных развилок и реакций персонажей демонстрирует потенциал динамического повествования. Однако её разработка вручную чрезвычайно трудоёмка. Генеративные модели могут стать отличным решением для автоматизации нарративного дизайна, вместо ручной проработки. Персонажи смогут анализировать внешние факторы и действия игрока в реальном времени, и отвечать на это, соответственно.

В статье [4] предложена гибридная архитектура, объединяющая три ключевых компонента:

1. Модуль обучения с подкреплением (RL-модуль) – отвечает за адаптацию поведения игровых агентов.
2. Генеративный языковой модуль (LLM-модуль) – формирует диалоги и сюжетные ветви в зависимости от действий игрока.
3. Сенсорный модуль анализа поведения пользователя, использующий элементы аффективных вычислений для интерпретации эмоций и скорости реакции.

Подобная структура позволит достичь значительно более естественного взаимодействия между игроком и виртуальной средой. В частности, агенты способны предсказывать намерения пользователя, изменять стратегию поведения и демонстрировать признаки «личности».

Помимо ИИ-поведения, нейросети активно внедряются в сферу генерации игровых ресурсов. Инструменты DreamFusion, NVIDIA GET3D и Unreal Engine 5 Neural Tools дают возможность создавать 3D-модели и текстуры по текстовому описанию. Это открывает дорогу к концепции «игрового соавторства», где игрок может формулировать запросы на естественном языке – например, «создай горный пейзаж с древним храмом и поселением внизу», – а система автоматически сгенерирует соответствующую сцену. Такой подход делает возможным появление игр, полностью создаваемых пользователями при поддержке ИИ, что радикально меняет роль игрока в экосистеме видеоигр. Он становится не потребителем, а активным участником творческого процесса. Анализ показывает, что внедрение нейросетевых технологий ведёт к качественному изменению самой природы видеоигр. Игровое пространство становится нелинейным, саморегулирующимся и персонализированным. Взаимодействие человека и машины превращается из формального обмена командами в полноценный когнитивный диалог. В статье подчёркивается, что нейросети постепенно переходят от инструмента разработчика к равноправному субъекту творческого процесса. Это создаёт новую исследовательскую парадигму – игровая среда становится лабораторией для изучения поведения, социальной динамики и эмоциональных реакций человека. Однако для практической реализации этих идей необходимы дальнейшие исследования в области оптимизации вычислений, энергоэффективности моделей и этической регуляции поведения ИИ. Вопросы, связанные с прозрачностью принятия решений нейросетью, безопасностью данных игроков и предотвращением непредсказуемых реакций системы, требуют отдельного анализа.

В ходе проведённого исследования выполнен теоретический и аналитический обзор направлений внедрения нейросетей в видеоигры. Определены основные тенденции – переход от статических алгоритмов к самообучающимся системам, развитие гибридных архитектур RL+LLM и внедрение процедурной генерации контента. Показано, что интеграция нейросетевых технологий позволит формировать новую форму цифрового взаимодействия, в которой игрок становится соавтором, а игра – развивающейся когнитивной системой. Основные результаты работы включают:

- выявление ключевых недостатков традиционных методов построения игрового ИИ и предложений по их устранению;
- формулировку концепции гибридной нейросетевой архитектуры для моделирования адаптивных миров;
- систематизацию существующих практических решений и определение направлений их дальнейшего развития;

В перспективе развитие данной области приведёт к созданию самообучающихся игровых экосистем, где искусственный интеллект будет не просто инструментом, а активным участником взаимодействия. В ближайшие десятилетия нейросетевые игры, вероятно, сформируют отдельный жанр цифрового искусства, в котором граница между разработчиком, игроком и машиной окончательно исчезнет, открывая новую эпоху симбиоза человека и искусственного интеллекта.

**Литература**

1. DeepMind and Blizzard open StarCraft II as an AI research environment [Электронный ресурс]. Режим доступа: https://deepmind.google/blog/deepmind-and-blizzard-open-starcraft-ii-as-an-ai-research-environment/ (Дата обращения 04.11.2025).
2. AlphaStar: Mastering the real-time strategy game StarCraft II [Электронный ресурс]. Режим доступа: https://deepmind.google/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/ (Дата обращения 04.11.2025).
3. Mnih V., Kavukcuoglu K., Silver D., et al. Playing Atari with Deep Reinforcement Learning [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/1312.5602 (дата обращения 04.11.2025).
4. Park J.S., O'Brien J., Cai C. J., Morris M.R., Liang P., Bernstein M.S. Generative Agents: Interactive Simulacra of Human Behavior [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2304.03442 (дата обращения 04.11.2025).

УДК 004.056.5:004.89

# ИСПОЛЬЗОВАНИЕ LLM-МОДЕЛЕЙ В ОБНАРУЖЕНИИ И ПРЕДОТВРАЩЕНИИ КИБЕРАТАК

**Большаков Г.В.**[1] (магистрант), **Лемешко А.В.**[1] (магистрант), **Рогаткин Н.А.**[1] (магистрант)
**Научный руководитель – кандидат технических наук Бутылкина К.Д.**[1]
[1]Университет ИТМО
zhora.vb@gmail.com

**Аннотация**
В статье рассматриваются возможности применения больших языковых моделей в задачах защиты и обнаружения кибератак. Отмечается, что архитектура трансформер обеспечивает моделям способность к контекстному анализу, выявлению закономерностей и построению причинно-следственных связей, что делает их перспективным инструментом для кибербезопасности и интеллектуального анализа угроз. На основе анализа четырёх исследований показано, что большие языковые модели могут выполнять функции как наступательного, так и оборонительного характера. Модели способны анализировать уязвимости, прогнозировать сценарии атак, интерпретировать сетевые события и участвовать в форензике инцидентов. В отличие от традиционных сигнатурных систем, большие языковые модели обеспечивают понимание контекста действий атакующих и позволяют создавать интеллектуальные системы реагирования нового поколения. В статье предлагается трёхуровневая концепция когнитивной обороны, включающая прогностический, оперативный и форензический уровни применения больших языковых моделей. Отмечаются ключевые ограничения: зависимость от обучающих данных, риски утечки информации и недостаточная объяснимость решений. Делается вывод о формировании нового направления в информационной безопасности – интеллектуальной адаптивной обороны, где большие языковые модели выступают аналитическим и предиктивным ядром систем киберзащиты.

**Ключевые слова**
Кибербезопасность, большие языковые модели, обнаружение атак, прогнозирование угроз.

Развитие больших языковых моделей стало одним из важнейших технологических событий последних лет, оказавших значительное влияние на сферу информационной безопасности. Их способность к контекстному анализу, обобщению информации и моделированию поведения делает LLM мощным инструментом не только для генерации текста или программного кода, но и для выполнения сложных аналитических задач в области киберзащиты. Исследования, рассмотренные в статье, показывают, что LLM способны выполнять функции, ранее считавшиеся исключительно прерогативой человека: анализировать уязвимости, выявлять закономерности в атаках и выстраивать цепочки рассуждений, ведущие к предсказанию инцидентов. Однако, несмотря на очевидные успехи, применение LLM в кибербезопасности остаётся противоречивым. С одной стороны, их возможности используются для автоматизации тестов на проникновение и моделирования атакующих сценариев; с другой – существует растущий интерес к их использованию в оборонительных целях. В отличие от традиционных систем обнаружения вторжений (IDS), основанных на сигнатурах и статистике, LLM позволяют анализировать действия атакующих в контексте, определять их мотивацию и выстраивать вероятностные модели поведения, что открывает перспективы создания интеллектуальных систем реагирования, способных не только фиксировать аномалии, но и понимать их смысл. Дальнейшее развитие данной области требует анализа существующих решений, выявления ограничений и оценки перспектив использования языковых моделей как аналитического и предиктивного ядра систем киберзащиты. Статья посвящена рассмотрению данного вопроса на основе четырёх исследований, каждое из которых раскрывает различные аспекты применения LLM в противодействии киберугрозам.

Основной вызов современного этапа цифровой безопасности заключается в росте количества инцидентов, масштабируемости атак и усложнении их логики. Традиционные средства защиты – антивирусы, сигнатурные системы, механизмы эвристического анализа – уже не способны обеспечивать необходимую глубину интерпретации событий.

Киберпреступники используют цепочки уязвимостей, распределённые инфраструктуры и средства социальной инженерии. В таких условиях возникает необходимость создания систем, которые могли бы не просто фиксировать признаки атаки, но и понимать контекст её развития. LLM, благодаря архитектуре трансформер, обладают способностью к рассуждению на уровне семантики и причинно-следственных связей. Данная архитектура делает их естественным кандидатом для интеграции в аналитические и защитные контуры безопасности. Основная задача при этом заключается не только в применении модели для генерации ответов, но и в разработке механизмов, позволяющих ей понимать, интерпретировать и прогнозировать кибератаки, исходя из накопленного опыта и текущего контекста.

Проекты Project Naptime и PentestGPT изначально создавались для оценки наступательных возможностей LLM, однако их результаты стали ценным источником данных для построения оборонительных систем. В работе «Project Naptime: Evaluating Offensive Security Capabilities of Large Language Models» показано, что модель способна выполнять разведку инфраструктуры, анализировать уязвимости и подбирать эксплойты без ручного управления. Для исследователей это стало доказательством того, что LLM понимает логику атакующего процесса, а не просто повторяет известные команды. Такая способность имеет прямое применение в защите: если модель может реконструировать поведение атакующего, она может и предсказать его. Использование LLM в режиме «обратного пентестинга» позволяет организациям моделировать потенциальные угрозы и формировать защитные сценарии заранее. Таким образом, наступательный потенциал становится инструментом профилактики. Проект «PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing» также продемонстрировал, что LLM могут выполнять интерактивный анализ инфраструктуры, уточняя гипотезы по мере получения новых данных. Такой адаптивный подход лежит в основе когнитивных систем защиты, где модель учится на каждом новом инциденте и корректирует собственные предположения, что позволяет перейти от статичных баз сигнатур к динамическому контекстному анализу, при котором система не просто реагирует на известные атаки, а предугадывает новые [1, 4].

Одним из открытий в работе «LLM Agents can Autonomously Exploit One-day Vulnerabilities» стало подтверждение того, что агенты на базе LLM способны самостоятельно находить и использовать уязвимости. Однако исследователи подчеркнули, что те же принципы можно обратить в защитную сторону, то есть если LLM может понять структуру эксплойта, она может выработать и контрмеру к нему. В оборонительном контексте LLM может служить ядром для построения автоматизированных систем мониторинга, где модель анализирует технические отчёты, описания CVE и сопоставляет их с текущими конфигурациями систем. Это даёт возможность обнаруживать потенциально уязвимые компоненты ещё до того, как они будут использованы злоумышленником. Такая проактивная стратегия защиты особенно важна для критической инфраструктуры, где время реакции определяет уровень риска. Кроме того, возможность LLM к рассуждению и выводу объяснений делает её полезным инструментом для форензики – анализа уже произошедших атак. Модель может реконструировать последовательность действий, выявить взаимосвязи между событиями и предложить возможные пути нейтрализации угрозы. Это превращает LLM в аналитический модуль систем постинцидентного реагирования [3].

Исследование «Introducing RedFlag: Using AI to Scale Addepar’s Offensive Security Team» представляет противоположный полюс применения языковых моделей – в качестве средства внутреннего анализа и классификации инцидентов. Система RedFlag, интегрированная в инфраструктуру компании Addepar, использует LLM для обработки сигналов безопасности, корреляции событий и выявления подозрительной активности. Главное отличие этого подхода в том, что LLM не только анализирует журналы и сетевые данные, но и интерпретирует смысл происходящего. Она способна связать действия пользователей, изменения в конфигурациях и системные логи в единую цепочку событий, тем самым определяя, является ли инцидент случайным сбоем или проявлением вредоносной активности. Практический эффект RedFlag проявился в сокращении времени реакции и

повышении точности классификации угроз. Такой результат особенно ценен, так как показывает, что языковые модели могут выполнять функции не просто фильтра, а интеллектуального аналитика. Для служб безопасности это означает переход от ручной оценки сигналов к полуавтоматическому анализу, где модель помогает человеку выделять наиболее значимые события [2].

Сопоставление четырёх рассмотренных проектов позволяет выделить общие закономерности, определяющие потенциал LLM в защите и обнаружении кибератак. Во-первых, все модели демонстрируют способность к пониманию контекста, что отличает их от предыдущих поколений инструментов. Во-вторых, LLM могут действовать в разных режимах – автономном, поддерживающем и консультативном, что делает их гибким элементом в архитектуре систем защиты. На основе этих исследований можно предложить аналитическую модель применения LLM в киберзащите, включающую три взаимосвязанных уровня:

1. Прогностический уровень – модель анализирует данные об уязвимостях, моделирует поведение потенциальных атакующих и вырабатывает прогноз вероятных инцидентов.
2. Оперативный уровень – LLM участвует в анализе событий в реальном времени для фильтрации логов, выявлении аномалий, интерпретации угроз.
3. Форензический уровень – после инцидента LLM анализирует следы атаки, восстанавливает её сценарий и предлагает меры по устранению уязвимостей.

В совокупности эти уровни формируют контур «когнитивной обороны» – системы, где человек и ИИ взаимодействуют на уровне рассуждения, а не простого реагирования. LLM становятся не инструментом подмены аналитика, а его интеллектуальным партнёром, обеспечивающим полноту картины угроз.

Несмотря на очевидные преимущества, исследования выявляют и ряд ограничений. Главная проблема – зависимость качества анализа от данных, на которых обучена модель. Если в обучающем корпусе отсутствуют актуальные сведения о новых угрозах, LLM может давать ложные интерпретации. Другим вызовом является риск утечки конфиденциальной информации при использовании облачных моделей. В работе «Introducing RedFlag: Using AI to Scale Addepar’s Offensive Security Team» особое внимание уделялось созданию локальной инфраструктуры для исключения подобных рисков. Также важным вопросом остаётся объяснимость решений LLM: несмотря на способность выдавать убедительные рассуждения, не всегда очевидно, на основании каких признаков был сделан тот или иной вывод. Тем не менее, исследователи сходятся во мнении, что эти проблемы могут быть решены с помощью гибридных архитектур, в которых LLM работает совместно с классическими системами мониторинга, сохраняя баланс между гибкостью и контролируемостью [2].

Проведённый анализ четырёх ключевых исследований позволяет сделать вывод о формировании нового подхода к защите информационных систем – интеллектуальной адаптивной обороны, в центре которой находятся большие языковые модели. LLM обеспечивают возможность глубокого контекстного анализа, прогнозирования угроз и автоматизации процессов реагирования. Основным достижением на текущем этапе является доказанная способность моделей выполнять функции прогнозирования и интерпретации атак, что переводит кибербезопасность из области реактивных мер в область проактивных. Исследования Project Naptime и PentestGPT показывают, что LLM могут выступать в роли предиктивного инструмента, имитирующего действия атакующего, а работы RedFlag и LLM Agents – что те же механизмы применимы для аналитики и защиты. Результаты анализа позволяют сформулировать несколько значимых выводов:

1. LLM способны объединять данные из разных источников и извлекать смысловые связи, недоступные традиционным системам.
2. Использование LLM повышает скорость реакции и снижает нагрузку на специалистов SOC, позволяя автоматизировать обработку инцидентов.
3. Возможность прогнозирования атак превращает LLM в инструмент стратегической защиты.

4. Эффективность систем на базе LLM напрямую зависит от прозрачности их обучения и наличия механизмов аудита решений.

Перспективным направлением дальнейших исследований является разработка локальных LLM, специально обученных на данных безопасности, создание механизмов интерпретации решений и интеграция таких моделей в экосистемы киберзащиты. В долгосрочной перспективе это позволит сформировать системы, где человек и искусственный интеллект действуют в едином аналитическом цикле: ИИ предсказывает угрозу, человек подтверждает и корректирует решение, а система обучается на совместном опыте. Следовательно, LLM перестают быть лишь инструментом автоматизации – они становятся основой нового поколения защитных систем, способных понимать контекст угроз, адаптироваться к изменениям и обеспечивать интеллектуальную устойчивость цифровой инфраструктуры.

**Литература**

1. Sergei Glazunov, Mark Brand, Google Project Zero. Project Naptime: Evaluating Offensive Security Capabilities of Large Language Models [Электронный ресурс]. Режим доступа: https://googleprojectzero.blogspot.com/2024/06/project-naptime.html (Дата обращения 06.11.2025).
2. Thomas Greenwood, Blane Honeycutt. Introducing RedFlag: Using AI to Scale Addepar's Offensive Security Team [Электронный ресурс]. Режим доступа: https://addepar.com/blog/introducing-redflag-using-ai-to-scale-addepar-s-offensive-security-team (Дата обращения 06.11.2025).
3. Richard Fang, Rohan Bindu, Akul Gupta, Daniel Kang. LLM Agents can Autonomously Exploit One-day Vulnerabilities [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2404.08144 (Дата обращения 06.11.2025).
4. Gelei Deng, Yi Liu, Víctor Mayoral-Vilches, Peng Liu, Yuekang Li, Yuan Xu, Tianwei Zhang, Yang Liu, Martin Pinzger, Stefan Rass. PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2308.06782 (Дата обращения 06.11.2025).

УДК 004.056.5:004.738

# РИСКИ УТЕЧКИ ИНФОРМАЦИИ ПРИ УТИЛИЗАЦИИ ИНТЕРЕНТ ВЕЩЕЙ

**Лемешко А.В.**[1] (магистрант), **Большаков Г.В.**[1] (магистрант), **Рогаткин Н.А.**[1] (магистрант)
**Научный руководитель – преподаватель Мешков А.В.**[1]
[1]Университет ИТМО
klaycompany358@gmail.com

**Аннотация**
В статье рассматриваются проблемы, связанные с рисками утечки персональных данных при утилизации устройств Интернет вещей (IoT). Исследуется структура и характер данных, сохраняемых в бытовых IoT-устройствах, таких как умные лампы, камеры видеонаблюдения, колонки и прочие элементы «умного дома». Проведен анализ известных случаев извлечения конфиденциальных сведений с утилизированных устройств и рассмотрены технические уязвимости, обусловленные как особенностями архитектуры IoT, так и отсутствием стандартов безопасного удаления информации. Особое внимание уделено сопоставлению методов очистки данных, применяемых различными производителями, и анализу степени их соответствия требованиям международных стандартов информационной безопасности, в частности ETSI EN 303 645. В статье показано, что большинство IoT-устройств сохраняют критически важные персональные данные, которые могут быть извлечены злоумышленниками даже после сброса настроек. Также предлагаются рекомендации, алгоритмы безопасной утилизации устройств и организационно-технические меры, направленные на снижение вероятности утечки данных.

**Ключевые слова**
Интернет вещей, IoT, информационная безопасность, утилизация, персональные данные, безопасное удаление данных.

Технологии Интернет вещей (Internet of Things, IoT) стремительно интегрируются в повседневную жизнь. Сегодня миллионы пользователей ежедневно взаимодействуют с умными колонками, видеокамерами, лампами, бытовыми датчиками и системами управления домом. Данные устройства не просто выполняют команды — они собирают, обрабатывают и передают данные о пользователях, их привычках, геолокации, расписании и параметрах домашней сети. Таким образом, каждая единица IoT-инфраструктуры становится потенциальным хранилищем конфиденциальной информации. На первый взгляд, проблема безопасности кажется решённой. Производители предлагают функции «сброса к заводским настройкам», и пользователи могут просто выбросить или продать устройство. Однако исследования последних лет показывают, что сброс настроек редко означает удаление данных. В исследовании, проведённом в Zhejiang University, было продемонстрировано, что даже после «полного сброса» в энергонезависимой памяти сохраняются логины, пароли Wi-Fi и токены облачных сервисов. В результате делает утилизированные устройства прямым источником утечки персональной информации. Следовательно, возникает противоречие между заявленной безопасностью и реальным состоянием дел. IoT-устройства, по сути, остаются «цифровыми архивами» владельцев, доступ к которым можно получить физически или программно. Отсутствие единых стандартов безопасного удаления данных и разнородность архитектур только усиливают масштаб проблемы. Цель данной работы — проанализировать риски утечки персональных данных при утилизации IoT-устройств, выявить слабые места существующих методов очистки и предложить меры, обеспечивающие реальную защиту пользователей [1].

Проблема хранения данных в IoT-устройствах носит комплексный характер. В отличие от персональных компьютеров или смартфонов, где существуют стандартные механизмы форматирования и шифрования, большинство «умных» гаджетов имеет закрытую архитектуру с минимальным контролем со стороны пользователя. При этом устройства накапливают значительные объёмы информации, такие как параметры подключения к Wi-Fi, учётные данные для синхронизации с облаком, внутренние журналы событий. В исследовании Zhejiang University было установлено, что умные лампы или розетки, сохраняют в прошивке незашифрованные пароли от домашней сети. Эти сведения можно

извлечь, подключившись к интерфейсам отладки (UART или SPI). Данные выводы подтверждаются практическим экспериментом «Pwn the LIFX Mini White», где исследователи получили доступ к конфигурационным данным лампы и смогли восстановить сетевые параметры пользователя. Подобные случаи показывают, что для злоумышленников физический доступ к утилизированному устройству открывает возможность вторжения в частную сеть [1, 2].

Производители устройств заявляют о наличие функции «сброс к заводским настройкам», однако на практике она чаще всего ограничивается удалением пользовательских сценариев и визуальных настроек. Физические данные в памяти при этом сохраняются. В рамках упомянутого исследования было протестировано несколько десятков бытовых IoT-устройств, и более чем в половине случаев после сброса оставались активные данные: сетевые ключи, токены и идентификаторы пользователя. Именно поэтому, привычная для потребителя процедура сброса не обеспечивает даже минимального уровня безопасности [1].

Международный стандарт ETSI EN 303 645 Cyber Security for Consumer Internet of Things закрепляет требование о наличии функции безопасного удаления персональных данных. Однако, как отмечается в анализе реализации стандарта, большинство производителей выполняют его частично или формально. Причина в отсутствии механизмов контроля: стандарт носит рекомендательный характер, а сертификация устройств по нему не обязательна. В результате рынок насыщен устройствами, которые потенциально способны раскрыть конфиденциальную информацию владельца после их утилизации. Для иллюстрации приведено сравнение нескольких популярных устройств в таблице [3].

Таблица

**Анализ соответствия методов очистки данных IoT-устройств требованиям стандарта**

| Тип устройства | Метод очистки по инструкции | Фактическое поведение | Соответствие стандарту ETSI EN 303 645 |
|---|---|---|---|
| Умная лампа LIFX / TP-Link | Сброс через кнопку питания | Wi-Fi-параметры остаются в памяти | Частично |
| Умная камера Xiaomi / Ezviz | Удаление через мобильное приложение | Логи и сетевые ключи сохраняются | Не соответствует |
| Голосовая колонка Amazon Echo / Google Nest | Удаление учётной записи | Остаточные токены авторизации | Частично |

Из таблицы видно, что ни одно из протестированных устройств не обеспечивает полной очистки памяти. Следовательно, при продаже, передаче или утилизации такие устройства могут стать источником компрометации сети.

Особую опасность представляют случаи, когда утилизированные устройства попадают на вторичный рынок. Камера, хаб или колонка, формально сброшенная к заводскому состоянию, но не очищенная полностью, может быть использована для атаки на прежнего владельца. Например, токен или идентификатор устройства позволяет подключиться к его облачному профилю и получить доступ к данным. В исследовании Smart Privacy and Security in IoT Devices этот сценарий описывается как «ретроспективная компрометация» — ситуация, при которой устройство, утратившее владельца, остаётся связанным с его цифровой идентичностью. Для минимизации подобных рисков необходим комплекс мер. Во-первых, производителям следует внедрять процедуру безопасного удаления данных, основанную на криптографическом уничтожении ключей шифрования, что делает невозможным восстановление информации даже при физическом доступе. Во-вторых, прошивка устройства должна предусматривать перезапись всех областей памяти при

обновлении. Такой метод позволит гарантировать, что конфиденциальные данные не сохраняются в скрытых разделах. Пользователи, со своей стороны, также могут существенно снизить риски. Прежде всего, необходимо перед утилизацией отвязать устройство от облачного аккаунта и удалить его из системы управления. Далее, по возможности, следует выполнить полное обновление прошивки, а для устройств, не поддерживающих функции шифрования, — физически разрушить чип памяти. Особое внимание рекомендуется уделить сетевой сегментации. Все IoT-устройства следует подключать не к основной, а к отдельной беспроводной сети Wi-Fi, созданной специально для «умных» гаджетов. Такая архитектура изолирует потенциально уязвимые устройства от компьютеров, смартфонов и других критичных узлов сети. Если злоумышленнику удастся получить доступ к IoT-устройству, его возможности будут ограничены рамками вспомогательной подсети. Данный подход — один из самых эффективных способов защиты инфраструктуры при эксплуатации и утилизации устройств Интернет вещей в настоящий момент [1].

Проведённый анализ показывает, что риск утечки персональных данных при утилизации устройств Интернета вещей остаётся крайне высоким. Несмотря на наличие механизмов «сброс для заводских настроек», так как большинство устройств сохраняют конфиденциальные сведения в энергонезависимой памяти. Исследование Smart Privacy and Security in IoT Devices и стандарт ETSI EN 303 645 подтверждают, что существующие методы очистки данных не обеспечивают полного соответствия принципам безопасного удаления информации. Причинами данной проблемы являются недостаточная проработанность архитектуры IoT-устройств, экономия производителей на реализации криптографических средств защиты и отсутствие обязательных стандартов сертификации. В результате превращает этап утилизации в слабое звено системы кибербезопасности. Развитие данной темы должно идти по пути стандартизации и сертификации IoT-устройств в области безопасности хранения и удаления данных. Перспективным направлением является создание международного протокола IoT Secure Disposal Framework, который объединит требования к аппаратной, программной и организационной защите информации на всех этапах жизненного цикла устройства. Только комплексный подход позволит предотвратить утечки данных и обеспечить доверие пользователей к экосистеме Интернет вещей [1, 3].

**Литература**

1. Zhejiang University. Smart Privacy and Security in IoT Devices: Risk Analysis and Practical Attacks [Электро нный ресурс]. Режим доступа: https://nesa.zju.edu.cn/download/lpy_pdf_sp23.pdf (Дата обращения: 10.11.2025).
2. Limited Results. Pwn the LIFX Mini White [Электронный ресурс]. Режим доступа: https://limitedresults.com/2019/01/pwn-the-lifx-mini-white (Дата обращения: 10.11.2025).
3. ETSI EN 303 645 V3.1.3 (2023-06). Cyber Security for Consumer Internet of Things: Baseline Requirements [Электронный ресурс]. Режим доступа: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (Дата обращения: 10.11.2025).

УДК 004.056.5

# СОВРЕМЕННЫЕ ТЕНДЕНЦИИ PHISHING-АТАК И АНАЛИЗ ЭФФЕКТИВНОСТИ АНТИФИШИНГОВЫХ ТЕХНОЛОГИЙ

**Лемешко А.В.**[1] (магистрант), **Большаков Г.В.**[1] (магистрант), **Рогаткин Н.А.**[1] (магистрант)
**Научный руководитель – преподаватель Мешков А.В.**[1]
[1]Университет ИТМО
klaycompany358@gmail.com

**Аннотация**
Фишинг переживает очередной виток развития и превращается в многослойную экосистему, где автоматизация, преступные сервисы и социальная инженерия соединяются в единое целое. Масштаб проблемы давно вышел за пределы традиционных писем-подделок, а угрозы направлены прежде всего на человека, как слабое звено цифровой безопасности. Анализ отчётов и исследований указывает, что злоумышленники активно отходят от прежних примитивных методов и переходят к тонко выстроенным многоэтапным схемам. AiTM-атаки (Adversary-in-the-Middle), сервисы перехвата многофакторной аутентификации вроде EvilProxy, гибридные модели QR-фишинга и динамически создаваемые фишинговые страницы становятся неотъемлемой частью современной преступной инфраструктуры. Ускорение этой эволюции поддерживается появлением phishing-as-a-service, что снижает порог входа и открывает доступ к сложным техникам даже малоопытным злоумышленникам. Параллельно развиваются защитные механизмы: облачные ML-фильтры и антифишинговые движки действительно становятся точнее, но сталкиваются с ограничениями, связанными с адаптивностью атакующих и активным использованием легитимных сервисов-посредников. Несмотря на формальный прогресс, эффективность защиты оказывается переменной, успешность атак остаётся высокой, а многие схемы обходят фильтры за счёт автоматической подмены контента, прокси-механизмов и точечного влияния на поведенческие признаки пользователей. Статья анализирует ключевые тенденции в современном фишинге, исследует причины его устойчивости и оценивает способность существующих технологий противостоять новым вектором угроз. Делается вывод о том, что дальнейшая борьба с фишингом потребует симбиоза машинных методов, персонализированного обучения пользователей и системного изменения архитектуры аутентификации.

**Ключевые слова**
Фишинг, AiTM, MFA-bypass, EvilProxy, QR-фишинг, phishing-as-a-service, антифишинговые технологии, машинное обучение.

Массовое распространение цифровых сервисов в последние годы не только упростило коммуникацию, но и создало удобную почву для фишинговых кампаний. Фишинг давно перестал быть хаотичным набором рассылок. Он стал частью хорошо организованной криминальной экономики, где статистика и отчёты крупных исследовательских центров лишь подтверждают устойчивый рост атак. Корпоративные отчёты безопасности фиксируют доминирование социальной инженерии в структуре инцидентов, а именно фишинг удерживает лидирующие позиции среди первичных векторов проникновения, зачастую являясь отправной точкой для последующего внедрения вредоносных программ, компрометации аккаунтов или внутренних сетей. Сходные тенденции прослеживаются и в оценках глобальных угроз. Крупные исследовательские структуры отмечают, что злоумышленники продолжают смещать фокус на методы, позволяющие обходить традиционные средства защиты и максимально довериться человеческому фактору. Как раз это дает нам понять, что именно пользователь, а не инфраструктура, остаётся ключевой целью атакующих. Развитие фишинга идёт не в сторону технического усложнения вредоносной нагрузки, а в сторону усложнения схем обмана и перехвата учётных данных [1, 2].

Текущая ситуация подталкивает преступников к более изощрённым сценариям. Фишинг перестал быть статичным. Он реагирует на защитные технологии не хуже, чем естественная экосистема на внешние раздражители. Когда традиционные фильтры стали эффективно обнаруживать массовые рассылки, злоумышленники переключились на персонализированные сценарии, укрытые за легитимными инфраструктурами, а затем — на

схемы, где атакуемый пользователь взаимодействует с прокси-сервисом, способным незаметно перехватывать параметры аутентификации в режиме реального времени.

Среди наиболее значимых тенденций — рост AiTM-атаки. В подобных схемах злоумышленник создаёт промежуточный прокси-сервер, через который проходит подлинная сессия пользователя. Когда жертва открывает фишинговую ссылку, ей показывается фактический интерфейс реального сервиса, но весь обмен данными проходит через руки атакующего. Такой подход позволяет перехватывать не только логин и пароль, но и сеансовые cookie-файлы, что критически важно в эпоху многофакторной аутентификации. Исследователи подчёркивают, что рост подобных атак особенно заметен благодаря популяризации сервисов-посредников, предлагающих полный набор инструментов для обхода MFA **(Multi-Factor Authentication)**. Платформы наподобие EvilProxy формируют новую преступную модель: phishing-as-a-service. Злоумышленнику больше не требуется обладать глубокими техническими навыками. Достаточно приобрести доступ к панели управления, где автоматически генерируются фишинговые URL, настраиваются прокси-механизмы и включаются функции обхода многофакторной аутентификации. Такой подход оказался в центре масштабных атак на корпоративные учётные записи, где злоумышленники активно использовали доверенные домены и легитимные хостинг-платформы. В отчетах говорится, что злоумышленники активно нацелены на сервисы подбора персонала, где человеческое доверие особенно предсказуемо, а компрометация учётной записи может привести к цепочке новых атак. Параллельно с усложнением AiTM-моделей развивается QR-фишинг. Подавляющее большинство пользователей относится к QR-кодам как к нейтральному и естественному элементу среды, что создаёт идеальные условия для социальной инженерии. QR-код скрывает ссылку визуально, а потому большинство фильтров электронной почты и корпоративных систем защиты изначально воспринимают его лишь как изображение. Как раз этим злоумышленники активно пользуются. QR-код помещается в тело письма или на физический носитель, после чего перенаправляет жертву на динамически созданный фишинговый сайт. Отчёты указывают, что, в сравнении с классическими письмами, QR-фишинг демонстрирует более высокий показатель успешных переходов, поскольку вызывает значительно меньше подозрений и часто проходит мимо автоматических фильтров. Не исчез и традиционный email-фишинг, хотя его структура меняется. Если раньше злоумышленники рассчитывали на массовость, то теперь ставка делается на точечные атаки. А точнее использование «живых» доменов, компрометированных бизнес-сервисов, легитимных облачных хранилищ и поддельных HTML-форм позволяет увеличивать эффективность. Интересно, что современные фишинговые страницы часто имеют всего несколько минут «времени жизни». Динамическая генерация URL усложняет работу антиспам-системам, ведь многие механизмы фильтрации полагаются на репутационные признаки, которые просто не успевают сформироваться. Исследовательские отчёты подтверждают, что фишинг движется в сторону краткосрочных, но высокоэффективных всплесков активности, опирающихся на автоматизацию инфраструктуры [1–5].

Состояние защитных технологий выглядит противоречиво. Машинное обучение позволило повысить точность классификации, но его эффективность во многом ограничена тем, что злоумышленники научились эксплуатировать слепые зоны. Использование легитимных доменов, прокси-платформ, динамических форм и шаблонов, загружаемых с доверенных CDN-источников (Content Delivery Network), не позволяет ML-модели учитывать полную контекстуальную картину. В отраслевых отчётах подчёркивается, что атакующие активно обходят фильтры за счёт минималистичных писем, содержащих всего одну ссылку или изображение, а также за счёт постепенной адаптации под механизмы анализа контента. Для удобства восприятия современного ландшафта ключевые тенденции фишинга приведены в сравнительной таблице [2, 3].

Таблица

**Ключевые тенденции современного фишинга**

| Техника | Уровень сложности атаки | Цель злоумышленника | Способ обхода защиты | Устойчивость к ML-фильтрам |
|---|---|---|---|---|
| AiTM / EvilProxy | Высокая | Перехват сеансовых cookie, MFA-bypass | Прокси-вмешательство | Высокая |
| QR-фишинг | Средняя | Перенаправление на скрытую страницу | Маскировка URL в изображении | Средняя–высокая |
| Классический email/web | Низкая–средняя | Кража данных | Использование легитимных доменов и вложений | Средняя |
| Целевая рассылка через PaaS | Средняя–высокая | Компрометация бизнес-учётных записей | Динамическая генерация контента | Высокая |

Анализ таблицы показывает, что фундаментальной проблемой остаётся невозможность для ML-фильтров полноценно оценивать доверенные инфраструктуры, которые используются злоумышленниками как транспорт. Не менее важную роль играет сам пользователь, потому что даже самые сложные фильтры бессильны в момент, когда жертва самостоятельно переходит по ссылке или сканирует QR-код. Эту мысль подтверждают и исследования, указывающие, что человеческий фактор остаётся центральным элементом цепочки атаки и определяет исход инцидента чаще, чем уровень технической защиты [2].

Если рассматривать перспективы развития антифишинговых технологий, всё больше внимания получает переход от классических систем фильтрации к многоуровневым моделям контекстного анализа. Речь идёт не только о статистическом анализе писем, но и о комплексном учёте поведенческой биометрии, динамической оценке сеансов и архитектурной перестройке систем аутентификации. Укрепление безопасности должно идти в направлении систем, где кража сеансовых cookie не позволит злоумышленнику перехватить сессию без дополнительных криптографических подтверждений. Некоторые отчёты подчёркивают необходимость перехода к принципам zero trust не только на уровне сетевых политик, но и на уровне пользовательской аутентификации [3].

Рекомендации по защите формируются вокруг нескольких ключевых направлений: формирование цифровой гигиены сотрудников, отказ от переносимых cookie-сессий, применение аппаратных ключей безопасности, контроль за использованием облачных сервисов и внедрение механизмов постоянной верификации. Однако все эти меры будут действенны лишь при условии, что организации перестанут рассматривать фишинг как проблему фильтрации контента. Реальная борьба со схемами AiTM и сервисами MFA-bypass требует системного подхода, включающего переосмысление процессов аутентификации и программ подготовки персонала. Индустрия информационной безопасности переживает момент, когда укрепление технических средств и улучшение алгоритмов недостаточно для снижения наблюдаемой успешности фишинговых атак. Преступники действуют быстро, гибко и способны настраивать инфраструктуру в реальном времени. Защитникам приходится реагировать не менее оперативно, а значит, ставка должна быть сделана на архитектурную устойчивость, минимизацию доверия и создание систем, где эксплуатация человеческого фактора будет не фатальной, а лишь одним из уровней риска.

Фишинг будет оставаться ключевой угрозой до тех пор, пока конфигурация цифровой экосистемы позволяет атакующим с минимальными затратами перехватывать идентификационные данные, обходить многофакторную аутентификацию и подменять

легитимные механизмы доставки контента. Противодействие должно стать более зрелым, многоуровневым и учитывающим поведение не только атакующих, но и самих пользователей. Только такой подход позволит удерживать баланс в постоянно меняющемся ландшафте угроз.

**Литература**

1. 2024 Data Breach Investigations Report [Электронный ресурс]. Режим доступа: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (дата обращения 10.11.2025).
2. Po G. How to Catch a Phish. SuriCon 2024 Lightning Talk [Электронный ресурс]. Режим доступа: https://suricon.net/wp-content/uploads/2024/12/SuriCon2024-Genina-Po_lightning-talk-HowToCatchAPhish.pdf (дата обращения 10.11.2025).
3. Microsoft Digital Defense Report 2024 [Электронный ресурс]. Режим доступа: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf (дата обращения 10.11.2025).
4. State-of-the-Art Phishing: MFA Bypass [Электронный ресурс]. Режим доступа: https://blog.talosintelligence.com/state-of-the-art-phishing-mfa-bypass (дата обращения 10.11.2025).
5. EvilProxy Phishing Attack Strikes Indeed [Электронный ресурс]. Режим доступа: https://www.menlosecurity.com/blog/evilproxy-phishing-attack-strikes-indeed (дата обращения 10.11.2025).

**УДК 2964**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДЕЙСТВУЮЩИХ ПРАКТИК ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭКОНОМИЧЕСКИЕ ПРОЦЕССЫ МЕГАПОЛИСОВ (НА ПРИМЕРЕ МОСКВЫ И САНКТ-ПЕТЕРБУРГА)

**Кирищев В.П.**[1] (студент), **Гаврилюк В.А.**[1] (студент)
[1]Университет Правительства Москвы
kirishchev.v.p@yandex.ru

**Аннотация**
В статье проводится сравнительный анализ современных практик интеграции технологий искусственного интеллекта (ИИ) в экономические и управленческие процессы крупнейших мегаполисов России – Москвы и Санкт-Петербурга. Исследуются ключевые векторы внедрения ИИ в таких сферах, как городское управление, транспортная инфраструктура, здравоохранение, потребительский рынок и финансовый сектор. Выявляются общие тенденции и специфические модельные подходы каждого города. На основе проведенного анализа определяются перспективные направления для дальнейшего развития «умных городов» в России.

**Ключевые слова**
Искусственный интеллект, умный город, цифровая экономика, городское управление, Москва, Санкт-Петербург, большие данные, машинное обучение, компьютерное зрение.

Современный мегаполис представляет собой сложную социально-технологическую систему, эффективное функционирование которой невозможно без применения передовых цифровых технологий. Искусственный интеллект, выступая в роли ключевого драйвера цифровой трансформации, позволяет перейти от реактивного к проактивному и продуктивному управлению городскими процессами, оптимизировать использование ресурсов и повысить качество жизни населения.

Для написания данной работы были выбраны соответствующие теме материалы из различных источников. На основании открытых официальных источников, таких как Государственная программа города Москвы «Цифровая столица» (постановление Правительства Москвы от 22.10.2021), стратегия социально-экономического развития Санкт-Петербурга на период до 2035 года. Был проведен анализ положения и сделаны выводы. Использовались эмпирическо-теоретические методы исследования, в частности метод анализа, метод сравнения и индукции [1–8].

Москва и Санкт-Петербург, как крупнейшие экономические и инновационные центры России, первыми приняли участие во внедрении технологий ИИ. Их опыт представляет значительный научный и практический интерес для анализа различных подходов к построению «умного города». Целью данного исследования является сравнительный анализ подходов и практик внедрения технологий ИИ в экономические процессы Москвы и Санкт-Петербурга. Основными задачами исследования являются:

1. Выявить ключевые направления внедрения ИИ.
2. Систематизировать и классифицировать реализованные проекты на основе ИИ.
3. Выявить общие тенденции и уникальные особенности подходов каждого города.
4. Сформулировать выводы о потенциале адаптации выявленных моделей для других городов.

Под технологиями искусственного интеллекта в контексте городского управления понимается комплекс решений на основе машинного обучения, обработки естественного языка (NLP), компьютерного зрения и предиктивной аналитики, направленный на автоматизацию, оптимизацию и принятие решений.

## Стратегия умного города в Москве

Органы власти города Москвы развивают концепцию умного города в управлении мегаполисом в рамках двух программ: «Электронная Москва» на основании закона Москвы от 09.07.2003 № 47 «О Городской целевой программе «Электронная Москва» и «Информационный город» с 2011 года. В 2018 году Департамент информационных

технологий (ДИТ) Москвы, бизнес-сообщество и москвичи разработали цифровую стратегию Москвы «Умный город – 2030» на основе ИИ для решения городских задач.

Выделено 6 направлений стратегии: 1) развитие социального и человеческого капитала, 2) комфортная городская среда, 3) цифровая мобильность, 4) умная экономика, 5) безопасность и экология, 6) цифровое правительство. Программа «Электронная Москва» обеспечила Департамент ИТ Москвы цифровым оборудованием. «Информационный город»: проведена автоматизация процессов управления и цифровизация услуг в Москве.

В Москве благодаря цифровизации на основе ИИ в здравоохранении обеспечена работа Единой медицинской информационно-аналитической системы (ЕМИАС) – запись на прием в поликлинику через ЕМИАС по полису ОМС, на основании Федерального закона «Об обязательном медицинском страховании в РФ» от 29.11.2010 № 326-ФЗ, спецпроекты Департамента здравоохранения Москвы: «Навигатор московского здравоохранения», «Ценности и принципы в работе поликлиник», «Московский стандарт онкологической помощи», «Эндоскопия по полису ОМС», «Станьте донором», «Календарь детских прививок», «Электронный рецепт», «Получите льготное лекарство» и другие.

В Москве сейчас реализуется более 90 цифровых проектов с применением ИИ. Среди них – медицинские сервисы для диагностики, интеллектуальная транспортная система и голосовой ассистент для общегородского контакт-центра. В городе работают 17 проектов в области транспорта, 16 – в сфере технологий и инноваций, еще 16 – в разных отраслях, а 22 – в строительстве и ЖКХ.

ИИ-система для анализа медицинских изображений (рентген, КТ, МРТ) в городских поликлиниках помогает врачам в ранней диагностике заболеваний (например, онкологических). В период пандемии компьютерное зрение использовалось для мониторинга соблюдения масочного режима.

Москва демонстрирует комплексный и централизованный подход к внедрению ИИ, интегрируя технологии в большинство аспектов городской жизни.

Единый Транспортный Центр (ЕТЦ) на основе ИИ проводит анализ данных с разных источников в реальном времени: камер, датчиков транспорта и радаров. Внедрены алгоритмы для адаптивной работы светофоров. По данным Центра организации дорожного движения г. Москвы (ЦОДД) они оптимизируют работу светофоров, позволяя сократить загруженность магистралей на 15–20%. Сервис «Яндекс.Карты» с функцией «Народный картограф» использует машинное обучение для построения маршрутов общественного транспорта с учетом пассажиропотока.

Платформа «Цифровой двойник Москвы» агрегирует данные о городской инфраструктуре для моделирования сценариев развития и управления ресурсами. Компьютерное зрение используется для мониторинга состояния дворовых территорий, выявления несанкционированных свалок и нарушений в парковочном пространстве, что позволяет перераспределять ресурсы коммунальных служб.

Широкое внедрение AI-чатов в систему госуслуг (МАС) для автоматического ответа на запросы граждан. Ритейл-сети активно используют предиктивные алгоритмы для управления запасами и персоналом.

Одним из целенаправленных проектов цифровизации городской среды выступает концепция (проект) «Умный город». Основными этапами его осуществления выступает создание физической и цифровой инфраструктур, цифровых платформ и на последнем этапе – создание «цифрового двойника» города. Наиболее распространенным для территорий РФ является вариант внедрения в городскую среду персональных интеллектуальных услуг, которое чаще всего носит инициативный характер. Вторым вариантом становятся прототипы умных городов - инфраструктурные площадки (Иннополис, Сколково, Инноград и пр.). Выявлена прямая зависимость между экономическим потенциалом территории, высоким уровнем бюджетной обеспеченности и эффективностью реализации подобных проектов, что является фундаментальным принципом. Высокий экономический потенциал — это основа для спроса и устойчивости.

Такие проекты изначально создаются как центры притяжения для крупного бизнеса, стартапов и исследовательских институтов (например, «Яндекс» в Иннополисе, IT-кластер в Сколково). Без сильной экономики региона или страны, которая может предложить льготы, инфраструктуру и рынок сбыта, привлечь таких игроков невозможно.

Экономический потенциал территории не просто используется, он умножается. Успешный инновационный кластер создает высокопроизводительные рабочие места, увеличивает валовой региональный продукт (ВРП) и налоговые поступления, что, в свою очередь, еще больше повышает бюджетную обеспеченность. Это цикл с положительной обратной связью.

Конечная цель таких проектов — переход от бюджетного финансирования к частным инвестициям и самостоятельному экономическому росту. Это возможно только на территории с изначально высоким потенциалом, где есть спрос на инновации и возможность их коммерциализации.

Для внедрения «умных» технологий в России наиболее привлекательными являются сферы, где преимущества их использования очевидны.

Искусственный интеллект в столичной системе видеонаблюдения помогает выявлять недочеты, оперативно передавать заявки и контролировать исполнение работ.

Минувшей зимой в Москве протестировали и внедрили три нейронные сети, которые находят на скриншотах с камер городского видеонаблюдения неочищенные дороги, а также сосульки, наледь и снег на крышах домов. За несколько месяцев нейросети помогли специалистам Центра автоматизированной фиксации административных правонарушений (ЦАФАП) выявить 15,5 тысячи подобных недочетов и передать информацию о них столичным службам. За прошедший сезон с помощью искусственного интеллекта исправили более 24,9 тысячи зимних недочетов [12].

**Стратегия умного города в Санкт-Петербурге**

Подход Санкт-Петербурга характеризуется большей фрагментарностью, но с акцентом на развитие наукоемких кластеров и точечные инновационные-проекты.

Внедряются «умные» светофоры, адаптирующиеся к потоку. Ведутся эксперименты с беспилотным общественным транспортом (например, проект беспилотного автобуса на острове Невская губа). Система анализа пассажиропотока на основе компьютерного зрения помогает оптимизировать графики движения общественного транспорта.

Также в 2024 году успешно ввели в работу робота, занимающегося проверкой оплаты штрафов за нарушение правил парковки. По мнению властей данное введение является инструментом повышения продуктивности обработки данных, а также оптимизации работы городской службы ГИБДД. Внедрение роботов произошло и в петербургском комитете по печати и взаимодействию со СМИ, такое решение позволило ускорить реагирование на обращения граждан.

В 2024 году служба 004 приняла 944,5 тысячи звонков и обработала 811,5 тысячи сообщений. Через портал «Наш Санкт-Петербург» решено больше полумиллиона вопросов ЖКХ, посещаемость сайта выросла на 14%. МФЦ приняли примерно 15 миллионов обращений. Среднее время ожидания составило 5 минут 4 секунды, а удовлетворённость качеством – 99,82% [8].

Правительством Санкт-Петербурга совместно с компанией «Сбер» было подписано соглашение о создании центра компетенций по искусственному интеллекту для городских органов власти.

В Санкт-Петербурге к концу 2024 года развернута крупная система городской безопасности, включающая более 102 тысяч камер во всех районах. Особое внимание уделяется защите детей: на детских площадках установлено около 1000 камер с видеоаналитикой, к 2025 году планируется добавить еще 1450. В 2023 году эта система помогла раскрыть свыше 4 тысяч преступлений, что на 70% больше, чем в 2022. Внедрение автоматического распознавания нелегальной торговли позволило снизить нагрузку на контролирующие органы [9].

На базе Технопарка «Ленполиграфмаш» и других инновационных центров развиваются стартапы в области ИИ, фокусирующиеся на компьютерном зрении для промышленности (контроль качества на производствах) и робототехнике. Это создает экосистему для генерации новых экономических моделей, основанных на ИИ.

Пилотные проекты по использованию ИИ для управления энергопотреблением в историческом центре города. Внедрение интеллектуальных систем для анализа туристических потоков и перенаправления их для снижения нагрузки на ключевые достопримечательности.

Как и в Москве, внедряются системы поддержки принятия врачебных решений на основе анализа медицинских изображений, однако масштаб внедрения несколько меньше.

Применение искусственного интеллекта в городах становится не просто ожиданием, а подтверждённым фактом. По информации от АО «Цифровая экономика» за 2024 год, внедрение нейросетей может заметно улучшить жизнь в крупных городах.

Помимо транспорта, ИИ положительно влияет на социальную сферу. Очереди в больницах могут стать короче на 30%, а потери из-за поломок и незапланированного ремонта городской инфраструктуры – снизиться на 65%. Данные показывают, что вложения в умные технологии напрямую связаны с большей безопасностью, экономией времени для жителей и оптимизацией бюджетных затрат.

В 2023 году российский рынок ИИ достиг 900 млрд рублей, показав рост на 37%. Ожидается, что в 2024 году он составит 1,48 трлн рублей, а в 2025 вырастет еще на 25–30%, достигнув 1,9 трлн рублей. Потенциал рынка цифровых решений для умных городов оценивается в 330-840 млрд рублей. Внедрение таких решений позволяет экономить 15–-30 минут на ежедневных поездках, снизить стоимость проживания до 3% и сократить расход воды на человека на 25-80 литров в день [10].

В Москве и Санкт-Петербурге ИИ улучшил безопасность и городские сервисы, повысив качество жизни. К 2028 году эффект от умных городов может превысить 20 триллионов долларов. Интеграция генеративного ИИ, биометрии и квантовых технологий создаст более комфортные и безопасные города [11].

Проведенный анализ позволяет сделать следующие выводы:

1. **Москва** демонстрирует модель «вертикальной интеграции», где городские власти выступают основным заказчиком и интегратором решений на основе ИИ. Это позволяет быстро масштабировать успешные практики на весь город и получать значительный синергетический эффект.
2. **Санкт-Петербург** развивается по модели «инновационного кластера», где роль властей сводится к созданию благоприятной среды для экспериментального бизнеса и научных групп. Это создает почву для генерации прорывных технологий, но затрудняет их быстрое масштабирование на весь город.
3. Оба мегаполиса успешно применяют ИИ в классических для «умного города» сферах: транспорт и здравоохранение. Однако Москва значительно преуспела в интеграции ИИ в повседневные городские процессы (ЖКХ, госуслуги).
4. Наиболее перспективным направлением является конвергенция двух моделей: создание централизованной платформы для данных и управления (опыт Москвы) с активным привлечением и акселерацией малого и среднего инновационного бизнеса (потенциал Петербурга).

## Заключение

Внедрение технологий искусственного интеллекта стало неотъемлемой частью стратегии развития Москвы и Санкт-Петербурга. Несмотря на различия в подходах, оба города добились значительных результатов в повышении эффективности экономических и управленческих процессов (таблица).

Таблица

**Экономические и управленческие процессы**

| Критерий | Москва | Санкт-Петербург |
|---|---|---|
| Общая стратегия и подход | Модель вертикальной интеграции: Централизованный, комплексный подход. Власти — главный заказчик и интегратор решений. Масштабирование успешных практик на весь город | Модель инновационного кластера: Децентрализованный, фрагментарный подход. Власти создают среду для бизнеса и научных групп. Акцент на точечные пилотные проекты и стартапы |
| Ключевые документы | «Умный город — 2030», «Цифровая столица», «Информационный город» | Стратегия социально-экономического развития до 2035 года |
| Транспорт | Единая интеллектуальная транспортная система (ИТС):<br>• Адаптивное управление светофорами (снижение загрузки магистралей на 15-20%)<br>• Анализ данных с камер и датчиков в реальном времени<br>• Интеграция с «Яндекс.Картами» для оптимизации маршрутов | Точечные проекты и эксперименты:<br>• «Умные» светофоры<br>• Эксперименты с беспилотным общественным транспортом<br>• Система анализа пассажиропотока |
| Здраво-охранение | Глобальная интеграция в единую систему (ЕМИАС):<br>• Система анализа медицинских изображений (рентген, КТ, МРТ) для помощи в диагностике<br>• Множество цифровых сервисов («Электронный рецепт», запись к врачу и др.)<br>• Компьютерное зрение для мониторинга масочного режима во время пандемии | Внедрение систем поддержки врачебных решений, но в меньшем масштабе по сравнению с Москвой |
| Городское управление и ЖКХ | Цифровое правительство:<br>• Платформа «Цифровой двойник» для моделирования и управления<br>• AI-чаты в системе госуслуг (МАС)<br>• Компьютерное зрение для мониторинга дворов, свалок, парковок | Развитие цифровых сервисов:<br>• Портал «Наш Санкт-Петербург» (решение вопросов ЖКХ)<br>• Робот для проверки оплаты штрафов за парковку<br>• Роботы для обработки обращений граждан (напр., в Комитете по печати) |
| Безопасность | Крупная система видеонаблюдения с видеоаналитикой:<br>В Москве более 270 тысяч камер наблюдения. Из них 113 тысяч подключены к системе распознавания лиц | Крупная система видеонаблюдения с видеоаналитикой:<br>• Более 102 тыс. камер<br>• Распознавание нелегальной торговли<br>• Камеры на детских площадках (около 1000) |
| Экономика и инновации | Создание условий для ведения «умного» бизнеса:<br>• Предиктивная аналитика в ритейле<br>• Активное внедрение в строительство и ЖКХ (22 проекта) | Развитие наукоемких кластеров:<br>• Центр компетенций по ИИ с «Сбером»<br>• Стартапы в технопарках (компьютерное зрение для промышленности, робототехника) |
| Уникальные особенности | • Высокая степень интеграции ИИ в повседневную жизнь горожан<br>• Быстрое масштабирование проектов<br>• Ориентация на массовые городские сервисы | • Акцент на генерацию инноваций и нишевых технологических решений<br>• Пилотные проекты в сфере энергоменеджмента и управления туристическими потоками<br>• Сильная ориентация на научно-промышленный потенциал |

Стремительное накопление объема данных в различных областях человеческой деятельности в начале XXI в. стало главным фактором, определившим развитие технологии ИИ. Это дает возможность значительно увеличить эффективность публичного управления.

На основе проведенного анализа можно сделать вывод, что использование технологий искусственного интеллекта (ИИ) является важным фактором для достижения необходимых показателей эффективности во многих сферах городского управления.

Опыт мегаполисов показывает, что успешная цифровая трансформация требует не только технологических решений, но и выверенной стратегии, адаптированной к специфике городской экономики и институциональной среды. Дальнейшее развитие будет связано с преодолением вызовов, связанных с защитой данных, этическим регулированием ИИ и необходимостью подготовки кадров для цифровой экономики. Синтез московской модели масштабирования и питерской модели генерации инноваций может стать оптимальным путем для создания устойчивой и Smart City-экосистемы российского образца.

**Литература**


1. Указ Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».
2. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утверждена Указом Президента РФ № 490).
3. Государственная программа города Москвы «Цифровая столица» (постановление Правительства Москвы от 22.10.2021).
4. Стратегия социально-экономического развития Санкт-Петербурга на период до 2035 года. – Комитет по экономической политике и стратегическому планированию Санкт-Петербурга.
5. Паспорт национального проекта «Цифровая экономика Российской Федерации» (утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).
6. Иванов А.В., Петрова С.М. Искусственный интеллект как инструмент управления транспортными потоками мегаполиса (на примере Москвы) // «Экономика и управление народным хозяйством». 2022. № 5. С. 45–58.
7. Смирнов К.Л., Федорова Е.А. Сравнительный анализ моделей внедрения технологий «умного города» в Москве и Санкт-Петербурге // «Государственное управление. Электронный вестник». 2023. Вып. 95. С. 120–145.
8. 360 тысяч обращений поступило на портал «Наш Санкт-Петербург» за полгода [Электронный ресурс]. Режим доступа: https://районы.рф/2025/07/23/360-tisyach-obrashchenii-postupilo-na-portal-nash-sanktpeterburg-za-polgoda (дата обращения 09.09.2025).
9. На 46 детских площадках Петербурга установили видеонаблюдение [Электронный ресурс]. Режим доступа: https://районы.рф/2024/09/26/na-46-detskikh-ploshchadkakh-peterburga-ustanovili-videonablyudenie (дата обращения 09.09.2025).
10. Российский рынок ИИ в 2023 году достиг 900 млрд руб., годовой рост составил 37% [Электронный ресурс]. Режим доступа: https://ict.moscow/projects/ai/news/3983/ (дата обращения 09.09.2025).
11. Тренды умных городов за 2024 год [Электронный ресурс]. Режим доступа: https://ict.moscow/news/smart-city-2024/ (дата обращения: 09.09.2025).
12. В Москве протестировали три нейросети, которые помогают коммунальным службам [Электронный ресурс]. Режим доступа: https://www.mos.ru/news/item/137211073/ (дата обращения 09.09.2025).

УДК 004.8

# ИННОВАЦИИ В УРБАНИСТИКЕ: АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ ДВОРОВЫХ ТЕРРИТОРИЙ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Скуратова Н.Б.**[1] (студент)
**Научный руководитель – кандидат экономических наук, доцент Година О.В.**[1]
[1]СКФУ
ab_torgi@mail.ru

**Аннотация**
В работе рассматриваются вопросы автоматизации проектирования дворовых территорий многоквартирных домов в России на примере предлагаемой web-платформы ideidvora.online, интегрирующей алгоритмы искусственного интеллекта для генерации генерального плана, подбора решений из библиотеки шаблонов, расчета сметы и подготовки юридической документации. Результаты исследования позволяют позиционировать платформу как масштабируемый инструмент цифровизации благоустройства дворовых территорий в российских условиях.

**Ключевые слова**
Искусственный интеллект; автоматизация проектирования; благоустройство дворов; многоквартирные дома; урбанистика; цифровизация городской среды.

Благоустройство дворовых территорий многоквартирных домов является важным направлением развития городской среды России. Однако значительная часть дворов, особенно в жилом фонде советской застройки, остается неудовлетворительной. Устаревшие игровые площадки, разрушенные покрытия и дефицит зеленых зон снижают качество жизни населения. В целом такая ситуация противоречит принципам устойчивого развития урбанистики.

Традиционные методы проектирования дворовых пространств характеризуются высокой стоимостью, длительными сроками и слабой вовлеченностью жителей. Ключевым барьером является отсутствие доступных цифровых инструментов, которые позволяли бы собственникам жилья и управляющим организациям самостоятельно инициировать, формировать и контролировать проекты благоустройства. При этом мировая практика показывает, что искусственный интеллект способен радикально изменить подход к урбанистике: автоматизация рутинных процессов, использование больших данных и интеграция параметрических моделей позволяют формировать более гибкие сценарии городского развития. Для России данный подход особенно актуален, поскольку нормативная база (СНиПы, СанПиНы) строго регламентирует требования к благоустройству и требует их точного соблюдения.

Целью настоящего исследования является изучение возможностей применения искусственного интеллекта для автоматизации проектирования дворов и придворовых территорий на примере web-платформы ideidvora.online.

Объектом исследования выступают процессы проектирования дворовых и придворовых территорий многоквартирных домов в России, а предметом – архитектура web-платформы ideidvora.online, основанная на алгоритмах искусственного интеллекта.

Методологическая база исследования включает системный анализ практик благоустройства и выявление барьеров их реализации, алгоритмическое моделирование для автоматизации ключевых этапов проектирования (генерация генплана, использование библиотеки шаблонов, расчет сметы, формирование юридической документации), а также сравнительный анализ с традиционными коммерческими решениями для оценки экономической эффективности. Эмпирическая апробация платформы проведена на примере дворовой территории МКД «Нефтестрой» в г. Ставрополе, что позволило проверить работоспособность алгоритмов в реальных условиях.

Современная практика благоустройства дворовых территорий в России характеризуется рядом системных проблем: высокая стоимость проектных работ, длительные сроки подготовки документации и низкая вовлеченность жителей в процесс принятия решений. Как

отмечают отечественные исследователи [1– ограничиваясь геоинформационными системами и разрозненными маркетплейсами строительных услуг, и не обеспечивают комплексного охвата. Так, в исследовании [1] указывает, что внедрение информационных решений в благоустройство ограничивается локальными инициативами и не выходит на уровень массового применения. Анализ, проведенный в работе [2], подтверждает, что на российском рынке отсутствуют комплексные цифровые инструменты, объединяющие проектирование, составление смет и юридическую поддержку. При этом социальный барьер – низкая вовлеченность жителей – остается одной из главных проблем реализации программ благоустройства [3].

В мировой практике наблюдается тренд на активное внедрение искусственного интеллекта (ИИ) в задачи урбанистики и проектирования. Классические работы по цифровизации городов [5] заложили теоретическую основу «науки о городах», а современные исследования показывают, что ИИ способен формировать новые модели управления городской средой за счет анализа больших данных и автоматизированного принятия проектных решений. Зарубежные примеры включают проекты «умные дворы» (smart-courtyard) в Китае [6] и «дизайн, ориентированный на общество» (community-driven design) в Европе, где жители участвуют в планировании через цифровые платформы [7]. Современные обзоры [7, 8] подчеркивают, что перспективность ИИ в урбанистике связана именно с автоматизацией рутинных процессов – от анализа параметров участка до подбора оптимальных решений – и снижением транзакционных издержек.

На этом фоне разработка web-платформы ideidvora.online демонстрирует уникальное решение для российских реалий. Web-платформа ideidvora.online представляет собой цифровую систему нового поколения для автоматизированного проектирования благоустройства дворовых и придворовых территорий многоквартирных домов. В отличие от существующих коммерческих архитектурных услуг, платформа ориентирована на массовый сегмент и учитывает не только нормативные требования (СНиП, СанПиН), но и запросы конечных пользователей – собственников жилья и управляющих компаний. На сегодняшний день в России отсутствуют аналоги, способные обеспечить автоматическую генерацию проектов дворового благоустройства в едином окне с функциями сметного расчета и юридического сопровождения. Предлагаемая нами система объединяет в едином цифровом пространстве:

- автоматическую генерацию генерального плана на основе фото или кадастровой схемы с учетом нормативных ограничений (СНиП, СанПиН);
- библиотеку шаблонов благоустройства (детские площадки, спортивные зоны, озеленение, малые архитектурные формы), которые могут быть кастомизированы под запросы жителей;
- модуль предварительной сметы, обеспечивающий прозрачность и прогнозируемость бюджета;
- юридический блок, позволяющий готовить заявки в государственные программы («Комфортная городская среда»).

Искусственный интеллект в платформе ideidvora.online выполняет функцию «интеллектуального посредника» между исходными данными о дворовой территории и итоговым проектным решением. На первом этапе система использует алгоритмы компьютерного зрения и пространственного анализа для обработки загруженных пользователем данных – фотографии участка или кадастровой схемы. Это позволяет автоматически определить границы территории, выделить существующие элементы (дорожки, зеленые зоны, парковочные места) и зафиксировать параметры участка: площадь, конфигурацию, рельеф, ориентацию по сторонам света. Затем в работу включается модуль генерации генерального плана. Здесь искусственный интеллект сопоставляет выявленные параметры с нормативными требованиями и распределяет территорию на функциональные зоны: детские, спортивные, рекреационные или хозяйственные. При этом система сразу проверяет корректность решений, например, при формировании детской площадки автоматически учитывается требование СНиП 2.07.01-89 о минимальной площади – не менее

6 м² на одного ребенка, рассчитанного исходя из демографической статистики дома. Если проектируемая площадь меньше нормы, алгоритм либо предлагает увеличить ее за счет перераспределения пространства, либо сигнализирует о нарушении. Дополнительно встроен модуль согласования с санитарными нормами. Так, на основе СанПиН 2.1.2.2645-10 система автоматически добавляет озелененные буферные зоны для защиты от шума и пыли, размещая деревья и кустарники вдоль автомобильных проездов. Таким образом, ИИ не просто предлагает готовые решения, а формирует проект, изначально соответствующий действующему законодательству.

На следующем этапе алгоритмы эвристического поиска подбирают из библиотеки шаблонов оптимальные элементы благоустройства (например, варианты спортивных площадок или детских комплексов), которые пользователь может кастомизировать. Возможность кастомизации позволяет адаптировать проект к локальным условиям и предпочтениям жителей. Все изменения в реальном времени проверяются на предмет соблюдения нормативов и пересчитываются в сметном модуле. Встроенный модуль предварительной сметы рассчитывает стоимость проекта в зависимости от площади, выбранных материалов и элементов, что делает процесс более прозрачным и доступным для инициативных групп и ТСЖ.

Благодаря такой логике работы искусственный интеллект обеспечивает двусторонний эффект, с одной стороны, автоматизация снимает рутинную нагрузку с проектировщиков, а с другой – гарантирует нормативную корректность решений еще на стадии проектирования, что минимизирует риск отклонений при согласовании и реализации проекта.

Апробация платформы на примере двора «Нефтестрой» в г. Ставрополе подтвердила ее практическую применимость. Алгоритмы ИИ автоматически выделили четыре функциональные зоны (входная, спортивно-игровая, рекреационная и творческая), сохранив при этом существующие зеленые насаждения и пешеходные маршруты. Это подтверждает способность системы адаптироваться к локальным условиям и формировать эргономичные решения.

Сравнительный анализ с традиционными проектными услугами (таблица) показывает, что использование платформы позволяет снизить стоимость разработки в 3–5 раз и сократить сроки проектирования с нескольких месяцев до нескольких дней. Такой эффект согласуется с зарубежными результатами, где применение ИИ в архитектуре и урбанистике демонстрирует аналогичное сокращение транзакционных издержек и рост вовлеченности пользователей, а также с другими российскими исследованиями, выделяющими необходимость проектирования с учетом специфики локальных сообществ и ограниченных ресурсов [3].

Таблица

**Сравнение традиционного и автоматизированного проектирования дворовых территорий**

| Параметр | Традиционный проект | Web-платформа ideidvora.online | Эффект |
|---|---|---|---|
| Сроки разработки | 2–4 месяца | 3–7 дней | ↓ в 10–20 раз |
| Стоимость проектирования | 100–500 тыс. руб. | 40–100 тыс. руб. | ↓ в 3–5 раз |
| Проверка нормативов | Выполняется вручную | Автоматически встроена в алгоритм | + качество |
| Участие жителей | Ограничено (опросы, собрания) | Онлайн-кастомизация и выбор решений | ↑ вовлеченность |

Таким образом, ideidvora.online можно рассматривать как первый в России пример масштабируемого инструмента, формирующего новый стандарт цифрового проектирования дворовых территорий. Его потенциал заключается в сочетании нормативной корректности, возможностей искусственного интеллекта, принципов урбанистического дизайна, экономической эффективности и социальной вовлеченности – факторов, которые в

совокупности определяют успешность цифровизации городской среды и позволяют заложить основу для дальнейшего развития технологий «умного города».

Проведенное исследование подтвердило эффективность применения ИИ для автоматизации проектирования дворовых территорий. Платформа ideidvora.online демонстрирует, что комплексная автоматизация рутинных этапов позволяет резко сократить сроки и стоимость проектирования, обеспечивая при этом соответствие нормативам и вовлечение жителей. Научная новизна работы заключается в интеграции алгоритмов ИИ с российскими нормативными документами (СНиП, СанПиН). Практическая значимость выражается в создании воспроизводимого цифрового конвейера проектирования, адаптированного к условиям массового благоустройства.

В дальнейшем развитие платформы может быть связано с внедрением модулей «умного города» – интеллектуального освещения, систем мониторинга и экологических датчиков. Это позволит перейти от проектирования к управлению жизненным циклом дворовых территорий.

**Литература**


1. Иванов М.А., Сушанский А.С. Использование цифровых технологий в деятельности Управы района Марьино по благоустройству дворовых территорий // Гос Рег. 2021. №. 2(36). С. 73–80.
2. Селиванов С.А., Куликова Е.С. Анализ цифровых технологий в сфере благоустройства территорий // Умная цифровая экономика. 2022. №. 4. С. 79–82.
3. Краснов И.В. Анализ благоустройства дворовых территорий России // Современное строительство и архитектура. 2023. №. 12(43) [Электронный ресурс]. Режим доступа: https://modern-construction.ru/archive/12-43-2023-december/10.18454/mca.2023.43.1 (дата обращения 05.09.2025).
4. Миркушина Л.Р. Российская урбанистика и вызовы современности: нейронные сети в дискурсе цифрового города // Современная наука и инновации. 2023. №. 3. С. 208–214.
5. Batty M. The New Science of Cities. – Cambridge, MA: MIT Press, 2013. 520 p.
6. Gao J., Xu H., Dao L. Multi-Generative Agent Collective Decision-Making in Urban Planning: A Case Study for Kendall Square Renovation // arXiv:2402.11314. 2024 [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2402.11314 (дата обращения 05.09.2025).
7. Yigitcanlar T., Kamruzzaman M., Buys L., Ioppolo G., Sabatini Marques J., Costa M.E., Yun J.H.J. Understanding "smart cities": intertwining development drivers with desired outcomes in a multidimensional framework // Cities. 2018. V. 81. Pp. 145–160.
8. He W., Chen M. Advancing Urban Life: A Systematic Review of Emerging Technologies and Artificial Intelligence in Urban Design and Planning // Buildings. 2024. V. 14. №. 3. P. 835.

УДК 004.8:004.942

# ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И РАЗВИТИЯ ИСПОЛЬЗОВАНИЯ VIBE CODING В РУССКОЯЗЫЧНОМ СЕГМЕНТЕ

**Файзиев Ф.Р.**[1] (студент)
**Научный руководитель – Юшков Е.Ю.**[1]
[1]Университет ИТМО
frfayziev@itmo.ru

**Аннотация**
В докладе рассматривается феномен vibe coding — инновационного подхода к программной разработке, предполагающего делегирование генерации кода системам искусственного интеллекта на основе вербального описания задачи. Анализируются ключевые тенденции распространения технологии на мировом и российском рынках: зафиксирован рост востребованности навыка vibe coding на 27 % с начала 2025 года, а также появление отечественных аналогов (в том числе решений от Яндекса и Сбера). Освещаются преимущества технологии (ускорение разработки, снижение затрат, демократизация доступа в IT) и сопряжённые с ней риски (избыточность кода, уязвимости, ослабление профессиональных навыков). В заключение подчёркивается двойственная природа vibe coding как инструмента, одновременно повышающего производительность и порождающего новые вызовы для индустрии.

**Ключевые слова**
Vibe coding, искусственный интеллект, мультимодельная ИИ-архитектура.

## Введение

В последние годы как мировой, так и российский рынок информационных технологий демонстрирует интенсивное освоение Vibe coding (вайб-кодинга) — инновационного подхода к программной разработке, предполагающего делегирование генерации исходного кода системам искусственного интеллекта (ИИ) на основе вербального описания задачи со стороны разработчика [1, 2], что наглядно отражает масштаб интереса к этой технологии в профессиональном и общественном пространстве. Словарь английского языка Collins назвал «вайбкодинг» (англ. vibe coding) словом 2025 года [3].

## Эмпирические данные о распространённости технологии

Согласно аналитическим данным, с начала 2025 года наблюдается существенный рост востребованности навыка Vibe coding на рынке труда. Количественный анализ вакансий выявил увеличение частоты упоминаний данного термина компетенции на 27% в сравнении с предшествующим периодом [4]. Эта динамика отражает фундаментальную трансформацию требований к квалификации IT-специалистов и свидетельствует о постепенной институционализации Vibe coding как стандартного элемента профессионального профиля разработчика.

## Преимущества технологии

Эксперты отрасли выделяют следующие положительные эффекты внедрения Vibe coding:

- ускорение процесса разработки — сокращение временных затрат на написание рутинного кода, исправления ошибок, тестирования и отладки кода;
- сокращение временных и финансовых затрат на запуск проекта. Это особенно актуально для стартапов и начальных этапов проектов, когда ресурсы ограничены, а техническая команда отсутствует [5];
- снижение порога входа в профессию в сфере IT — Vibe coding дает возможность принятия участия в проектах молодых специалистов с базовым уровнем программирования при условии владения навыками формулировки технических заданий для ИИ.

Все эти эффекты дают возможность повышения эффективности труда и возможности развития творческого потенциала разработчиков при создании кода.

**Потенциальные риски и ограничения**

Вместе с тем применение технологии сопряжено с рядом существенных недостатков:

- увеличение ресурсоёмкости кода — генерируемые ИИ решения зачастую характеризуются избыточностью конструкций и неоптимальным использованием вычислительных ресурсов;
- можно назвать вытекающим из первого недостатка второй: трудности с отладкой и устранением проблем, созданного с помощью технологий ИИ;
- рост уязвимости программных продуктов — повышенный риск возникновения уязвимостей вследствие недостаточного контроля за логикой сгенерированного кода и возможных ошибок в моделях ИИ;
- ослабление уровня навыков программирования у разработчиков. Увеличение использование делегирования процесса написания кодов приводит к уменьшению практических навыков и наработки опыта, а также понимаю ошибок систем.

Изучение специализированных форумов и площадок русскоязычного интернета показывает, что разработчик из России и стран СНГ также активно использую данный продукт в своих проектах [6–10]. Это можно объяснить легкой доступностью сервиса, относительной простой использования и возможностью получить быстрые результаты, что является крайне востребованным в современном мире.

Российские гиганты, такие как Яндекс, Сбер разработали собственные платформы, функционирующие по аналогии с технологией Vibe coding.

Среди доступных российским разработчикам сервисов можно отметить:

1. Cursor [11]. Программа представляет собой специализированную интегрированную среду разработки (IDE — integrated development environment), ориентированную на оптимизацию процесса написания исходного кода программ с точки зрения скорости и эффективности.

   В основе функциональности Cursor лежит модель GPT-4. Среда позволяет:

   - генерировать программный код на широком спектре поддерживаемых языков программирования (включая Python, JavaScript/TypeScript, Swift, C, Rust и др.);
   - выявлять и устранять ошибки в существующем коде;
   - получать развёрнутые пояснения к любым фрагментам разрабатываемого программного обеспечения.

   Кроме базовых возможностей, Cursor предоставляет ряд расширенных функций:

   - интеллектуальное автодополнение кода;
   - автоматизированную генерацию сопроводительной документации (в том числе файлов README);
   - инструменты Multi-Edits и Smart Rewrites, предназначенные для ускоренного рефакторинга кода.
2. GitHub Copilot [12]. Программный инструмент, разработанный компанией GitHub (оператором одноимённого хостинга IT-проектов), реализующий концепцию интеллектуальной поддержки процесса программирования.

Функционирование сервиса базируется на комплексе современных моделей искусственного интеллекта. В технологическом стеке задействованы:

- модели семейства GPT (GPT-4o, GPT-4.1, GPT-4.5);
- модели серии o (o1, o3, o3-mini, o4-mini);
- Claude 3.5 Sonnet и Claude 3.7 Sonnet;
- Gemini 2.0 Flash и Gemini 2.5 Pro.

При этом инструмент обеспечивает мультиплатформенную поддержку за счёт интеграции с популярными средами разработки таких, как Visual Studio Code (VS Code) и IDE-решениями JetBrains.

Сервис предоставляет две ключевые функции: интеллектуальное автодополнение (прогнозирование и дописывание строк кода на основе контекста) и генерация программного кода (создание функций и структурных блоков программы по текстовым запросам

пользователя). И имеет доступ к репозиториям — интеграция с библиотеками и шаблонами кода для ускорения разработки.

Таким образом, GitHub Copilot представляет собой масштабируемое решение для автоматизации программирования, сочетающее мультимодельную ИИ-архитектуру с гибкой системой доступа и интеграции.

Дополнительным индикатором распространения технологии служит рост образовательных программ:

- число онлайн-курсов по Vibe coding увеличилось на 45% с начала 2025 года (по данным платформы GetCourse);
- 18 ведущих технических университетов включили модуль по ИИ-генерации кода в программы бакалавриата;
- объём инвестиций в EdTech-стартапы, фокусирующиеся на обучении Vibe coding, достиг $210 млн за первое полугодие 2025 года.

Совокупность этих данных позволяет утверждать, что вайб-кодинг переходит из категории экспериментальных практик в разряд стандартизированных инструментов разработки. Однако гетерогенность показателей по отраслям и регионам указывает на неравномерность процесса адаптации технологии, требующую дальнейшего мониторинга и анализа.

**Заключение**

Таким образом, Vibe coding представляет собой двуединый феномен: с одной стороны, он способствует демократизации IT-разработки и повышению производительности, с другой — порождает новые вызовы в области качества и безопасности программного обеспечения. Дальнейшее развитие технологии требует системного исследования её долгосрочных последствий для индустрии, а также изучения возможных рисков.

**Литература**


1. Will the future of software development run on vibes? [Электронный ресурс]. Режим доступа: https://arstechnica.com/ai/2025/03/is-vibe-coding-with-ai-gnarly-or-reckless-maybe-some-of-both/ (дата обращения 05.11.2025).
2. Tihanyi N., Bisztray T., Ferrag, M.A., Jain R., Cordeiro L.C. How secure is AI-generated Code: A Large-Scale Comparison of Large Language Models. 2024. arXiv:2404.18353.
3. Вайб-кодинг: новый тренд в программировании или забава разработчиков [Электронный ресурс]. Режим доступа: https://trends.rbc.ru/trends/industry/6800e2f19a79473690efda30 (дата обращения 07.11.2025).
4. Коммерсантъ: Максим Тятюшев о вайб-кодинге [Электронный ресурс]. Режим доступа: https://platformv.sbertech.ru/blog/kommersant-maksim-tyatyushev-o-vajb-kodinge (дата обращения 07.11.2025).
5. Взрывной рост ИИ-разработки: как вайб-кодинг меняет программирование [Электронный ресурс]. Режим доступа: https://companies.rbc.ru/news/FCbfsHIMwO/vzryivnoj-rost-ii-razrabotki-kak-vajb-koding-menyaet-programmirovanie/ (дата обращения 07.11.2025).
6. Почему разработчики не доверяют вайб-кодингу и как это исправить [Электронный ресурс]. Режим доступа: https://habr.com/en/companies/cloud_ru/articles/959876/ (дата обращения 07.11.2025).
7. Вайб кодинг (Vibe coding) [Электронный ресурс]. Режим доступа: https://www.linux.org.ru/forum/talks/18128064 (дата обращения 07.11.2025).
8. Вайб-кодинг в 1С или "еще год два и программисты будут не нужны....." [Электронный ресурс]. Режим доступа: https://forum.mista.ru/topic/899842 (дата обращения 07.11.2025).
9. "Вайб-кодинг и замена программистов на AI" [Электронный ресурс]. Режим доступа: https://www.opennet.ru/openforum/vsluhforumID9/10492.html (дата обращения 07.11.2025).
10. Взрывной рост ИИ-разработки: как вайб-кодинг меняет программирование [Электронный ресурс]. Режим доступа: https://companies.rbc.ru/news/FCbfsHIMwO/vzryivnoj-rost-ii-razrabotki-kak-vajb-koding-menyaet-programmirovanie/ (дата обращения 07.11.2025).
11. Cursor [Электронный ресурс]. Режим доступа: https://cursor.com/?roistat_visit=6407457 (дата обращения 07.11.2025).
12. GitHub Copilot [Электронный ресурс]. Режим доступа: https://github.com/features/copilot?roistat_visit=6407457 (дата обращения 07.11.2025).

УДК 577

# АНАЛИЗ НЕЦЕЛЕВОЙ АКТИВНОСТИ СИСТЕМЫ ГЕНОМНОГО РЕДАКТИРОВАНИЯ CRISPR/CAS9 НА МОДЕЛИ ДРОЖЖЕЙ *SACCHAROMYCES CEREVISIAE*

**Девяткин Д.М.**[1] (аспирант), **Шумега А.Р.**[1] (научный сотрудник)
**Научный руководитель – кандидат биологических наук Степченкова Е.И.**[1]
[1]СПбГУ
dimi02121@gmail.com

**Аннотация**
Одним из главных препятствий для широкого применения систем редактирования CRISPR/Cas9 в медицине является риск возникновения нежелательных мутаций в геноме вследствие нецелевой активности редактирующего комплекса. Разработка чувствительной тест-системы для оценки нецелевой активности является важной задачей на пути к широкому применению системы CRISPR/Cas9 в практической сфере. Наша работа посвящена разработке такой тест-системы на основе модельного организма – дрожжей Saccharomyces cerevisiae. С помощью разработанной тест-системы нам удалось оценить влияние неспаренностей между сайтом-мишенью и гидовой РНК, а также влияние последовательности сайта PAM на уровень нецелевой активности CRISPR/Cas9.
**Ключевые слова**
CRISPR/Cas9, нецелевая активность, геномное редактирование, Saccharomyces cerevisiae, генотоксичность.

## Введение

Открытие у бактерий системы адаптивного иммунитета CRISPR/Cas9 произвело революцию в геномном редактировании благодаря разработке на ее основе простых и эффективных инструментов для внесения направленных изменений генетического материала. Редактирующий комплекс состоит из эндонуклеазы Cas9 и молекулы single guide RNA (sgRNA), содержащей последовательность гидовой РНК. Гидовая РНК длиной 20 нуклеотидов, комплементарно связывается с мишенью в геноме, направляя таким образом Cas9 к месту редактирования. Для связывания редактирующего комплекса с мишенью необходимо, чтобы к ней примыкал короткий мотив PAM с последовательностью NGG. Редактирование целевого гена происходит в результате мутагенной репарации ДНК с двунитевым разрывом, внесенным комплексом Cas9/sgRNA. Система CRISPR/Cas9 широко используется в фундаментальных исследованиях, однако её практическое применение, особенно в области генной терапии, ограничено тем, что такие системы обладают нецелевой активностью, или способностью вносить разрывы ДНК сайтах, сходных по последовательности с целевым [1].

Актуальной задачей является изучение факторов, влияющих на уровень нецелевой активности sgRNA/Cas9. Проведение таких исследований с использованием организмов со сложными геномами требует значительных ресурсов, а эксперименты *in vitro* не учитывают все то многообразие факторов, которые присутствуют в живых клетках. Решением этой проблемы может стать разработка тест-системы на основе дрожжей *Saccharomyces cerevisiae*, использование которых позволяет работать с большими выборками *in vivo*.

## Результаты и обсуждение

На первом этапе выполнения работы мы разработали тест-систему для оценки эффективности редактирующего комплекса, которая основана на оценке токсичности двуцепочечных разрывов, вносимых эндонуклеазой Cas9 в ходе редактирования. С двуцепочечным разрывом связываются специальные киназы, которые сигнализируют о повреждении ДНК и могут вызывать как остановку клеточного цикла, так и клеточную гибель [2]. Чем выше частота индукции двуцепочечных разрывов в геноме, тем выше вероятность гибели клетки. Таким образом, если комплекс Cas9/sgRNA эффективно связывается с сайтом-мишенью и вносит в него двуцепочечный разрыв, то клетка, скорее

всего, не выживет. В то же время, если комплекс по тем или иным причинам имеет низкую активность, он практически не будет влиять на жизнеспособность клеток [3].

Для доставки редактирующего комплекса Cas9/sgRNA в дрожжевые клетки мы использовали плазмиды, сконструированные на основе pML107-GAL1. Плазмида pML107-GAL1 была получена на основе плазмиды pML107 [4] путем замены промотора *GAP* на промотор гена *GAL1*. Таким образом, продукция Cas9 в дрожжах, трансформированных плазмидой pML107-GAL1, запускается при добавлении в среду галактозы. Также pML107-GAL1 имеет сайт для встраивания в нее последовательности, кодирующей гидовую РНК. В качестве сайта-мишени мы выбрали 20-нуклеотидную последовательность в гене *URA3* (**GATTGGTTGATTATGACACC**CGG, мишень выделена жирным шрифтом, PAM — подчеркнут).

Для количественной оценки активности Cas9/sgRNA в дрожжевых клетках мы использовали следующий протокол (рис. 1). Дрожжи трансформировали плазмидой, кодирующей белок Cas9 и sgRNA. Равные аликвоты суспензии клеток дрожжей из одной реакции трансформации высевали на чашку без лейцина с глюкозой (MD) и чашку без лейцина с галактозой (MG). Трансформантов инкубировали 5 дней в термостате при 30°C, затем подсчитывали число колоний, выросших на каждой чашке. Относительную эффективность трансформации (ОЭТ) определяли как отношение числа колоний, выросших на среде MG, к числу колоний на среде MD, умноженное на 100%. По снижению относительной эффективности трансформации на среде MG судили об эффективности Cas9/sgRNA.

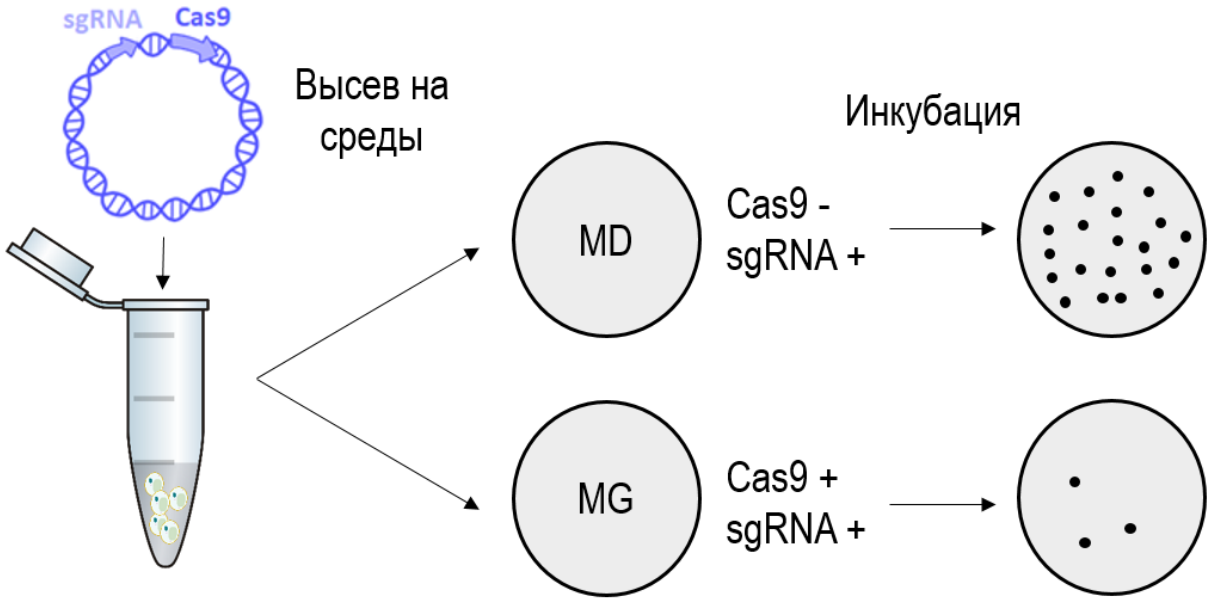



Рис. 1. Тест-система для оценки активности CRISPR/Cas9 в дрожжевых клетках *Saccharomyces cerevisiae*

Вторым этапом работы стала проверка чувствительности разработанной нами тест-системы. Для этого мы измерили относительную эффективность трансформации клеток дрожжей двумя плазмидами: pML107-GAL1 (кодирует только Cas9) и pML107-GAL1-sgRNA (кодирует как Cas9, так и sgRNA). Результаты представлены на рисунке 2. Из графика следует, что одновременная продукция Cas9 и sgRNA в дрожжевых клетках приводит к значительному снижению выживаемости трансформантов из-за высокой частоты двуцепочечных, что выражается чрезвычайно низкой относительной эффективностью трансформации (5–10%). В то же время, продукция только Cas9 не снижает количество трансформантов, вырастающих на среде MG, поскольку Cas9 без sgRNA не вносит двуцепочечные разрывы. В этом случае ОЭТ находится в районе 100%. Таким образом, измеряя ОЭТ мы можем делать выводы об активности Cas9/sgRNA в клетках.

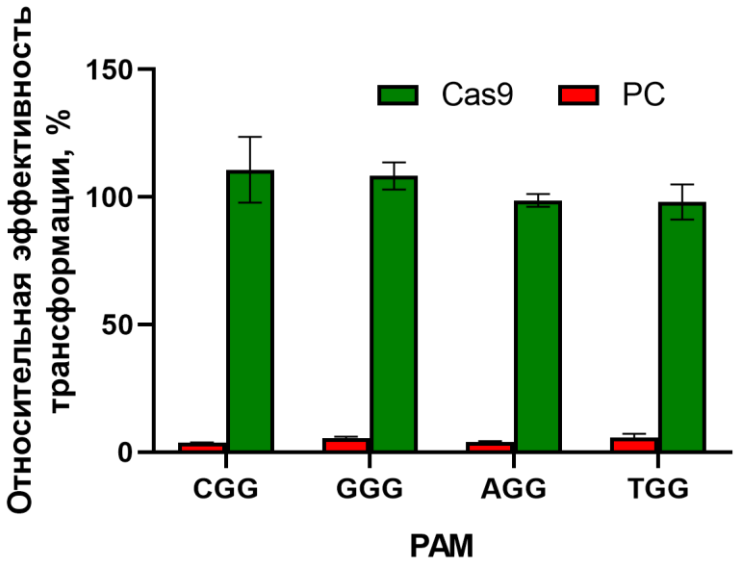



Рис. 2. Апробация разработанной тест-системы с использованием 4 изогенных штаммов дрожжей, отличающихся первым нуклеотидом мотива PAM (CGG, GGG, AGG, TGG)

Убедившись в высокой чувствительности разработанной тест-системы на третьем этапе работы мы оценили влияние одиночных неспаренностей между целевым сайтом в геноме и последовательностью гидовой РНК на эффективность внесения двуцепочечного разрыва эндонуклеазой Cas9. В отличие от традиционных подходов, где нецелевая активность оценивается в разных локусах генома, мы предлагаем использовать одну мишень и набор частично некомплементарных гидовых РНК. Это позволяет изучить влияние только одного параметра — числа и позиции несовпадений в последовательности гидовой РНК, исключив побочные факторы, такие как статус хроматина или транскрипционная активность в различных локусах генома.

На основе pML107-GAL1 мы получили библиотеку плазмид, кодирующих sgRNA с однонуклеотидными заменами во всех 20 позициях. Нуклеотиды в каждом положении мы заменяли на комплементарный, получив таким образом 20 плазмид: C1G, C2G… Для каждой плазмиды с помощью разработанной тест-системы мы измерили ОЭТ. На основе полученных результатов, мы разделили позиции замен по классам, в зависимости от степени влияния на показатель ОЭТ (таблица).

Таблица

**Относительная эффективность трансформации плазмидами, содержащими одиночные замены в последовательности гидовой РНК**

| Класс | Относительная эффективность трансформации | Позиции гидовой РНК (относительно PAM) |
|---|---|---|
| I | До 10% | 20, 19 |
| II | 10–40% | 18 |
| III | 40–70% | 1, 2, 3, 4, 5, 6, 11, 13, 14, 17 |
| IV | 70–100% | 7, 8, 9, 10, 12, 15, 16 |

Замены в наиболее дистальных позициях гидовой РНК - 20 и 19 не приводят к возрастанию ОЭТ по сравнению с положительным контролем (pML107-GAL-sgRNA), что говорит об отсутствии влияния неспаренностей в этой области на активность Cas9/sgRNA. Неспаренность в 18-ой позиции лишь немного снижает активность редактирующего комплекса, несоответствия в позициях 1-6, 11, 13, 14, 17 — умеренно, а замены в позициях 7-10, 12, 15, 16 практически инактивируют Cas9/sgRNA, поскольку ОЭТ для

соответствующих плазмид приближается к значению, полученному для плазмиды pML107-GAL1.

Ранее было показано [5, 6], что только первые 10 нуклеотидов (seed-область) критически важны для связывания эндонуклеазы Cas9 с сайтом-мишенью, в то время как остальные 10 дистальных нуклеотидов практически не оказывают влияния на активность редактирующего комплекса. Однако по нашим данным влияние разных позиций на активность редактирующего комплекса имеет более сложный профиль. Разработанная нами тест-система *in vivo* позволила разделить seed-область и дистальную область гидовой РНК на несколько зон в зависимости от их функциональной значимости.

На следующем этапе работы с использованием изогенных штаммов дрожжей, несущих различные PAM вблизи целевого сайта, мы проверили влияние первого нуклеотида этого мотива на активность Cas9 при наличии несоответствий между целевым сайтом и гидовой РНК (рис. 3). Оказалось, что последовательность PAM влияет на эффективность Cas9 в при наличии неспаренностей в некоторых позициях (13, 15), но не при полном соответствии гидовой РНК целевому сайту. Вероятно, при полной комплементарности афинность редактирующего комплекса к сайту-мишени достаточно высокая, из-за чего влияние первого нуклеотида PAM минимально или отсутствует вовсе. Наличие же неспаренностей увеличивают свободную энергию взаимодействия Cas9/sgRNA с ДНК, из-за чего влияние PAM начинает проявляться [7].

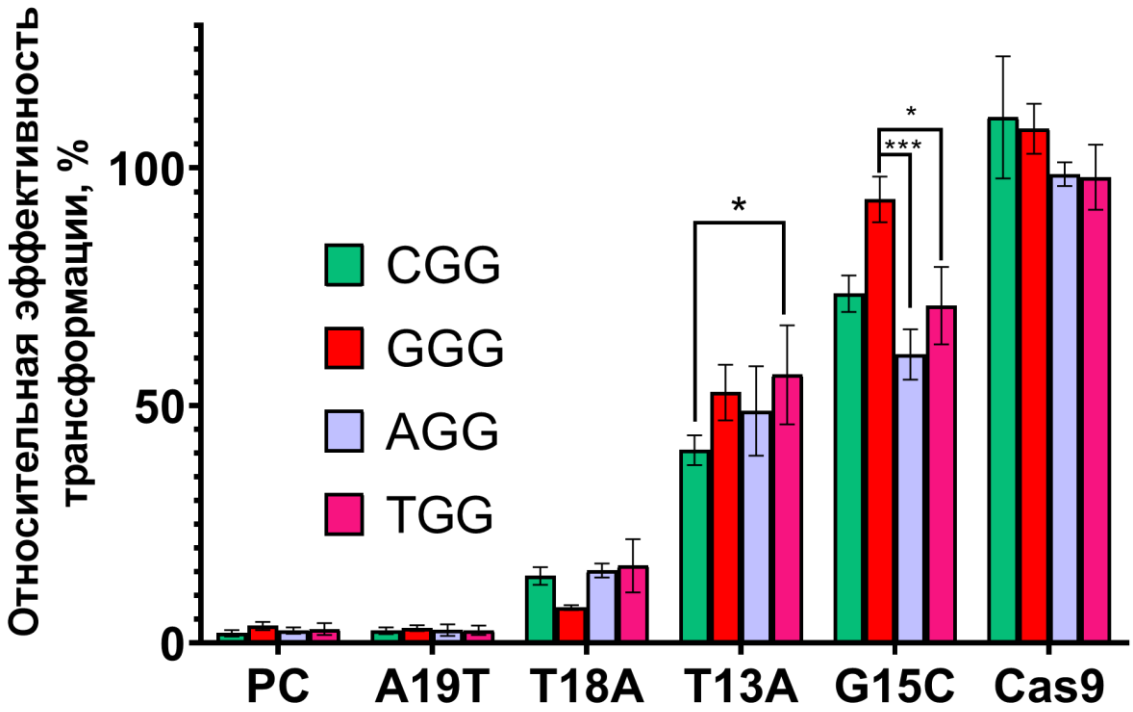



Рис. 3. Относительная эффективность трансформации дрожжевых штаммов, различающихся мотивом PAM вблизи целевого сайта, плазмидами, кодирующими sgRNA с одиночными заменами в различных позициях

**Заключение**

Нам удалось разработать тест-систему для оценки эффективности системы геномного редактирования CRISPR/Cas9 в дрожжах *Saccharomyces cerevisiae*. С ее помощью мы оценили влияние неспаренностей между гидовой РНК и сайтом-мишенью на активность эндонуклеазы Cas9. Наши результаты, с одной стороны, подтвердили данные предыдущих работ о толерантности CRISPR/Cas9 к неспаренностям в дистальной области гидовой РНК. С другой стороны, мы смогли установить, что нуклеотиды в пределах seed-области имеют разное значение для активности Cas9. Также, согласно полученным данным, при наличии

наспаренностей в некоторых позициях гидовой РНК на эффективность Cas9 может оказывать влияние первый нуклеотид мотива PAM. В дальнейшем, с использованием разработанной тест-системы мы планируем изучить влияние на нецелевую активность CRISPR/Cas9 других факторов, таких как состояние хроматина, транскрипционный статус в конкретном локусе, а также тип неспаренности.

*Работа была выполнена при поддержке ООО «Компания Хеликон» (ИНН 7704543951).*

**Литература**

1. Shumega A.R. et al. CRISPR/Cas9 as a mutagenic factor // International journal of molecular sciences. 2024. V. 25. №. 2. P. 823.
2. Burhans W.C. et al. Apoptosis-like yeast cell death in response to DNA damage and replication defects // Mutation Research/Fundamental and Molecular Mechanisms of Mutagenesis. 2003. V. 532. №. 1-2. Pp. 227–243.
3. Deviatkin D.M., Stepchenkova E.I., Shumega A.R. Cas9 Endonuclease Toxicity in Haploid and Diploid Strains of Saccharomyces cerevisiae // Cell and Tissue Biology. 2025. V. 19. №. Suppl 1. Pp. S44–S48.
4. Laughery M.F., Wyrick J.J. Simple CRISPR-Cas9 genome editing in Saccharomyces cerevisiae // Current protocols in molecular biology. 2019. V. 129. №. 1. P. e110.
5. Anderson E.M. et al. Systematic analysis of CRISPR–Cas9 mismatch tolerance reveals low levels of off-target activity // Journal of biotechnology. 2015. V. 211. Pp. 56–65.
6. Boyle E.A. et al. High-throughput biochemical profiling reveals sequence determinants of dCas9 off-target binding and unbinding // Proceedings of the National Academy of Sciences. 2017. V. 114. №. 21. Pp. 5461–5466.
7. Corsi G.I. et al. CRISPR/Cas9 gRNA activity depends on free energy changes and on the target PAM context // Nature Communications. 2022. V. 13. №. 1. P. 3006.

УДК 615.252.349.7

# ТЕРАПИЯ САХАРНОГО ДИАБЕТА MODY - 4 ГЕННОТЕРАПЕВТИЧЕСКИМИ МЕТОДАМИ

**Воронцов А.А.**[1] (студент)
[1] Университет ИТМО
1404artemiy@gmail.com

**Аннотация**
В работе рассматривается возможность применения геннотерапевтических методов для лечения сахарного диабета MODY - 4, вызываемого мутацией в гене PDX1. Проведён анализ генетических особенностей заболевания, механизмов его развития и существующих видов вирусных векторов, применяемых для доставки терапевтических генов. Обоснован выбор аденоассоциированного вируса (AAV) как оптимального вектора для доставки корректной версии гена PDX1 в клетки двенадцатиперстной кишки. Рассмотрены ограничения, связанные с малой вместимостью капсида AAV, и предложено решение на основе технологии транс-сплайсинга, позволяющей объединять два фрагмента крупного гена непосредственно в клетке-мишени. Описан концепт геннотерапевтического препарата, включающий этапы трансдукции, восстановления гена и его интеграции в геном пациента с использованием CRISPR-Cas9 или сходных систем. Работа демонстрирует перспективность генной терапии для лечения моногенных форм диабета и подчёркивает важность выбора корректного вектора и оптимальных молекулярных механизмов для восстановления функции PDX1.

**Ключевые слова**
MODY-4, PDX1, генная терапия, вирусные векторы, AAV, транс - сплайсинг, CRISPR.

Сахарный диабет взрослого типа у молодых (MODY) объединяет гетерогенную группу заболеваний с аутосомно-доминантным типом наследования, вызванных мутациями, приводящими к дисфункции секретирующих инсулин - клеток (рис. 1) или к нарушению закладки и развития поджелудочной железы [1]. По оценкам европейских когорт, распространенность MODY составляет 1 на 10 000 человек среди взрослых и 1 на 23 000 человек среди детей [2], что в сумме составляет 1–6,5% всех пациентов с сахарным диабетом [1]. Сахарный диабет взрослого типа у молодых впервые был описан в 1964 году. Однако тогда не были известны причины, вызывающие MODY, но были обнаружены типичные для данного заболевания признаки: ранний дебют (проявление симптомов происходит в возрасте от 12 до 30 лет), а также чувствительность к препаратам ПСМ [3]. Патогенез MODY стал понятен лишь в 1992 году, когда была доказана связь между развитием MODY 2-го типа и мутацией в гене, кодирующем глюкокиназу GSC [4]. Позднее исследователи обнаружили мутации в генах ядерных факторов гепатоцитов 1α и 4α *(*HNF1a*,* HNF4a*)*, приводящие к развитию диабета MODY 1-го и 3-го типа. 1-ый, 2-ой и 3-ий типы диабета MODY вместе составляют до 90% всех случаев данного заболевания. Всего же на данный момент известно 13 типов диабета MODY, вызываемых мутациями в генах, кодирующих белки углеводного обмена, а именно:

1. MODY-1. Данный тип диабета вызван мутацией в гене HNF4A (ядерный фактор гепатоцитов 4a) между D20S169 и D20S176 [6], чья длина равна 17 954 п.н. Его продукт участвует в контроле обмена и распределения глюкозы, а также влияет на экспрессию ядерного фактора гепатоцитов 1a [5]. У пациентов сданным типом MODY развивается легкая форма диабета, однако высок риск развития хронической гипергликемии и полиурии. Лечение заключается в принятии пероральных гипогликемических препаратов и инсулина.
2. MODY-2. Данный тип диабета вызван одной из 130 известных мутаций в гене глюкокиназы (GSK), имеющем длину 46 227 п.н., чей продукт контролирует опосредованное глюкозой выведение инсулина из железистых клеток [7]. MODY 2-го типа является инсулиннезависимым сахарным диабетом, приводит к развитию легкой непрогрессирующей гиергликемии и считается благоприятной формой, не вызывающей осложнений и не требующей какого-либо лечения.

3. MODY-3. Данный тип диабета вызван мутацией в гене HNF1A (ядерный фактор гепатоцитов 1a) между D12S86 и D12S342, который по своей длине (39 044 п.н.), а также вызываемой поломкой клинической картине практически идентичен диабету MODY 1-го типа, рассмотренному ранее [8]. Однако, несмотря на схожесть с диабетом MODY 1-го типа, диабет MODY 3-го типа приводит к гипергликемии с тяжелым дефектом секреции инсулина, что доказывает роль HNF1A в развитии клеток поджелудочной железы (рис. 1).
4. MODY-4. Данный тип диабета вызван мутацией в первой паре нуклеотидов гена PDX1 (IPF1), чья длина (6 314 п.н.) является наименьшей среди всех генов, мутации в которых вызывают тот или иной тип диабета MODY. Данная длина и точная локализация мутации делают PDX1 наиболее перспективной целью для геннотерапевтического препарата. Продукт экспрессии гена PDX1 является важным транскрипционным фактором инсулина и глюкокиназы, тогда как изоформа данного белка, синтезируемая с поломанного гена, является ингибитором транскрипции и понижает уровень экспрессии инсулина [9]. Симптомы MODY 4-го типа идентичны симптомам 1-го, 2-го и 3-го типов MODY (гипергликемия, полиурия, гликозурия и повышенная жажда), однако мутация PDX1 является редкой причиной возникновения диабета в популяции [10].
5. MODY-5. Данный тип диабета вызван мутацией в факторе HNF-1$\beta$ (ядерный фактор гепатоцитов 1b), имеющем длину 58 628 п.н. [11]. Его продукт влияет на эмбриональное развитие печени и почек, а мутация в нем приводит к прогрессирующей нефропатии - уникальному симптому диабета MODY 5-го типа [12].
6. MODY-6. Данный тип диабета вызван нелокализованной мутацией в гене NEUROD1, имеющем длину 22 222 п.н. [13]. Продукт экспрессии является важным фактором дифференцировки клеток, в случае поломки которого нарушается развитие инсулин - производящих клеток и клеток нервной системы, что приводит к развитию диабета с неврологической патологией (нейропатией) [14].
7. MODY-7. Данный тип диабета вызван мутацией неустановленного гена, однако наиболее вероятной причиной является поломка фактора Круппеля 11 (KLF11), работа которого связана с развитием чувствительности клеток к инсулину при высокой концентрации глюкозы [15]. Симптоматика диабета MODY 7-го типа неизвестна по причине низкой распространенности данного заболевания в популяции.
8. MODY-8. Данный тип диабета вызван мутацией в гене CEL, имеющем длину 62 443 п.н. Его продуктом является человеческая карбоксилэфирлипаза, физиологическая роль которой заключается в гидролизе и всасывании эфиров холестерина жирорастворимых витаминов. Дисфункция данного белка приводит к прогрессирующему липоматозу (замещению панкреатической паренхимы жировой тканью), развитию кист поджелудочной железы и хроническому панкреатиту [16].
9. MODY-9. Данный тип диабета вызван мутацией в гене PAX4, имеющем длину 18 225 п.н. Его продукт, фактор PAX4, как и NEUROD1 (MODY-6), является частью каскада дифференцировки клеток поджелудочной железы, секретирующих инсулин [17]. При этом точную локализацию мутации выявить не удалось: среди 244 пациентов тайского происхождения с подозрением на MODY-9 не было обнаружено ни одного соответствия [9], а среди людей русской национальности случаи MODY 7-го типа единичны [18].
10. MODY-10. Данный тип диабета вызван мутацией в гене инсулина (INS), имеющего длину 1 430 п.н. [19]. MODY 10-го типа является крайне редким заболеванием и единственным типом MODY, связанным с мутацией в гене инсулина. MODY-11 является крайне редким заболеванием и единственным типом диабета MODY, связанным с геном инсулина. В литературе имеются единичные описания семей с MODY-INS или MODY-10, клиническое течение данного заболевания практически не изучено [20].
11. MODY-11. Данный тип диабета вызван мутацией в гене BLK, имеющем длину 70 212 п.н., между D8S1706 и D8S1721 [21]. Он кодирует B-лимфоидную тирозинкиназу, осуществляющую фосфорилирование Ig-альфа субъединицу рецептора клеток (BCR), что приводит к активации - клеток, секреции инсулина и клональной экспансии (увеличению

количества клеток одного или нескольких клонов) [22]. Является крайне редким типом диабета MODY.

12. MODY-12. Данный тип диабета вызван мутацией в гене АТФ-связывающего кассетного транспортера подсемейства С8 (ABCC8), имеющего длину 84 347 п.н. [23]. MODY-12 крайне редким типом диабета с неустановленной клинической картиной. При этом известно. Что данный тип диабета может привести к непролиферативной диабетической ретинопатии и диабетическому макулярному отеку.
13. MODY-13. Данный тип диабета вызван мутацией в гене KCNJ11, имеющем длину 14 102 п.н. Его влияние на организм, как и клиническая картина MODY-13 , не исследованны, однако известно, что белок, кодируемый геном KCNJ11, является АТФ - чувствительным калиевым каналом (KATP), связанным с возбудимостью мембран различных типов клеток, в том числе - клеток поджелудочной железы [24].

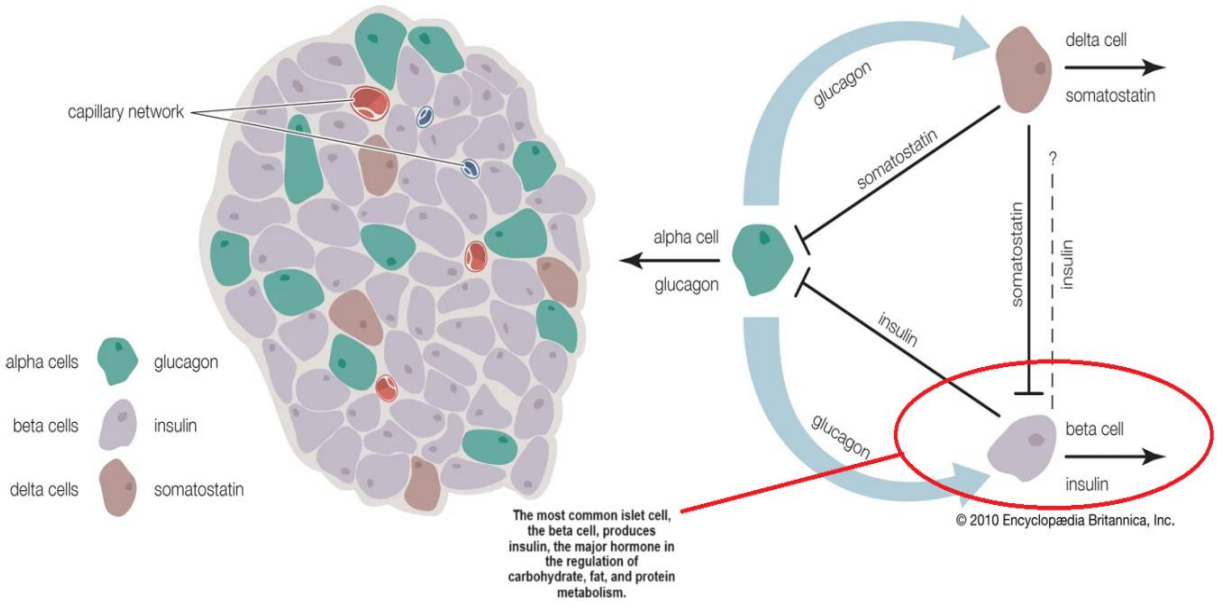



Рис. 1. Островки Лангерганса (Britannica, 2022). Beta cell - b-клетки поджелудочной железы

13 типов диабета MODY отличаются друг от друга клиническим течением и необходимостью лечения. В настоящее время наиболее изучены диабеты MODY 1-5, которые в сумме составляют более 90% случаев диабета MODY. Описание остальных форм носит спорадический характер [23].

Проанализировав данные таблицы (таблица), мною был выбран ген PDX1 за его размер и точно локализованную мутацию, приводящую к развитию диабета MODY 4-го типа, который по сравнению с MODY 6-13 типов встречается в популяции достаточно часто и требует своевременного лечения.

PDX-MODY или MODY-4 – моногенное заболевание, вызываемое гетерозиготной мутацией в гене PDX1 (рис. 4), кодирующем белок гомеобокса поджелудочной железы и двенадцатиперстной кишки 1 (PDX1), известный как фактор промоутера инсулина 1 (IPF 1) [26]. В нормальном состоянии основной островковый белок гомеобокса связывается с двумя консервативными мутационно чувствительными АТ-богатыми последовательностями, расположенными в промоутере гена INS между -214 и -211 и между -82 и -78 нуклеотидами, повышая уровень экспрессии инсулина (рис. 3). Однако в случае миссенс-мутации (делеции первой пары нуклеотидов) происходит сдвиг рамки считывания на границе С-конца трансактивационного домена IPF1, что приводит к трансляции 59 новых кодонов перед терминацией [27]. В итоге, у пораженного пациента не может сформироваться функциональный белок IPF1 [28], что приводит к потере поджелудочной железой своих функций, так как доказано, что IPF1 является критически важным регулятором развития клеток [29]. Согласно последним исследованиям, IPF1 служит главным контрольным переключателем для экспрессии программы развития поджелудочной [30], полная делеции которого приводит к «нулевому фенотипу

поджелудочной железы», а миссенс-мутация – к дисфункции и диабету MODY 4-го типа. Симптомы данного типа диабета типичны, за исключением описанных в 1993 году случаев полной агенезии поджелудочной железы [31]. Причиной же развития данного заболевания является не только снижение дозы нормального гена PDX1, но и доминантно -негативное ингибирование транскрипции гена инсулина и других генов клеток, регулируемых мутантным IPF1.

Таблица

**Сравнение типов диабета MODY**

| Тип MODY | Ген | Размер гена | Локализация мутации(й) | Частота |
|---|---|---|---|---|
| MODY-1 | HNF4A | 17 954 п.н. | Известна | Часто встречающийся |
| MODY-2 | GSK | 46 227 п.н. | Известна | Часто встречающийся |
| MODY-3 | HNF1A | 39 004 п.н. | Известна | Часто встречающийся |
| MODY-4 | PDX1 | 6 314 п.н. | Известна | Редко встречающийся |
| MODY-5 | HNF-1$\beta$ | 58 628 п.н. | Известна | Редко встречающийся |
| MODY-6 | NEUROD1 | 22 222 п.н. | Известна | Редко встречающийся |
| MODY-7 | KLF11 (?) | - | Неизвестна | Крайне редко встречающийся |
| MODY-8 | CEL | 62 443 п.н. | Неизвестна | Крайне редко встречающийся |
| MODY-9 | PAX4 | 18 225 п.н. | Неизвестна | Крайне редко встречающийся |
| MODY-10 | INS | 1 430 п.н. | Неизвестна | Крайне редко встречающийся |
| MODY-11 | BLK | 70 212 п.н. | Известна | Крайне редко встречающийся |
| MODY-12 | ABCC8 | 84 347 п.н. | Неизвестна | Крайне редко встречающийся |
| MODY-13 | KCNJ11 | 14 102 п.н. | Неизвестна | Крайне редко встречающийся |

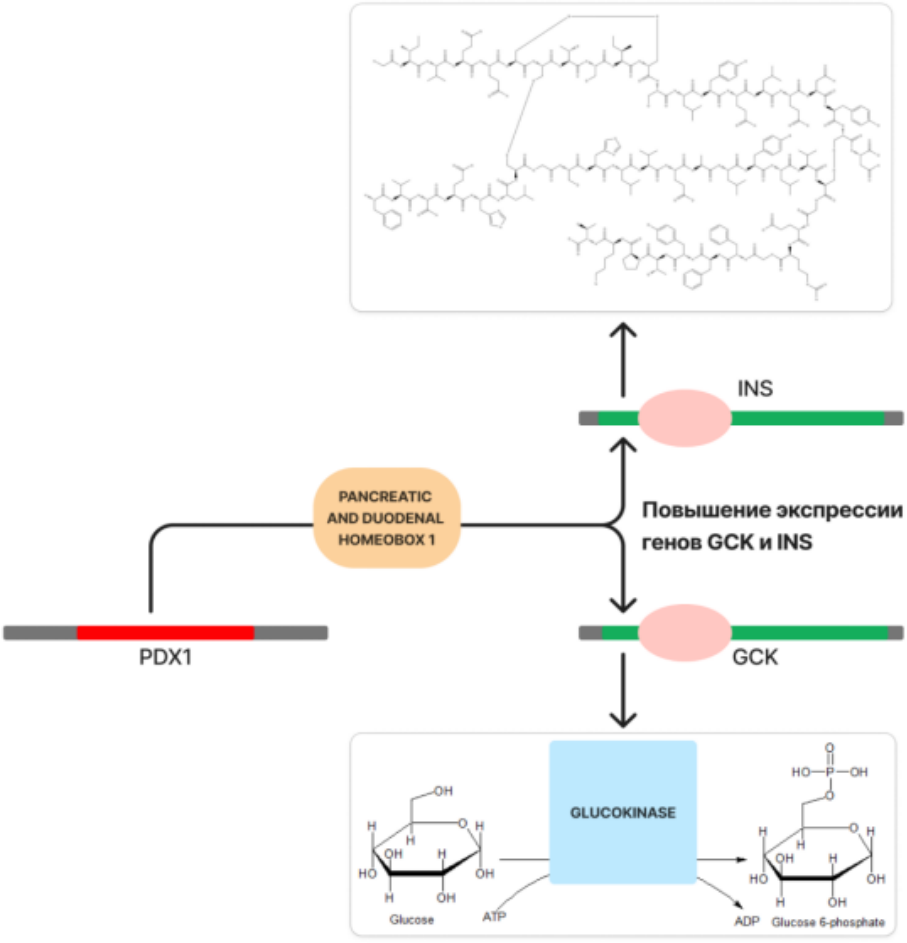



Рис. 2. Влияние продукта экспрессии гена PDX1 (гомеобокс белка поджелудочной железы и двенадцатиперстной кишки) на экспрессию генов углеводного обмена

PDX1:

GAGATCAGTGCGGAGCTGTCAAAGCGAGCAGGGGTGGCGCCGGGAGT
GGGAACGCCACACAGTGCCAAATCCCCGGCTCCAGCTCCCGACTCCCGG
CTCCCGGCTCCCGGCTCCCGGTGCCCAATCCCGGGCCGCAGCCATGAAC
GGCGAGGAGCAGTACTACGCGGCCACGCAGCTTTACAAGGACCCATGC
GCGTTCCAGCGAGGCCCGGCGCCGGAGTTCAGCGCCAGCCCCCCTGCGT
GCCTGTACATGGGCCGCCAGCCCCCGCCGCCGCCGCCGCACCCGTTCCCT
GGCGCCCTGGGCGCGCTGGAGCAGGGCAGCCCCCCGGACATCTCCCCGT

Рис. 3. Ген PDX1 (6 314 п.н., 13 хромосома) (UCSC Genome Browser on Human)

В данной работе предлагается использование вирусных векторов для доставки трансгена и лечения диабета MODY 4-го типа геннотерапевтическими методами. Для этого необходимо выбрать наиболее оптимальный вариант вирусного вектора из тех, которые существуют и активно используются в генной терапии. К ним относятся аденовирусы, аденоассоциированные вирусы, лентивирусы, вирус везикулярного стоматита, осповирусы, герпесвирусы, бакуловирусы, вирусы гриппа и ретровирусы, являющиеся наиболее распространенными вирусными векторами, использующимися для трансдукции клеток ex vivo (Parkman и др., 2000).

Рассмотрим упомянутые вирусные вектора подробнее:

**Аденовирусы**. Вирусный вектор, созданный на основе аденовируса, применяется повсеместно, в том числе для терапии рака [32]. Чаще других используют вектор аденовируса человека 5-го (Ad5) и 26-го (Ad26) серотипов (к примеру, в вакцинах против коронавируса «Спутник V» [33] и “Oxford-AstraZeneca”, а также в “Zabdeno” – вакцине против вируса Эбола [34]. Преимуществами данного вирусного вектора являются высокая эффективность трансдукции, способность инфицировать как делящиеся, так и неделящиеся клетки, отсутствие тропизма к тканям [35], а также то, что он не интегрируются в геном хозяина, что снижает риск случайного мутагенеза, однако может вызвать сильный иммунный ответ (так как организм каждого человек не раз сталкивался с вирусами семейства аденовирусов) [36]. Помимо этого, вирусные вектора на основе аденовируса имеют небольшие размеры, малую вместительность (до 8 п.н.), а также обеспечивают лишь временную экспрессию трансгена [37].

Аденоассоциированные вирусы (AAV). Вирусный вектор на основе аденноасоциированного вектора имеет максимальный уровень безопасности (BSL-1) и, в отличии от аденовирусов, при постоянной экспрессии трансгена не интегрируется в геном и не вызывает иммунный ответ, то есть обладает низкой иммуногенностью [38], что делает его наиболее подходящим для использования в препаратах генной терапии [39], таких как “Luxturna” (препарат против RPE65-ассоциированной дистрофии сетчатки [40]) или “Zolgensma” (препарат против СМА [41]). Недостатком же является небольшой размер и наименьшая вместительность капсид среди всех предложенных вариантов - 4 700 п.н. [42], что делает невозможным трансдукцию трансгена большого размера без дополнительных регуляторных систем.

**Лентивирусы**. Уникальность вектора, созданного на основе лентивируса, заключается в его способности реплицироваться в неделящихся клетках, обеспечивая тем самым стабильную долгосрочную экспрессию гена интереса [43]. Однако данный вектор интегрируется в геном, что может вызвать серьезный мутагенез и дальнейшие осложнения в клинической картине пациента [44]. Все же лентивирусы продолжают использоваться при создании терапевтических препаратов, направленных на борьбу с раком, таких как Kymriah и Yescarta, предназначенных для противораковой CAR-T терапии (модификации Т-клеток) [45]. Вектор на основе лентивирусов обладает малыми размерами и вместительностью 8 000 п.н. [46].

Вирус везикулярного стоматита. Данный тип вирусного вектора имеет тропизм к опухолевым клеткам, используется в противораковых препаратах и вакцинах (к примеру, в вакцине rVSV-ZEBOV против вируса Эболы [47]), обладает высокой эффективностью экспрессии, но при этом имеет небольшие размеры и вместительность (до 5 000 п.н.), а также

высокую иммуногенность и специфичность исключительно к раковым клеткам (Barber, 2005), что делает его применение в препарате против диабета MODY 4-го типа невозможным.

**Осповирусы**. Вирусный вектор создан на основе ослабленного штамма вируса оспы, из-за чего его основной недостаток – способность вызвать сильный иммунный ответ в ослабленном организме [48]. При этом сам вектор обладает оптимальной вместительностью (до 25 000 п.н.) и способен доставлять в клетку сразу несколько генов [49]. Вирусный вектор активно применяется для создания вакцин против патогенного дикого типа вируса оспы обезьян, таких как JYNNEOS (JYNNEOS vaccine. Accessed January 10, 2024)

**Герпесвирусы**. Вирусный вектор, созданный на основе герпесвируса, обладает большой вместительностью (100 000 п.н.) и способен транспортировать в клетку сразу несколько генов [50]. Однако данный вирусный вектор потенциально иммуногенный и способен сохраняться в организме в латентной форме, что осложняет прогнозирование и контроль лечения [51]. Герпесвирусы применяются при создании вакцин и противораковых прапаратов. К примеру, в препарате, применяемом против меланомы, Talimogene laherparepvec (T-VEC) [52].

**Бакуловирусы**. Вирусный вектор практически не используется в препаратах для лечения людей, но активно применяется для лечения других млекопитающих, так как обладает большой вместительностью (до 100 000 п.н.), не иммуногенный и не вызывает инфекций. Однако эффективная экспрессия гена продолжается короткий период времени [53]. Данный вектор применяется в основном в вакцинах против гриппа, к примеру, в препарате Flublok [54].

**Вирусы гриппа**. Вирусные вектора, созданные на основе вирусов гриппа, вызывают сильный иммунный ответ и обладают малой вместительностью (до 4 600 п.н.) [55], однако они сохраняют способность к модификации и вызывают сильную и продолжительную экспрессию гена [56]. Они активно используются в вакцинах против сезонного группа, таких как Fluzone и FluMist [57].

**Ретровирусы**. Вирусный вектор, созданный на основе ретровируса, способен инфицировать делящиеся клетки, приводя к сильной экспрессии гена, однако данный вирус имеет малую вместительность (6 000 п.н.), интегрируется в геном хозяина и подвержен мутагенезу [58]. Ретровирусы используются при создании препаратов против иммунодефициты состояний, таких как SCID (тяжелый комбинированный иммунодефицит) [59].

Существуют и другие вирусные вектора, реже использующиеся в качестве основы для геннотерапевтического препарата, такие как модифицированный вирус лейкоза мыши Молони (MMLV), вирус табачной мозаики (BTM) и другие, однако они не подходят для использования в препарате против диабета MODY 4-го типа. Вышеперечисленные вирусы же необходимо сравнить по определенным критериям и выбрать из них наиболее оптимальные для решения поставленных задач.

Проанализировав данные, мною был выбран вектор на основе аденоассоциированного вируса (AAV) за его низкую иммуногенность, низкий мутагенез и отсутствие тропизма, позволяющее использовать его для доставки гена в любой тип тканей, в том числе в клетки двенадцатиперстной кишки, в которой экспрессия гена PDX1 максимальна.

В данной работе предлагается создать геннотерапевтический препарат против диабета MODY 4-го типа, вызванного мутацией в гене PDX1, экспрессия которого максимальна в клетках двенадцатиперстной кишки (рис. 4). Для этого сначала необходимо выбрать вирусный вектор, который доставит трансген в клетку-мишень (в данном случае в клетку двенадцатиперстной кишки). Предлагаю использовать для этого аденоассоциируемый вирус штамма AAV9, не имеющего тропизма к конкретным тканям и успешно применяющегося в препарате Zolgensma [60]. Однако, для применения данного вектора необходимо решить проблему вместительности вирусного капсида AAV, недостаточного для хранения трансгенов больших размеров (в том числе трансгена PDX1, 6 314/4 700 п.н.). Для ее решения можно применить один из методов «двойных векторов», к которым относятся фрагментированные, перекрывающиеся, транс-сплайсинговые и гибридные векторы [61]. Фрагментированный подход работает по принципу того, что AAV-векторы могут упаковывать большие гены, разбивая их на более мелкие фрагменты. Каждый вектор несет фрагмент терапевтического гена, и в итоге целевой клетке необходимо получить оба фрагмента, чтобы восстановить полный ген. Основной

недостаток этого метода заключается в том, что он часто приводит к нежелательным продуктам и плохой контролируемости упаковки трансгена [61]. Метод перекрывающихся векторов предполагает наличие перекрывающихся регионов в двух фрагментах терапевтического гена, которые помогают им объединиться в одну последовательность. Преимущество заключается в том, что он не требует дополнительных генетических элементов, однако необходимо проводить предварительное тестирование, чтобы определить оптимальную длину перекрывающейся последовательности. Недостаток метода — потенциальная возможность возникновения нежелательных продуктов [61]. Суть метода транс-сплайсинга заключается в разделении трансгена на равные части с добавлением специфических регуляторных сайтов SA (акцептор) или SD (донор), в зависимости от конкретной половины терапевтического трансгена. В процессе транс-сплайсинга две равные части одного трансгена, доставленные двумя разными вирусными частицами, "сшиваются", образуя полноценный рабочий ген. Метод транс-сплайсинга более совершенный и, в отличии от существующих аналогов, обладает высокой точностью [61]. Гибридный метод сочетает в себе элементы перекрывающихся и транс-сплайсинговых методов, предоставляя два шанса на успешное восстановление гена. Этот подход использует как перекрывающиеся последовательности, так и элементы сплайсинга. Гибридный метод может быть более эффективным, но требует оптимизации как перекрывающихся, так и сплайсинговых последовательностей [61]. В данной работе предлагаю использовать метод транс-сплайсинга за его высокую точность эффективность.

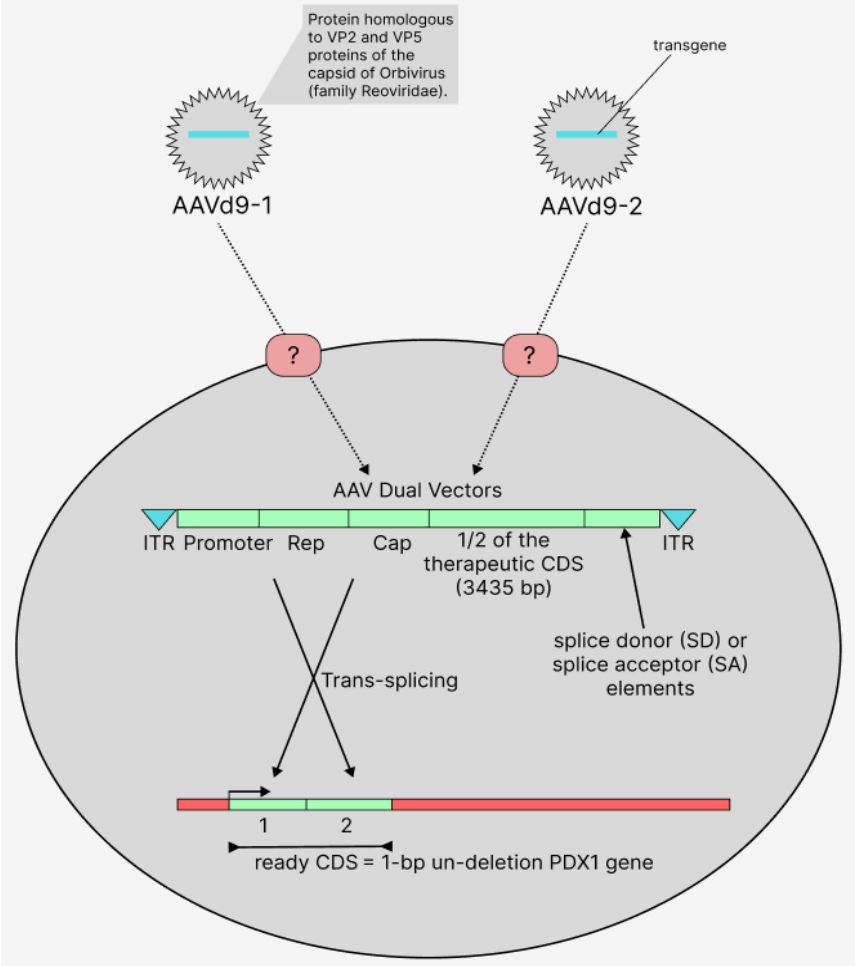



Рис. 4. Концепт препарата против диабета MODY 4-го типа

Трансдукция гена PDX1, лишенного делеции первой пары нуклеотидов, происходит в три этапа:

1. Проникновение генетического материала вируса в клетку. Так как аденоассоциированый вирус не обладает тропизмом к конкретным типам тканей, его необходимо доставить непосредственно к клеткам двенадцатиперстной кишки. На

самой вирусной частице можно разместить антигены к рецепторам gpr40 и gpr120, специфичных для эндокринных клеток двенадцатиперстной кишки.

2. Транс-сплайсинг. В процессе транс-сплайсинга две равные части одного трансгена, доставленные двумя разными вирусными частицами, "сшиваются", образуя полноценный рабочий ген, который будет интегрирован в геном клетки вместо гена PDX1 с делецией первой пары нуклеотидов.
3. Вырезание поврежденного и встраивание нормального гена PDX1 в геном пациента, больного диабетом MODY 4-го типа с помощью системы CRISPR-Cas9 или иных систем таргетного редактирования генома.

**Литература**


1. Rusyaeva N.V., Kononenko I.V., Vikulova O.K., Isakov M.A., Shestakova M.V., Mokrysheva N.G. Characteristics of patients with diagnosis of maturity-onset diabetes of the young, according to the Russian diabetes registry // Diabetes mellitus. 2024;27(4):321-335. (In Russ.) https://doi.org/10.14341/DM13100.
2. Nkonge K.M., Nkonge D.K., Nkonge T.N. The epidemiology, molecular pathogenesis, diagnosis, and treatment of maturity-onset diabetes of the young (MODY) // Clin Diabetes Endocrinol 6, 20 (2020). https://doi.org/10.1186/s40842-020-00112-5.
3. Tosur M., Philipson L.H. Precision diabetes: Lessons learned from maturity-onset diabetes of the young (MODY) // J Diabetes Investig. 2022;13(9):1465-1471. https://doi.org/10.1111/jdi.13860.
4. Hattersley A.T., Turner R.C., Permutt M.A. et al. Linkage of type 2 diabetes to the glucokinase gene. Lancet. 1992;339(8805):1307-1310. https://doi.org/10.1016/0140-6736(92)91958-b.
5. Fajans S.S., Bell G.I., Polonsky K.S. Molecular mechanisms and clinical pathophysiology of maturity-onset diabetes of the young // New Eng. J. Med. 345: 971-980, 2001.
6. Yamagata K., Furuta H., Oda N., Kalsaki P.J., Menzel S., Cox N.J., Fajans S.S., Signorini S., Stoffel M., Bell G.I. Mutations in the hepatocyte nuclear factor-4-alpha gene in maturity-onset diabetes of the young (MODY1) // Nature 384: 458-460, 1996.
7. Froguel P., Velho G., Cohen D., Passa P. Strategies for the collection of sibling-pair data for genetic studies in type 2 (non insulin-dependent) diabetes mellitus // (Letter) Diabetologia 34: 685 only, 1992.
8. Vaxillaire M., Boccio V., Philipi A., Vigouroux C., Terwilliger J., Passa P., Beckmann J.S., Velho G., Lathrop G.M., Froguel P. A gene for maturity onset diabetes of the young (MODY) maps to chromosome 12q // Nature Genet. 9: 418-423, 1995.
9. Stoffers D.A., Ferrer J., Clarke W.L., Habener J.F. Early-onset type-II diabetes mellitus (MODY4) linked to IPF1 // (Letter) Nature Genet. 17: 138-141, 1997.
10. Fajans S.S., Bell G.I., Paz V.P., Below J.E., Cox N.J., Martin C., Thomas I.H., Chen M. Obesity and hyperinsulinemia in a family with pancreatic agenesis and MODY caused by the IPF1 mutation Pro63fsX60 // Transl. Res. 156: 7-14, 2010.
11. Haider A., Symczyk O., Hassan A., Khan M.A., Madahar I., Holland D. Maturity-Onset Diabetes of Young Type 5: Diabetes with Extrapancreatic Features // Case Rep Endocrinol. 2021 Nov 10;2021:8243471. DOI: 10.1155/2021/8243471. PMID: 34804616; PMCID: PMC8598366.
12. Iwasaki N., Ogata M., Tomonaga O. et al. Liver and kidney function in Japanese patients with maturity-onset diabetes of the young. Diabetes Care. 1998;21(12):2144–2148. DOI: 10.2337/diacare.21.12.2144.
13. Malecki M.T., Jhala U.S., Antonellis A., Fields L., Doria A., Orban T., Saad M., Warram J.H., Montminy M., Krolewski A.S. Mutations in NEUROD1 are associated with the development of type 2 diabetes mellitus // Nature Genet. 23: 323-328, 1999.
14. Lee J.E., Hollenberg S.M., Snider L., Turner D.L., Lipnick N., Weintraub H. Conversion of Xenopus ectoderm into neurons by NeuroD, a basic helix-loop-helix protein // Science 268: 836-844, 1995.
15. Mancera-Rincón P., Luna-España M.C., Rincon O., Guzmán I., Alvarez M. Maturity-onset Diabetes of the Young Type 7 (MODY7) and the Krüppellike Factor 11 Mutation (KLF11) // A Review. Curr Diabetes Rev. 2024;20(1):e210323214817. DOI: 10.2174/1573399819666230321114456. PMID: 36944622.
16. Sun S., Gong S., Li M., Wang X., Wang F., Cai X., Liu W., Luo Y., Zhang S., Zhang R., Zhou L., Zhu Y., Ma Y., Ren Q., Zhang X., Chen J., Chen L., Wu J., Gao L., Zhou X., Li Y., Zhong L., Han X., Ji L. Clinical and genetic characteristics of CEL-MODY (MODY8): a literature review and screening in Chinese individuals diagnosed with early-onset type 2 diabetes // Endocrine. 2024 Jan;83(1):99-109. DOI: 10.1007/s12020-023-03512-6. Epub 2023 Sep 19. PMID: 37726640.

17. Plengvidhya N., Kooptiwut S., Songtawee N., Doi A., Furuta H., Nishi M., Nanjo K., Tantibhedhyangkul W., Boonyasrisawat W., Yenchitsomanus P., Doria A., Banchuin N. PAX4 mutations in Thais with maturity onset diabetes of the young // J. Clin. Endocr. Metab. 92: 2821-2826, 2007.
18. Zubkova N.A., Gioeva O.A., Petrov V.M., Vasiliev E.V., Timofeev A.V., Abrukova A.V., Tiulpakov A.N. Monogenic diabetes associated with PAX4 gene mutations (MODY9): first description in Russia. Diabetes mellitus. 2017;20(5):384-387. (In Russ.).
19. Edghill E.L., Flanagan S.E., Patch A.-M., Boustred C., Parrish A., Shields B., Shepherd M.H., Hussain K., Kapoor R.R., Malecki M., MacDonald M.J., Stoy J., Steiner D.F., Philipson L.H., Bell G.I., Neonatal Diabetes International Collaborative Group, Hattersley A.T., Ellard S. Insulin mutation screening in 1,044 patients with diabetes: mutations in the INS gene are a common cause of neonatal diabetes but a rare cause of diabetes diagnosed in childhood or adulthood // Diabetes 57: 1034-1042, 2008.
20. Sechko E.A., Kuraeva T.L., Andrianova E.A., Zilberman L.I., Emelyanov A.O., Laptev D.N., Bezlepkina O.B. MODY caused by a mutation in the insulin gene. Diabetes mellitus. 2022;25(1):89-94. (In Russ.) https://doi.org/10.14341/DM12807.
21. Borowiec M., Liew C.W., Thompson R., Boonyasrisawat W., Hu J., Mlynarski W.M., El Khattabi I., Kim S.-H., Marselli L., Rich S.S., Krolewski A.S., Bonner-Weir S., Sharma A., Sale M., Mychaleckyj J.C., Kulkarni R.N., Doria A. Mutations at the BLK locus linked to maturity onset diabetes of the young and beta-cell dysfunction // Proc. Nat. Acad. Sci. 106: 14460-14465, 2009.
22. Compeer E.B., Janssen W., van Royen-Kerkhof A., van Gijn M., van Montfrans J.M., Boes M. Dysfunctional BLK in common variable immunodeficiency perturbs B-cell proliferation and ability to elicit antigen-specific CD4+ T-cell help // Oncotarget 6: 10759-10771, 2015.
23. Ovsyannikova A.K., Rymar O.D., Shakhtshneider E.V., Klimontov V.V., Koroleva E.A., Myakina N.E., Voevoda M.I. ABCC8-Related Maturity-Onset Diabetes of the Young (MODY12): Clinical Features and Treatment Perspective // Diabetes Ther. 2016 Sep;7(3):591-600. DOI: 10.1007/s13300-016-0192-9. Epub 2016 Aug 18. PMID: 27538677; PMCID: PMC5014798.
24. Bonnefond A., Philippe J., Durand E., Dechaume A., Huyvaert M., Montagne L., Marre M., Balkau B., Fajardy I., Vambergue A., Vatin V., Delplanque J., Le Guilcher D., De Graeve F., Lecoeur C., Sand O., Vaxillaire M., Froguel P. Whole-exome sequencing and high throughput genotyping identified KCNJ11 as the thirteenth MODY gene // PLoS One 7: e37423, 2012.
25. Britannica The Editors of Encyclopaedia. "Islets of Langerhans" Encyclopedia Britannica [Электронный ресурс]. Режим доступа: https://www.britannica.com/topic/nutmeg (дата обращения 09.09.2023).
26. Schwitzgebel V.M., Mamin A., Brun T., Ritz-Laser B., Zaiko M., Maret A., Jornayvaz F.R., Theintz G.E., Michielin O., Melloul D., Philippe J. Agenesis of human pancreas due to decreased half-life of insulin promoter factor 1 // J. Clin. Endocr. Metab. 88: 4398-4406, 2003.
27. Hansen L., Urioste S., Petersen H.V., Jensen J.N., Eiberg H., Barbetti F., Serup P., Hansen T., Pedersen O. Missense mutations in the human insulin promoter factor 1 gene and their relation to maturity-onset diabetes of the young and late-onset type 2 diabetes mellitus in Caucasians // J. Clin. Endocr. Metab. 85: 1323-1326, 2000.
28. Stoffers D.A., Zinkin N.T., Stanojevic V., Clarke W.L., Habener J.F. Pancreatic agenesis attributable to a single nucleotide deletion in the human IPF1 gene coding sequence // Nature Genet. 15: 106-110, 1997.
29. Jonsson J., Carlsson L., Edlund T., Edlund H. Insulin-promoter-factor 1 is required for pancreas development in mice // Nature 371: 606-609, 1994.
30. Sharma S., Jhala U.S., Johnson T., Ferreri K., Leonard J., Montminy M. Hormonal regulation of an islet-specific enhancer in the pancreatic homeobox gene STF 1 // Molec. Cell. Biol. 17: 2598-2604, 1997.
31. Wright N.M., Metzger D.L., Borowitz S.M., Clarke W.L. Permanent neonatal diabetes mellitus and pancreatic exocrine insufficiency resulting from congenital pancreatic agenesis // Am. J. Dis. Child. 147: 607-609, 1993.
32. Wold W.S., Toth K. Adenovirus vectors for gene therapy, vaccination and cancer gene therapy // Curr Gene Ther. 2013 Dec;13(6):421-33. doi: 10.2174/15665232136661311250950 46. PMID: 24279313; PMCID: PMC4507798.
33. Jones I., Roy P.. Sputnik V COVID-19 vaccine candidate appears safe and effective. Lancet. 2021 Feb 20;397(10275):642-643. DOI: 10.1016/S0140-6736(21)00191-4. Epub 2021 Feb 2. PMID: 33545098; PMCID: PMC7906719.

34. Woolsey C., Geisbert T.W. Current state of Ebola virus vaccines: A snapshot. PLoS Pathog. 2021 Dec 9;17(12):e1010078. DOI: 10.1371/journal.ppat.1010078. PMID: 34882741; PMCID: PMC8659338.
35. Brunetti-Pierri N., Ng P. Helper-dependent adenoviral vectors for liver-directed gene therapy // Hum Mol Genet. 2011 Apr 15;20(R1):R7-13. DOI: 10.1093/hmg/ddr143. Epub 2011 Apr 5. PMID: 21470977; PMCID: PMC3095052.
36. Lee C.S., Bishop E.S., Zhang R., Yu X., Farina E.M., Yan S., Zhao C., Zheng Z., Shu Y., Wu X., Le J., Li Y., Zhang W., Yang C., Wu K., Wu Y., Ho S., Athiviraham A., Lee M.J., Wolf J.M., Reid R.R., He T.C. Adenovirus-Mediated Gene Delivery: Potential Applications for Gene and Cell-Based Therapies in the New Era of Personalized Medicine // Genes Dis. 2017 Jun;4(2):43-63. DOI: 10.1016/j.gendis.2017.04.001. Epub 2017 Apr 27. PMID: 28944281; PMCID: PMC5609467.
37. Nayerossadat N., Maedeh T., Ali P.A. Viral and nonviral delivery systems for gene delivery // Adv Biomed Res. 2012;1:27. DOI: 10.4103/2277-9175.98152. Epub 2012 Jul 6. PMID: 23210086; PMCID: PMC3507026.
38. Kotterman M.A., Chalberg T.W., Schaffer D.V. Viral Vectors for Gene Therapy: Translational and Clinical Outlook // Annu Rev Biomed Eng. 2015;17:63-89. DOI: 10.1146/annurev-bioeng-071813-104938. PMID: 26643018.
39. He X., Urip B.A., Zhang Z., Ngan C.C., Feng B. Evolving AAV-delivered therapeutics towards ultimate cures // J Mol Med (Berl). 2021 May;99(5):593-617. DOI: 10.1007/s00109-020-02034-2. Epub 2021 Feb 16. PMID: 33594520; PMCID: PMC7885987.
40. Maguire A.M., Bennett J., Aleman E.M., Leroy B.P., Aleman T.S. Clinical Perspective: Treating RPE65-Associated Retinal Dystrophy // Mol Ther. 2021 Feb 3;29(2):442-463. DOI: 10.1016/j.ymthe.2020.11.029. Epub 2020 Dec 3. PMID: 33278565; PMCID: PMC7854308.
41. Schwartz M., Likhite S., Meyer K. Onasemnogene abeparvovec-xioi: a gene replacement strategy for the treatment of infants diagnosed with spinal muscular atrophy. Drugs Today (Barc). 2021 Jun;57(6):387-399. DOI: 10.1358/dot.2021.57.6.3264117. PMID: 34151905.
42. Daya S., Berns K.I. Gene therapy using adeno-associated virus vectors // Clin Microbiol Rev. 2008 Oct;21(4):583-93. DOI: 10.1128/CMR.00008-08. PMID: 18854481; PMCID: PMC2570152.
43. Milone M.C., O'Doherty U. Clinical use of lentiviral vectors // Leukemia. 2018 Jul;32(7):1529-1541. doi: 10.1038/s41375-018-0106-0. Epub 2018 Mar 22. PMID: 29654266; PMCID: PMC6035154.
44. Schambach A., Zychlinski D., Ehrnstroem B., Baum C. Biosafety features of lentiviral vectors // Hum Gene Ther. 2013 Feb;24(2):132-42. DOI: 10.1089/hum.2012.229. PMID: 23311447; PMCID: PMC3581032.
45. Sterner R.C., Sterner R.M. CAR-T cell therapy: current limitations and potential strategies // Blood Cancer J. 2021 Apr 6;11(4):69. DOI: 10.1038/s41408-021-00459-7. PMID: 33824268; PMCID: PMC8024391.
46. Naldini L. Gene therapy returns to centre stage // Nature. 2015 Oct 15;526(7573):351-60. DOI: 10.1038/nature15818. PMID: 26469046.
47. Marzi A., Engelmann F., Feldmann F., Haberthur K., Shupert W.L., Brining D., Scott D.P., Geisbert T.W., Kawaoka Y., Katze M.G., Feldmann H., Messaoudi I. Antibodies are necessary for rVSV/ZEBOV-GP–mediated protection against lethal Ebola virus challenge in nonhuman primates // Proc. Natl. Acad. Sci. U.S.A. 110 (5) 1893-1898, https://doi.org/10.1073/pnas.1209591110.
48. McCart J.A., Ward J.M., Lee J., Hu Y., Alexander H.R., Libutti S.K., Moss B., Bartlett D.L. Systemic cancer therapy with a tumor-selective vaccinia virus mutant lacking thymidine kinase and vaccinia growth factor genes // Cancer Res. 2001 Dec 15;61(24):8751-7. PMID: 11751395.
49. Moss B., Winters E., Jones E.V. 1983. Replication of vaccinia virus // Mechanics of DNA replication and recombination (ed. Cozzarelli N). Pp. 449–461 A. Liss, New York.
50. Liu F., Zhou Z.H. Comparative virion structures of human herpesviruses // Arvin A, Campadelli-Fiume G, Mocarski E, et al., eds. Human Herpesviruses: Biology, Therapy, and Immunoprophylaxis. Cambridge University Press; 2007:27-43.
51. Advani S.J., Roizman B. The Strategy of Conquest // Palese, P. (eds) Modulation of Host Gene Expression and Innate Immunity by Viruses. Springer, Dordrecht. 2005. https://doi.org/10.1007/1-4020-3242-0.
52. Andtbacka R.H., Kaufman H.L., Collichio F., Amatruda T., Senzer N., Chesney J,. Delman K.A., Spitler L.E., Puzanov I., Agarwala S.S., Milhem M., Cranmer L., Curti B., Lewis K., Ross M., Guthrie T., Linette G.P., Daniels G.A., Harrington K., Middleton M.R., Miller WH Jr., Zager J.S., Ye Y., Yao B., Li A., Doleman S., VanderWalde A., Gansert J., Coffin R.S. Talimogene Laherparepvec Improves Durable Response Rate in Patients With Advanced Melanoma // J Clin

Oncol. 2015 Sep 1;33(25):2780-8. DOI: 10.1200/JCO.2014.58.3377. Epub 2015 May 26. PMID: 26014293.
53. van Oers M.M., Vlak J.M. Baculovirus genomic // Curr Drug Targets. 2007 Oct;8(10):1051-68. DOI: 10.2174/138945007782151333. PMID: 17979665.
54. Cox M.M., Hollister J.R. FluBlok, a next generation influenza vaccine manufactured in insect cells // Biologicals. 2009 Jun;37(3):182-9. DOI: 10.1016/j.biologicals.2009.02.014. Epub 2009 Mar 17. PMID: 19297194.
55. Krammer F., Fouchier R.A.M., Eichelberger M.C., Webby R.J., Shaw-Saliba K., Wan H., Wilson P.C., Compans R.W., Skountzou I., Monto A.S. NAction! How Can Neuraminidase-Based Immunity Contribute to Better Influenza Virus Vaccines? mBio. 2018 Apr 3;9(2):e02332-17. DOI: 10.1128/mBio.02332-17. PMID: 29615508; PMCID: PMC5885027.
56. Glaser L, Conenello G, Paulson J, Palese P. Effective replication of human influenza viruses in mice lacking a major alpha2,6 sialyltransferase // Virus Res. 2007 Jun;126(1-2):9-18. DOI: 10.1016/j.virusres.2007.01.011. Epub 2007 Feb 20. PMID: 17313986.
57. de Vries R.D., Rimmelzwaan G.F. Viral vector-based influenza vaccines. Human Vaccines & Immunotherapeutics, 2016. 12(11), 2881–2901. https://doi.org/10.1080/21645515.2016.1210729.
58. Hudecek M., Izsvák Z., Johnen S., Renner M., Thumann G., Ivics Z. Going non-viral: the Sleeping Beauty transposon system breaks on through to the clinical side // Critical Reviews in Biochemistry and Molecular Biology, 2017. 52(4), 355–380. https://doi.org/10.1080/10409238.2017.1304354.
59. Justiz Vaillant A.A., Mohseni M. Severe Combined Immunodeficiency [Электронный ресурс]. Режим доступа: https://www.ncbi.nlm.nih.gov/books/NBK539762/ (дата обращения 15.09.2025).
60. Li C., Samulski R.J. Engineering adeno-associated virus vectors for gene therapy // Nat Rev Genet. 2020 Apr;21(4):255-272. DOI: 10.1038/s41576-019-0205-4. Epub 2020 Feb 10. PMID: 32042148.
61. McClements M.E., MacLaren R.E. Adeno-associated Virus (AAV) Dual Vector Strategies for Gene Therapy Encoding Large Transgenes // Yale J Biol Med. 2017 Dec 19;90(4):611-623. PMID: 29259525; PMCID: PMC5733846.

# Оглавление

# Известия студенческой науки

**Сборник научных трудов**

**Выпуск 1. Том 2**

Текстовое электронное издание

Минимальные системные требования:
Компьютер: процессор x86 с тактовой частотой 500 МГц и выше; ОЗУ 512 Мб; 8Мб на жёстком
диске; видеокарта SVGA 1280x1024 High Color (32 bit); привод CD-ROM.
Операционная система: Windows XP/7/8 и выше.
Программное обеспечение: Adobe Acrobate Reader версии 6 и старше.

Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Дизайн обложки П.А. Леушина
Вёрстка К.Д. Бутылкина
Подписано к печати 05.12.2025
Объем издания 2069 Мб
Заказ № 4933 от 05.12.2025
Материалы печатаются в авторской редакции

Издательство Университет ИТМО

ISBN 978-5-7577-0741-9


ИТМО