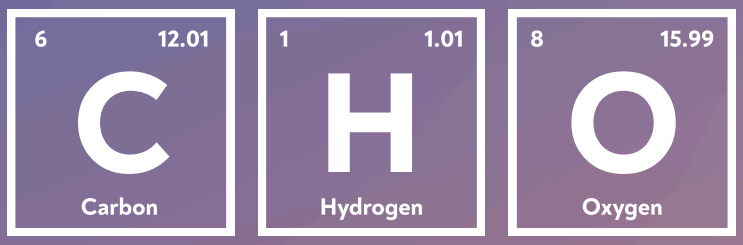
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

известия студенческой науки



Выпуск 1

Том 4

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 4

Текстовое электронное издание

Санкт-Петербург
2025

УДК 004, 063, 065, 504
ББК 20, 32, 40
Известия студенческой науки. Выпуск 1. Том 4. Текстовое электронное издание (1899 Мб). СПб.: Университет ИТМО. 2025. 63 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 978-5-7577-0743-3 (Том 4)

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 004.056.5

РИСКИ КОМПРОМЕТАЦИИ IDENTITY PROVIDER КАК КЛЮЧЕВАЯ УГРОЗА ZERO TRUST

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 современном цифровом инфраструктуре, где взаимодействие распределённых систем и облачных сервисов стало неотъемлемой частью функционирования организаций, архитектура Zero Trust постепенно превращается из концептуальной модели в обязательный стандарт. Нарастающее число кибератак, направленных на инфраструктуру идентичностей, подчёркивает, что традиционная модель периметральной защиты больше не справляется со своей ролью. В центре Zero Trust неизбежно оказывается Identity Provider (IdP) – система, определяющая подлинность пользователя и формирующая доверие между субъектами и сервисами. Когда IdP работает корректно, он становится фундаментом безопасного взаимодействия, но при его компрометации всё построенное вокруг доверие рассыпается мгновенно. Влияние успешной атаки на IdP выходит далеко за пределы отдельной учётной записи. Злоумышленник получает возможность генерировать легитимно выглядящие токены, управлять федерацией, выдавать себя за любого пользователя или сервис. В итоге разрушается сам принцип Zero Trust, который предполагает постоянную проверку и невозможность получения доступа на основе одного лишь факта аутентификации. Статья анализирует специфику угроз, связанных с компрометацией IdP, показывает, каким образом они проявляются в реальных инцидентах и рассматривает рекомендации NIST как основу для повышения устойчивости организации к подобным атакам.
Ключевые слова
Zero Trust, Identity Provider, идентичность, федерация, компрометация ключей, MFA.

Развитие облачных технологий, гибридных корпоративных сред и удалённого доступа постепенно сделало идентичность основным механизмом, определяющим, кто и к чему может получить доступ. Zero Trust базируется на том, что доверие должно постоянно проверяться, а сама аутентификация не являться гарантом безопасности. В этой среде IdP становится своеобразным центром мира. Он подтверждает подлинность субъекта, формирует утверждения и выдаёт токены, которые затем принимают сервисы. Именно этот компонент становится ключевой точкой, через которую проходят все решения о допуске, и поэтому угроза его компрометации выглядит особенно значимой. Цель статьи рассмотреть, почему атаки на IdP обладают разрушительным характером, какие механизмы атак используются сегодня и какие защитные меры позволяют снизить уровень риска.

Когда речь заходит о современных подходах к обеспечению безопасности, разговор неизбежно возвращается к идентичности как основному объекту защиты. Zero Trust создаёт правила, в которых доступ нельзя получить по умолчанию, а требуется непрерывная проверка контекста, устройства, сети, поведения и множества других факторов. Однако именно IdP объединяет эти аспекты в единое решение. Он выступает источником утверждений, которые доверенные сервисы принимают как основу фактов об идентичности субъекта. В этом доверии и заложен парадокс: чем больше ответственности концентрируется в одном компоненте, тем страшнее последствия его компрометации. Если злоумышленник получает возможность выдавать токены, подписанные легитимным ключом IdP, он фактически может превращаться в любого пользователя системы. Identity Provider – это не просто сервис аутентификации. В логике федераций он выполняет функцию посредника, который подписывает утверждения, действующие как дипломатические грамоты,

следовательно сервисы принимают их без сомнений, ведь подпись соотносится с заранее установленным доверительным соглашением. В NIST SP 800-63C подчёркивается центральная роль криптографически подписанных утверждений, в которых указываются идентификатор субъекта, сведения об аутентификации и атрибуты, определяющие права доступа. Когда злоумышленник получает доступ к ключу подписи IdP, он получает возможность штамповать такие «дипломатические паспорта» в любом количестве. Именно поэтому компрометация ключей подписи рассматривается как угроза высшего уровня. Нельзя забывать и о конфигурационном аспекте. В крупных облачных средах, например Entra ID, федерационная конфигурация определяет доверенные источники аутентификации. Приводилось несколько случаев, когда группы уровня UNC3944 создавали фальшивые федерации, подменяя их в административном интерфейсе. В результате злоумышленник добавлял собственный IdP как доверенный, после чего выдавал сам себе любые утверждения. Не требовалось даже красть ключи: достаточно было иметь административный доступ, полученный через фишинг или атаки adversary-in-the-middle. Подобное изменение федерационных настроек проходило незаметно для пользователей, но полностью меняло структуру доверия системы. По мере развития угроз становится заметно, что злоумышленники всё чаще действуют не грубой силой, а точечными вмешательствами в механизмы идентичности. Microsoft в своём отчёте подчёркивает, что более 97% атак на предприятия связаны именно с идентичностями. Идентичность стала новой целью атаки. В отличие от паролей и сессий, которые можно отозвать, компрометация IdP приобретает стратегический характер, злоумышленник может находиться внутри системы месяцами, при этом каждый раз подтверждая себя легитимным токеном. Именно поэтому ITDR-подход (Identity Threat Detection and Response) становится важнейшим направлением развития защиты, так как он позволяет распознавать аномалии в конфигурации IdP, отслеживать редкие изменения параметров федерации и автоматически отзывать подозрительные токены. Если внимательно рассмотреть угрозы, связанные с IdP, становится ясно, что большинство из них сводится к трём ключевым категориям, а именно к компрометации ключей подписи, административных полномочий и манипуляции доверительными соглашениями. Компрометация ключей подписи позволяет злоумышленнику создавать токены, которые выглядят абсолютно легитимными. Административный доступ обеспечивает возможность менять параметры федерации, добавлять новые доверенные отношения или даже заменять ключи подписи. Манипуляции федерацией открывают путь для создания rogue-IdP – поддельного поставщика идентичности, которому сервисы начинают доверять в силу фальсифицированной конфигурации. В условиях Zero Trust подобная атака разрушает фундамент, на котором держится вся модель [1-5].

В практическом плане компрометация IdP превращает Zero Trust в фикцию. Сервисы продолжают выполнять проверки токенов, но не могут установить факт подлинности субъекта, поскольку доверяют подписи и структуре утверждения. При этом в утверждении могут быть подменены не только идентификаторы пользователей, но и атрибуты, а то есть роли, разрешения, уровни доступа. Таким образом, злоумышленник может не просто «войти» в систему, а войти сразу как администратор, сервисная учётная запись или критически важное приложение. В таком случае принцип «никому не доверять» оказывается нарушен на самом базовом уровне.

С ростом количества облачных интеграций угроза IdP-компрометации становится всё масштабнее. В современной архитектуре один IdP может обслуживать сотни сервисов, от почтовых систем до финансовых платформ. Потеря контроля над IdP приводит к тому, что злоумышленник получает доступ ко всему спектру корпоративных ресурсов, не прибегая к отдельным атакам на каждый сервис. Подобная ситуация превращает IdP в критическую точку единой неустранимой компрометации. Организациям сложно понять масштаб ущерба, особенно если атака остаётся незамеченной продолжительное время, а такие случаи уже происходили, злоумышленникам удавалось сохранять доступ через поддельные федерации неделями [4].

Рассматривая меры защиты, можно выделить несколько направлений. В первую очередь, речь идёт о защите ключей подписи, а именно хранение их в HSM, минимизация числа администраторов, проведение ротации с разумной периодичностью и контроль за всеми операциями. CISA подчёркивает, что stateless-токены особенно опасны в условиях компрометации ключей, поскольку их невозможно отозвать при помощи механизма серверной проверки. Это заставляет организации внимательно подходить к использованию подобных токенов в критических системах. Следующим направлением является использование механизмов MFA, устойчивых к фишингу. Microsoft показывает, что phishing-resistant MFA блокирует почти все современные атаки, ориентированные на кражу токенов или перехват сессий. Такие факторы, как аппаратные ключи, FIDO-совместимые токены и протоколы с привязкой к устройству, формируют новую основу доверия, сложнее подделываемую и менее уязвимую к атакам посредника. Немаловажную роль играет контроль конфигурации. Организациям необходимо отслеживать любые изменения в федерации, trust agreements, параметрах OAuth и SAML-интеграций. Инструменты ITDR позволяют обнаруживать редкие или подозрительные изменения, которые могут указывать на попытку манипуляции IdP. Регулярные аудиты, автоматические уведомления, контроль над административными привилегиями и разделение ролей снижают вероятность того, что злоумышленник сможет беспрепятственно изменять параметры доверия [3, 5].

С практической точки зрения одной из важнейших мер становится готовность к быстрому реагированию. В случае малейших подозрений на компрометацию IdP организация должна иметь возможность быстро ротировать ключи, отзывать токены, пересоздавать конфигурацию федерации и блокировать все административные сессии. NIST и CISA подчеркивают необходимость планов contingency response именно для инфраструктуры идентичностей, поскольку время реакции здесь определяет степень ущерба [1, 3].

Компрометация IdP формирует угрозу системного уровня, способную дестабилизировать всю архитектуру Zero Trust, поскольку подрывает главный принцип – проверку подлинности каждого запроса. Потеря контроля над ключами подписи, федерационными настройками или административными привилегиями делает невозможным различение легитимных и поддельных токенов, нарушает механизмы атрибутивного доступа и позволяет злоумышленнику действовать в статусе любого пользователя или сервиса. Исследования показывают, что подобные атаки уже давно перестали быть редкостью и всё чаще становятся долгосрочными, скрытыми и сложно обнаруживаемыми. Минимизировать такие риски можно только комплексным подходом, включающим защиту ключей подписи, применение стойкой к фишингу многофакторной аутентификации, постоянный контроль параметров федерации и использование ITDR-практик для мониторинга аномалий в поведении систем идентичности. Zero Trust по-прежнему остаётся эффективной концепцией, но лишь при условии сохранения целостности и надежности IdP как центрального узла доверия.

Литература

1. NIST. Zero Trust Architecture: Special Publication 800-207 [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (Дата обращения 20.11.25).
2. NIST. Digital Identity Guidelines: Federation and Assertions. SP 800-63C [Электронный ресурс]. Режим доступа: https://pages.nist.gov/800-63-4/sp800-63c.html (Дата обращения 20.11.25).
3. CISA. Securing Core Cloud Identity Infrastructure: Addressing Advanced Threats through Public-Private Collaboration [Электронный ресурс]. Режим доступа: https://www.cisa.gov/news-events/news/securing-core-cloud-identity-infrastructure-addressing-advanced-threats-through-public-private (Дата обращения 20.11.25).
4. Mandiant. M-Trends 2024 [Электронный ресурс]. Режим доступа: https://services.google.com/fh/files/misc/m-trends-2024.pdf (Дата обращения 20.11.25).
5. Microsoft. Microsoft Digital Defense Report 2025 [Электронный ресурс]. Режим доступа: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf (Дата обращения 20.11.25).

УДК 373.1

ПРИЧИНЫ И ПОСЛЕДСТВИЯ ПЕРЕГРУЖЕННОСТИ УЧЕНИКОВ В ЯПОНСКОМ ШКОЛЬНОМ ОБРАЗОВАНИИ

Новиков В.В.[1] (магистрант), **Большаков Г.В.**[1] (магистрант), **Рогаткин Н.А.**[1] (магистрант)
Научный руководитель – кандидат технических наук Бутылкина К.Д.[1]
[1]Университет ИТМО
work_vladmir_novikov@mail.ru

Аннотация
Статья посвящена проблеме перегруженности школьников в Японии и её социальным, культурным и экономическим аспектам. Японская школа является не только образовательным, но и социальным институтом, формирующим ценности, поведение и готовность к роли в обществе. Анализ исторического развития школьной системы показывает, что её современная структура сложилась под влиянием модернизации, экономического роста и конкуренции за престижные учебные заведения. Экзаменационная система и интенсивная подготовка к поступлению в старшие школы и университеты создают высокую нагрузку на учащихся, что стимулирует развитие дополнительного образования через juku и yobiko. Перегрузка проявляется не только в объёме формальных занятий, но и во внеклассной деятельности, домашних заданиях и подготовке к экзаменам, влияя на психическое и физическое здоровье школьников, включая тревожность, депрессивные симптомы и социальную изоляцию. Нагрузка распространяется также на педагогов, вовлечённых во внеурочную работу и организацию школьной жизни. Социальные последствия перегрузки включают рост образовательного неравенства и закрепление классовых различий. Реформы, направленные на снижение нагрузки, показали ограниченную эффективность из-за устойчивости системных стимулов и адаптивного поведения учащихся и семей. Опыт Японии может быть полезен для других стран в части системной организации и уважения к учителю, однако чрезмерная зависимость от экзаменов и коммерциализации образования создаёт риски для благополучия детей и справедливости системы.
Ключевые слова
Школьное образование, дополнительное образование, педагогическая нагрузка, Япония.

Школьное образование формирует у человека не только набор знаний, но и модель поведения, систему ценностей и готовность к роли в обществе. В Японии школа выступает как мощный институт, который с ранних лет включает ребёнка в систему взаимных ожиданий и нормативов. Именно поэтому вопрос о перегруженности школьников в этой стране имеет большую социальную значимость и требует комплексного анализа. Данная статья анализирует причины и последствия перегруженности учащихся в японской школьной системе.

Школьная система Японии отразила в себе исторические этапы модернизации и национального развития. В послевоенный период образование приобрело массовый характер и служило ресурсом для восстановления экономики. В последующие десятилетия рост промышленности и усложнение трудового рынка усилили значение качества образования как фактора индивидуального и национального успеха. С ростом значимости высшего образования и престижных учебных заведений появилась острая конкуренция за места. Она стала основой для формирования институциональных традиций и культурных стереотипов, которые превратили школу в механизм отбора. Экзамены стали главным инструментом, с помощью которого осуществляется распределение и определяются семейные стратегии инвестирования в образование. Попытки смягчения нагрузки производились, например, через реформы, известные как yutori, которые предполагали сокращение объёма формального материала и изменение учебных программ. Однако реформы зачастую действовали на формальном уровне и не устраняли коренной стимул к интенсивной подготовке. Семьи и учащиеся адаптировали своё поведение и начали переносить усилия во внешкольные каналы. Исторический анализ показывает, что современная система образования включает в себя как официальные учебные заведения, так и обширную сеть

дополнительного образования, которая стала неотъемлемой частью образовательной инфраструктуры.

Перегруженность школьников нельзя свести к одному фактору, так как это комплекс причин, где взаимодействуют организационные, культурные и экономические элементы. Учебный план и школьное расписание сами по себе задают существенный объём учебной нагрузки. Учебная программа предусматривает изучение широкого спектра дисциплин и выполнение домашних заданий. Следует отметить, что фактическая нагрузка на школьников не ограничивается официальным расписанием. Система образования включает в себя разнообразные внеклассные клубы, мероприятия и обязанности, которые, хоть и не имеют четкого регламента, тем не менее отнимают время у детей [3].

Экзаменационная система является одним из основных факторов, способствующих перегрузке. Она делает будущие возможности настолько зависимыми от результатов единоразовых экзаменов, что стимулирует раннюю и интенсивную подготовку. В результате возникает рынок репетиторских и подготовительных услуг, который активно используется семьями с достаточными ресурсами для повышения шансов своих детей на успех. В связи с широким распространением таких образовательных учреждений, как juku и yobiko, дополнительное образование стало не только желательным, но и фактором, влияющим на социальное расслоение. Этот сектор создаёт эффект двойного обучения, поскольку школьные программы повторяются вне школы для подготовки к экзаменам. Культурные установки могут оказывать значительное влияние на структурные факторы. Групповая культура, уважение к усилиям и нормам, а также ожидания родителей относительно академических успехов формируют восприятие образовательной деятельности как совместного проекта семьи и школы. Это, в свою очередь, снижает индивидуальную готовность отказываться от интенсивной подготовки, даже если родители и дети осознают её потенциальный вред [1, 5].

Официальные отчёты указывают что формальное учебное время для средней и старшей школы составляет от тридцати часов в неделю. Эта цифра относится к официальным урокам и не охватывает внеурочную деятельность в клубах, занятиях у репетиторов и домашнюю работу. Также опросы показывают, что примерно треть учащихся систематически посещают дополнительные занятия каждый день, либо регулярно в выходные. При интенсивной подготовке к экзаменам число часов внешкольной подготовки может достигать десяти и более часов в неделю и более в периоды активной подготовки. В то же время рабочая неделя учителя в Японии по данным международных исследований часто превышает пятьдесят часов в неделю что делает японских педагогов одними из наиболее загруженных в мире. Большая часть этих часов связана с внеклассной работой, организацией клубов и административными задачами. Исходя из этого можно сделать вывод о том, что системная перегрузка действует одновременно на учеников и на учителей [3, 4].

Данные по психическому здоровью отражают тревожные сигналы. Статистика по обращениям за психологической помощью и по случаям самоубийств демонстрирует всплески в периоды экзаменационной нагрузки. Это не означает что экзамены являются единственной причиной, но они выступают одним из ключевых факторов стресса. Постоянная и большая учебная нагрузка вызывает у учащихся хронический стресс. Он сказывается на концентрации внимании, на способности к восстановлению и на общем эмоциональном фоне учащегося. Такие состояния ведут к повышенному уровню тревожности изменению режима сна и снижению мотивации. Исследования показывают, что дефицит сна связан с ухудшением когнитивной функции эмоциональной регуляции и ростом риска депрессивных симптомов. Учитывая, что многие школьники сокращают сон в пользу подготовки, ситуация влечёт за собой накопительный эффект. Особое внимание вызывает феномен социальной изоляции hikikomori и случаи самоизоляции, когда подросток уходит из общественной жизни. В литературе отмечается сложная связь между академическим давлением и ростом проявлений социальной дезадаптации. Для ряда молодых людей постоянное ощущение невозможности соответствовать ожиданиям приводит к уходу от школы и общества. Психологические последствия также проявляются в поведении учеников.

Например, учащаются случаи пропусков занятий, возникают конфликты в классе, а интерес к учёбе падает. В долгосрочной перспективе это может привести к снижению творческой инициативы и сужению возможностей для выбора карьерного пути [1, 4].

Перегрузка учащихся может привести к увеличению неравенства в обществе. Когда возможность получить дополнительную подготовку становится важным условием для поступления, семьи с более высоким доходом получают значительное преимущество. Это способствует тому, что образование перестаёт быть исключительно показателем способностей и превращается в инструмент, отражающий уровень семейного капитала. Для системы образования такая ситуация означает, что отбор по уровню образования усиливает социальную стратификацию и снижает мобильность населения. В долгосрочной перспективе это может привести к закреплению классовых различий и снижению социальной сплочённости. На уровне семьи экономические последствия проявляются в увеличении расходов на образование и перераспределении семейных ресурсов в пользу репетиторов. Это, в свою очередь, влияет на потребительские расходы и может негативно сказаться на экономическом благополучии семей [1, 2, 4].

В японском образовании педагогическое взаимодействие строится на принципах сотрудничества, соглашения и опеки, а роль партнёрства ограничена. Такая модель предполагает высокую вовлечённость учителя во внеклассную деятельность и воспитательные практики, что одновременно усиливает социальную поддержку учащихся и создаёт дополнительную нагрузку на педагогов. Типология педагогических отношений в японской школе демонстрирует, что механизмы групповой ответственности и практики букацу способствуют социальной интеграции и воспитанию коллективизма, что даёт преимущества в поддержании социальной дисциплины и профилактике девиантного поведения. Однако, с другой стороны, повышенная вовлечённость учителя во внеурочную работу приводит к увеличению его временных затрат и росту системной нагрузки. Таким образом, педагогическое взаимодействие в японском образовании выступает одновременно как ресурс, поддерживающий учащихся, и как фактор, который может привести к перегрузке человеческих ресурсов системы. Это делает его ключевым объектом для любых реформ, направленных на снижение нагрузки [5].

Реформы, направленные на снижение учебной нагрузки, показали неоднозначные результаты. Переход к более «естественным» формам оценивания и попытки сократить количество формального материала иногда приводили к снижению учебной нагрузки. Однако зачастую это вызывало адаптацию в виде увеличения дополнительных занятий, что свидетельствует о стойкости системных стимулов и необходимости комплексного подхода. Сравнение с зарубежными моделями позволяет выявить потенциально полезные элементы. Например, подходы, ориентированные на развитие компетенций и на постоянную оценку вместо единичных экзаменов, в некоторых странах показывают снижение давления экзаменов и способствуют более равномерному распределению учебной нагрузки. Тем не менее, любой перенос практик требует адаптации к культурному и институциональному контексту [1].

Особое значение в данном контексте приобретает российский опыт. В последнее время система на основе ОГЭ и ЕГЭ двигается по тому же пути, что и японская экзаменационная система, она становится всё более зависимой от интенсивного репетиторства и внешкольной подготовки. Успех на экзамене всё чаще определяется не только школьной программой, но и объёмом дополнительных занятий, что создаёт риск формирования аналогичной модели неравенства, где доступ к качественной подготовке зависит от материальных ресурсов семьи. Такая тенденция фактически подталкивает систему к усилению коммерциализации образования и росту давления на учащихся, повторяя те проблемы, которые Япония уже переживает. Российская школа, чтобы избежать накопления перегрузки и социального разрыва, должна рассматривать японский опыт не как образец, а как предупреждение того, что чрезмерная опора на единый экзамен и рынок репетиторства в долгосрочной перспективе подрывает благополучие детей, снижает мотивацию и ухудшает справедливость системы. Противодействие этим процессам требует развития альтернативных форм оценивания,

расширения возможностей для школьного обучения и укрепления роли государства в обеспечении равного доступа к образовательным ресурсам.

Японская школьная система имеет сильные институциональные преимущества и одновременно встроенные механизмы перегрузки. Система способствует развитию высокой организованности, ответственности и дисциплины, что, в свою очередь, помогает ученикам добиваться высоких академических результатов. Однако сочетание факторов, таких как экзамены, коммерциализация дополнительного образования, групповые культурные установки и демографическая конкуренция, приводит к тому, что многие дети сталкиваются с хронической нагрузкой. И именно это, в свою очередь, негативно сказывается на их психическом и физическом здоровье, семейных бюджетах и устойчивости всей образовательной системы в целом.

Из японского опыта другие страны могут позаимствовать организованность, уважение к учителю, системный подход и стремление к качеству. Однако стоит избегать практик, при которых экзамены становятся важнее благополучия учеников, коммерциализация образования приводит к усилению неравенства, а школьная жизнь не оставляет детям времени на отдых и творческое развитие. Образование должно быть инструментом для развития личности и общества, а не просто способом отбора. Чтобы решить проблему перегрузки, необходимы комплексные меры, направленные на оценивание, обеспечение доступности, поддержку учителей и изменение общественных ценностей, чтобы достичь баланса между результатами и благополучием.

Литература

1. Wiggins G. A true test: Toward more authentic and equitable assessment. The Phi Delta Kappan, 1989. №. 70. Pp. 703–713.
2. В чем отличия школ Японии от школ России. [Электронный ресурс]. Режим доступа: https://need4study.com/articles/5127 (Дата обращения 01.12.25).
3. Мачехина О.Н. Средняя школа в Японии. [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=29256677 (Дата обращения 01.12.25).
4. Учись, трудись, не выделяйся как устроено школьное образование в Японии. [Электронный ресурс]. Режим доступа: https://pedsovet.org/article/ucis-trudis-ne-vydelajsa-kak-ustroeno-skolnoe-obrazovanie-v-aponii (Дата обращения 01.12.25).
5. Данилова Л.Н. Педагогическое взаимодействие в японской школе как социокультурный феномен // Коммуникативные исследования. 2023. Т. 10. №. 1. С. 165–180.

УДК 004.056.5

ЭВОЛЮЦИЯ ZERO TRUST: ПРОБЛЕМЫ МАСШТАБИРОВАНИЯ И ЗРЕЛОСТИ ВНЕДРЕНИЯ

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
Современное развитие корпоративных информационных систем показывает, что переход от периметровой модели к архитектуре минимального доверия является неизбежным следствием усложнения цифровых экосистем, роста облачных сред и распределённости вычислений. Однако, несмотря на интенсивное продвижение концепции Zero Trust в индустрии, фактическая зрелость её внедрения остаётся ограниченной. В основе исследования лежит анализ четырёх источников, описывающих эволюцию Zero Trust, практический опыт внедрения в крупных организациях, а также структурные и операционные препятствия, возникающие в процессе трансформации архитектуры доверия. Результаты анализа показывают существенный разрыв между заявленными моделями и реальной практикой. Управление идентичностями является наиболее зрелым компонентом, однако сохраняет фрагментарный характер из-за гибридных систем, распределённых каталогов и неполной интеграции сигналов. Сетевой контроль и сегментация в большинстве организаций применяются ограниченно и не достигают уровня, необходимого для предотвращения бокового перемещения внутри инфраструктуры. Динамическая оценка контекста практически не реализуется вследствие отсутствия унифицированной телеметрии и недостаточной автоматизации процессов принятия решений. Наиболее значимым препятствием остаётся наследуемая инфраструктура, не поддерживающая механизмы Zero Trust и формирующая островные зоны доверия, противоречащие самой сути модели. Полученные выводы позволяют сделать обобщённый вывод о низкой зрелости реализации Zero Trust в корпоративном секторе и определить ключевые направления дальнейшего развития, включая расширение автоматизации, модернизацию наследуемых систем, усиление сегментации и построение единой архитектуры сигналов и политик доступа.

Ключевые слова
Zero Trust, сегментация, наследуемая инфраструктура, корпоративная безопасность, автоматизация политик.

Трансформация корпоративной кибербезопасности в последние десять лет демонстрирует чётко выраженную тенденцию перехода от периметровой модели к архитектурам, основанным на принципах минимального доверия и непрерывной проверки подлинности субъектов, устройств и сервисов. Концепция Zero Trust стала одним из ключевых ориентиров этой трансформации, однако анализ современных корпоративных практик показывает, что между теоретической моделью и её фактической реализацией существует глубокий разрыв. Несмотря на широкое распространение терминологии Zero Trust, программы внедрения часто ограничиваются отдельными технологическими элементами, тогда как сама концепция предполагает фундаментальную перестройку механизмов доверия, моделей взаимодействия и процессов контроля доступа.

Классические подходы, которые долгое время формировали корпоративную безопасность, опирались на предположение о существовании надёжного внутреннего периметра и разделении мира на «доверенные» и «недоверенные» зоны. Расширение облачных сервисов, массовая удалённая работа, развитие микросервисных архитектур и растущая мобильность вычислений привели к тому, что этот принцип утратил актуальность. Исследования поднимают важный вопрос о том, что концептуальная эволюция Zero Trust опередила способность организаций перестроить инфраструктуру и процессы таким образом, чтобы фактически реализовать заявленные принципы.

Критический анализ существующих решений показывает целый комплекс проблем. На уровне идентичностей многие компании внедряют многофакторную аутентификацию, но не переходят к полнофункциональной модели управления контекстом, необходимой для

динамической оценки риска. В области сегментации широко заявляется о применении микро-сегментации, но фактическая практика всё ещё ограничивается крупными сетевыми зонами, которые не препятствуют боковому перемещению злоумышленников. В части инфраструктуры сохраняется значительный объём наследуемых систем, не поддерживающих современные требования Zero Trust. Наблюдаемые внедрения демонстрируют борьбу между стремлением к повышению уровня контроля и реальными операционными ограничениями крупных организаций, которые вынуждены функционировать в условиях высокой сложности и множественности технологических слоёв.

Особенность предлагаемого подхода заключается в рассмотрении Zero Trust не как набора разрозненных решений, а как целостной модели, определяющей правила принятия доступа, характер доверительных сигналов и структуру сетевых и облачных взаимодействий. Такой ракурс позволяет выявить разницу между формальным соблюдением отдельных принципов и их реальным содержательным исполнением. Четыре рассматриваемых источника дают возможность сформировать комплексное представление о проблеме, поскольку сочетают практический опыт крупных организаций, аналитические выводы индустриальных лидеров и независимые оценки исследователей. Такой подход обеспечивает целостное понимание эволюции концепции и фактической зрелости её внедрения [1–4].

Формирование Zero Trust проходило постепенно и отражало переосмысление принципов доверия в цифровых экосистемах. На ранних этапах внимание уделялось усилению контроля при доступе к сетевым ресурсам и сокращению поверхности атаки в условиях исчезновения понятного внутреннего периметра. Позднее стало очевидно, что распределённые системы обладают такой сложностью, что прежнее понимание доверенной среды утратило смысл, поэтому возникла идея оценивать каждый запрос доступа динамически, независимо от местоположения пользователя или сервиса. В дальнейшем развитие концепции сопровождалось переходом от локальных механизмов к облачным моделям управления доступом и идентичностями, что расширило понимание Zero Trust и позволило рассматривать его как комплексный подход, охватывающий устройства, приложения, данные, инфраструктуру и мониторинг. Аналитические обзоры подчеркивают, что историческое развитие шло неоднородно. Концепция складывалась из множества инициатив, каждая из которых устраняла слабости в своей области. Это привело к тому, что разные организации по-разному представляют себе суть Zero Trust и нередко сводят его к сегментации, управлению идентичностями или проверке состояния устройств. Такой разнобой стал одной из причин частичных и несогласованных программ внедрения. Исследования показывают, что современный этап характеризуется ориентацией на работу с сигналами доверия, автоматизацию решений и оценку риска в реальном времени. Такой подход трудно свести к традиционным методам аутентификации или сетевым политикам, поскольку он предполагает постоянную интеграцию данных из множества элементов цифровой экосистемы. Анализ показывает общую траекторию развития от защиты периметра к защите каждого запроса, от сетевой логики к логике идентичностей, от статических правил к анализу контекста и от разрозненных инструментов к согласованной архитектуре сигналов. Данная траектория демонстрирует ускорение смысловой и технологической сложности Zero Trust по сравнению с тем, как быстро организации способны перестраивать свои процессы и инфраструктуру [1, 3].

Управление идентичностями является фундаментом Zero Trust. Теоретическая модель требует строгой верификации каждого субъекта, системной оценки риска, проверки факторов аутентификации и анализа поведения. Исследования показывают, что именно эта область стала наиболее продвинутой в реальных корпоративных практиках, во многом благодаря развитию облачных платформ и широкому распространению многофакторной аутентификации. Однако реальная зрелость значительно ниже предполагаемой. В материалах подчёркивается, что фактическое внедрение ограничивается в основном MFA и частичной интеграцией с облачными службами. Многие компании сохраняют локальные каталоги, используют разрозненные домены и не обеспечивают единую модель телеметрии для процессов авторизации. Такой гибридный характер инфраструктуры затрудняет создание

сквозных политик. Также выделяют распространённую ошибку восприятия, когда компании смотрят на MFA как на конечную цель, тогда как Zero Trust требует непрерывной проверки контекста — состояния устройств, поведения пользователя, геолокационных отклонений, уровня риска. Этот разрыв между пониманием и реализацией является одной из главных причин, почему зрелость программ внедрения оценивается экспертами как низкая. Отмечается и проблема фрагментации систем управления идентичностями. Организации используют облачные IDaaS-сервисы, локальные каталоги, специализированные IAM-платформы и множество приложений со встроенной авторизацией. В результате единая политика доступа становится труднореализуемой, а логика принятия решений неполной. Следовательно, управление идентичностями демонстрирует наибольшую степень приближения к Zero Trust среди всех компонентов, однако остаётся далёким от идеала. Фактическая зрелость ограничена отсутствием координации между системами, разрывами в телеметрии, наличием локальных компонент и недостаточным применением поведенческих моделей анализа риска. Сегментация сети является одним из ключевых принципов Zero Trust, направленным на предотвращение бокового перемещения внутри инфраструктуры. Однако подчёркивают, что именно эта область является минимально зрелой. Большинство корпоративных сетей изначально создавались как монолитные или лишь условно разделённые на крупные зоны. Такая структура не препятствует перемещению злоумышленника после первичного доступа. Подобная архитектура до сих пор типична для больших организаций, которым сложно внедрять микро-сегментацию из-за высокой плотности взаимосвязей между сервисами. Анализ развития подхода Zero Trust показывает, что его идеальная модель предполагает глубокую сегментацию, основанную на сервисных и поведенческих зависимостях, а не на физическом размещении систем. Но на практике компании чаще ограничиваются несколькими крупными сегментами и редко проводят детальный разбор реальных взаимосвязей между приложениями [2].

В практическом опыте внедрения Zero Trust отмечается, что организации нередко избегают сегментации на уровне отдельных сервисов, поскольку для этого требуется детальный разбор потоков, инвентаризация систем и точная настройка сетевых политик. Такая работа трудоёмка, затратна и усложняет оперативную адаптацию к изменениям инфраструктуры. В итоге сегментация часто остаётся формальной, а фактическая поверхность атаки почти не уменьшается. Дополнительную сложность создаёт смешанная среда, в которой многие сервисы распределены между локальными центрами обработки данных и облачными платформами. Это формирует новые зоны риска и требует согласованного контроля на границах сетей, что пока недоступно большинству компаний. В результате сегментация в крупных организациях остаётся на начальном уровне, применяется ограниченно и считается одним из самых сложных и дорогостоящих элементов Zero Trust.

Один из центральных принципов Zero Trust заключается в том, что доверие должно быть динамичным и зависеть от контекста запроса, включая риск, устройство, состояние сети, телеметрию поведения и соответствие политики. Реализация этой модели является наиболее технологически сложной и потому редко достигает зрелости. В аналитических обзорах по Zero Trust отмечается, что у большинства организаций отсутствует единая система телеметрии, охватывающая устройства, приложения, сети, облачные сервисы и инфраструктурные компоненты: данные обычно распределены между разрозненными решениями и не сводятся в общую логику принятия решений, что делает невозможным непрерывную проверку доверия. Автоматизация, являясь ключевым элементом Zero Trust, на практике заменяется статическими политиками, которые не учитывают изменения среды. Дополнительно подчёркивается культурный аспект: компании традиционно воспринимают безопасность как набор отдельных слоёв, тогда как Zero Trust требует их согласованной работы и постоянного анализа. В результате внедрение ограничивается частичными мерами без формирования целостной архитектуры сигналов, а динамическая оценка контекста остаётся одним из наиболее труднодостижимых элементов, поскольку требует унифицированной телеметрии, координации систем, машинного анализа и высокой степени автоматизации, что редко встречается в корпоративных инфраструктурах [1, 2].

Ключевым препятствием для внедрения Zero Trust остаются устаревшие корпоративные системы, не способные поддерживать необходимые принципы и механизмы. Отмечается, что во многих организациях продолжают функционировать локальные серверы, старые версии операционных систем, приложения без современной аутентификации и полноценного журналирования, из-за чего такие компоненты не могут предоставлять нужные сигналы безопасности и формируют гибридные зоны доверия. Подчеркивается, что модернизация подобных систем часто практически недостижима, как из-за технологических ограничений и несовместимостей, так и из-за высокой бизнес-зависимости от этих решений. В результате компаниям приходится оставлять их в качестве исключений, что нарушает целостность модели Zero Trust. Аналитические материалы также указывают, что новые элементы архитектуры вынуждены взаимодействовать поверх старых протоколов и инфраструктуры, создавая «островки доверия» и снижая управляемость отдельных сегментов. Такой дисбаланс делает невозможным равномерный контроль рисков и ограничивает масштабируемость, из-за чего фактический уровень зрелости Zero Trust остаётся низким [1–4].

Аналитическая оценка источников также показывает, что проблемы корпоративного внедрения Zero Trust не ограничиваются техническими аспектами. Они имеют глубокие организационные, культурные и процессные корни. Модель Zero Trust предполагает жёсткие механизмы проверки, строгий контроль доступа и существенные ограничения на перемещение данных между элементами инфраструктуры, что нередко вступает в противоречие с требованиями бизнеса, особенно при высокой динамике разработки цифровых продуктов. В аналитических обзорах отмечается, что чрезмерно строгие политики могут замедлять рабочие процессы и вызывать сопротивление со стороны команд, ориентированных на скорость и операционную эффективность. В итоге такие правила постепенно смягчаются, и архитектура безопасности превращается в набор компромиссных решений [3, 4].

Сегментация и принцип минимальных привилегий предполагают детальный разбор взаимодействий между системами, включая анализ сервисных цепочек, выявление зависимостей и определение минимально необходимых разрешений, однако на практике многим организациям не хватает ресурсов для такой работы или они избегают её из-за высокой стоимости и длительности, что приводит к чрезмерно широким доступам и ослаблению требований Zero Trust. Дополнительную сложность создаёт разнородность средств безопасности, когда одновременно используются локальные системы мониторинга, облачные инструменты оценки рисков и сетевые решения разных производителей, что приводит к фрагментации сигналов, снижению видимости и отсутствию непрерывного контроля. Также отмечается, что архитектура Zero Trust предполагает автоматическое принятие решений на основе телеметрии, но большинство компаний продолжают полагаться на ручные политики, из-за чего возникают задержки, ошибки и непоследовательность работы механизмов защиты, что делает модель малоэффективной в динамично меняющихся средах [1].

Анализ материалов позволяет выделить ряд основных выводов:

1. Корпоративное внедрение Zero Trust остаётся фрагментарным. Организации внедряют отдельные элементы, такие как MFA, сетевые решения, облачные IDaaS-сервисы, но не формируют целостную архитектуру визуальности и доверия.
2. Управление идентичностями является наиболее зрелой областью, но даже здесь остаются значительные ограничения, связанные с гибридной природой инфраструктуры.
3. Сегментация и контроль бокового перемещения являются наиболее слабыми областями. Большинство компаний ограничиваются крупными зонами, избегая микро-сегментации.
4. Динамическая оценка контекста реализована крайне слабо. Отсутствие единой телеметрии и автоматизации приводит к тому, что большинство решений принимается на основе статических правил.
5. Наследуемая инфраструктура является главным структурным барьером, препятствующим достижению зрелости.

Анализ четырёх источников позволяет сформировать целостное представление о зрелости внедрения Zero Trust в корпоративных средах. Несмотря на широкое распространение концепции, её реализация остаётся ограниченной, фрагментарной и несоответствующей принципам, которые лежат в её основе. Практика показывает, что многие организации сводят внедрение к отдельным инструментам, не перестраивая архитектуру доверия, что создаёт видимость прогресса, но не обеспечивает качественного изменения структуры безопасности. Ключевыми факторами, препятствующими развитию, являются наследуемая инфраструктура, отсутствие единой телеметрии, недостаточная сегментация, ограниченная автоматизация и культурные барьеры внутри организаций. Управление идентичностями демонстрирует наибольший прогресс, но даже оно сталкивается с ограничениями гибридных сред. Сегментация остаётся наименее зрелым элементом, а динамическая оценка контекста практически недостижима при существующей фрагментации инструментов. Тем не менее эволюция концепции Zero Trust продолжается, так как наблюдается рост интереса к унифицированным архитектурам сигналов, автоматизации принятия решений и переходу к более глубокому уровню сегментации. Дальнейшее развитие модели будет определяться способностью организаций синхронизировать процессы, модернизировать наследуемые системы и переосмыслить фундаментальные механизмы доверия. Только при выполнении этих условий Zero Trust сможет перейти из категории деклараций в категорию зрелых архитектур безопасности.

Литература

1. Weinert A. Evolving Zero Trust—Lessons learned and emerging trends [Электронный ресурс]. Режим доступа: https://www.microsoft.com/en-us/security/blog/2021/11/03/evolving-zero-trust-lessons-learned-and-emerging-trends/ (Дата обращения 17.11.2025).
2. IBM. The Evolution of Zero Trust and the Frameworks that Guide It [Электронный ресурс]. Режим доступа: https://www.ibm.com/think/insights/the-evolution-of-zero-trust-and-the-frameworks-that-guide-it?ysclid=mi4d7m962f235168399 (Дата обращения 17.11.2025).
3. Atwell E. The history, evolution, and controversies of zero trust [Электронный ресурс]. Режим доступа: https://1password.com/blog/history-of-zero-trust (Дата обращения 17.11.2025).
4. Loveless M. The evolution of Zero Trust [Электронный ресурс]. Режим доступа: https://about.gitlab.com/blog/evolution-of-zero-trust/ (Дата обращения 17.11.2025).

УДК 004.93:004.056

ЭВОЛЮЦИЯ DEEPFAKE: АНАЛИЗ ТЕХНОЛОГИИ И ИССЛЕДОВАНИЙ

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

Аннотация
Статья посвящена анализу эволюции технологий deepfake на основе исследований, охватывающих синтетические изображения лиц, мультимодальные аудиовизуальные deepfake, угрозы, создаваемые генеративным голосовым синтезом, и развитие индустрии цифровых аватаров. Показано, что современные модели генерации достигли уровня, при котором синтетические лица не только стали неотличимы от настоящих, но и воспринимаются как более надёжные, что указывает на смещение проблемы из области технической подделки в сферу когнитивной уязвимости человека. Анализ мультимодальных deepfake демонстрирует, что интеграция визуального и аудиального каналов делает подделку более устойчивой и снижает эффективность традиционных методов обнаружения. Исследования голосовых deepfake выявляют угрозы для биометрических систем, а также подчёркивают необходимость учёта микроструктур речи как наиболее устойчивых к манипуляциям элементов. Коммерческие разработки «цифровых копий человека», представленные индустрией цифровых аватаров, выводят deepfake за пределы манипулятивного использования, превращая его в инструмент цифровой идентичности, что вызывает новые этические и правовые вопросы. Полученные результаты демонстрируют, что deepfake-технологии формируют целостную экосистему цифрового воспроизведения человека, развитие которой требует комплексного подхода в сферах безопасности, регуляции и мультимодального анализа. В статье подчёркивается необходимость разработки систем детектирования нового типа, формирующих устойчивость как технических инфраструктур, так и когнитивных механизмов восприятия.

Ключевые слова
Deepfake, синтетические лица, голосовые подделки, цифровые аватары, биометрическая безопасность.

Технологии синтетической генерации аудио и видео данных, объединяемые общим термином deepfake, за последние годы прошли путь стремительного и качественного развития, радикально преобразовав медиапространство и вызвав необходимость фундаментального пересмотра представлений о достоверности цифрового контента. На протяжении долгого времени визуальные подделки оставались в зоне экспериментальных достижений энтузиастов, однако с появлением мощных генеративных архитектур ситуация изменилась, так как современные модели способны производить изображения человеческих лиц, которые не только неотличимы от настоящих, но и воспринимаются наблюдателями как более надёжные и вызывающие большее доверие. Этот неожиданный феномен стал ключевым аргументом в пользу того, что проблема deepfake больше не ограничивается вопросом технической точности. Она перешла в область когнитивной уязвимости человека и подрыва базовых механизмов доверия.

Параллельно с эволюцией визуальной составляющей deepfake происходил переход от статической подделки к динамическому мультимодальному воздействию. Появление крупномасштабных аудиовизуальных наборов данных, подобных AV-Deepfake1M, отражает масштаб и зрелость этой трансформации. Возможность моделировать многопрофильные подмены, включающие голос, артикуляцию, синхронизацию речи и мимику, открыла путь к созданию более совершенных систем генерации, которые воспроизводят человека не в виде фрагментарного искажения, а как связное медиапроявление личности. Одновременно исследования угроз, связанных с синтезированной речью, продемонстрировали, что вокальные deepfake способны обходить как человеческое восприятие, так и инфраструктурные системы подтверждения личности. Работа «Defending your voice against deepfakes» указывает на то, что голос становится одним из наиболее уязвимых векторов атаки, поскольку уже сегодня синтетическая речь может вводить в заблуждение не только

слушателей, но и биометрические алгоритмы, используемые в банковских и коммуникационных сервисах [2, 3].

Все эти тенденции происходят на фоне стремительно развивающейся индустрии коммерческих цифровых аватаров, где компании, такие как Tencent Cloud, создают высокореалистичные «цифровые копии человека», способные воспроизводить поведение человека по минимальному количеству входных данных. Коммерциализация deepfake превращает его из инструмента манипуляции в продукт массового применения – вместе с тем усиливая потребность в регуляции, защите и понимании технологической логики этих систем. Таким образом, данное исследование ставит целью анализ эволюции deepfake-технологий. Вначале обозначим ключевые проблемы, рассмотрим существующие решения и особенности подходов. Далее рассмотрим развитие технологий, проанализируем результаты экспериментальных работ. В заключении подведём итоги, обозначим последствия технологической эволюции и направления дальнейшего развития в контексте безопасности, когнитивной устойчивости и нормативной адаптации общества [4].

Эволюция deepfake-технологий тесно связана с постепенным усложнением генерируемого контента. Одним из первых значимых этапов стало достижение высокого качества синтезированных лиц, что убедительно показано в исследовании, посвящённом восприятию искусственно созданных изображений. Центральным результатом этого исследования является вывод о том, что синтетические лица не только неотличимы от реальных, но и обладают более высоким уровнем воспринимаемого доверия, что указывает на двойственную природу прогресса в области генеративных моделей, так как, с одной стороны, алгоритмы достигают уровня, при котором точность копирования превышает возможности человеческого анализа; с другой стороны, сама структура синтетического изображения оказывается так устроена, что оптимизационные процессы модели создают лицо, соответствующее статистическим ожиданиям «дружелюбности» и «надёжности». Данный эффект имеет глубокие последствия. Человек эволюционно приспособлен к чтению сигналов на лице, и эта способность является основой социального взаимодействия. Однако генеративная модель, формирующая изображение, не обязана воспроизводить реальные отклонения или микродефекты, присущие настоящим людям. Она создаёт обобщённый, симметричный и статистически усреднённый образ, который воспринимается как более привлекательный и честный. Возникает парадокс, что чем искусственнее изображение, тем более «надёжным» оно может казаться. Deepfake в данном контексте перестаёт быть «подделкой» и начинает выполнять роль семантического усилителя доверия, что открывает спектр манипулятивных возможностей – от политического воздействия до мошенничества [1].

Переход от визуальных deepfake к мультимодальным стал следующим этапом технологической эволюции. Создание масштабного датасета AV-Deepfake1M не является просто накоплением большого числа примеров. Оно отражает понимание того, что для глубокого моделирования человека необходима интеграция нескольких каналов передачи информации. Человек воспринимает другого человека не только глазами, но и через голос, интонацию, синхронность движений губ и мимики. Поэтому единичная подмена изображения может быть легко обнаружена визуальным вниманием, но синхронная подмена голоса и движения губ производит впечатление подлинности даже при наличии мелких неточностей. В лабораторных условиях, моделируемых датасетом, учитываются разные режимы: корректная синхронизация губ, намеренная рассинхронизация, замена отдельных участков лица, манипуляции голосом без изменения изображения и их комбинации. Всё это формирует среду, в которой алгоритмы обучения получают возможность работать с разнообразием фальсификаций, приближенных к реальным сценариям атак. Таким образом, мультимодальность становится не дополнительной функцией deepfake, а его структурной основой. Она усиливает вероятность успешной имитации человеческого поведения и делает обнаружение подделок значительно сложнее, поскольку каждый дополнительный канал синтеза повышает общую устойчивость ложного сообщения [2].

Особое место в развитии deepfake занимает голосовой синтез. Исследование «Defending your voice against deepfakes» показывает, что современные генеративные модели речи

обладают высоким уровнем точности, позволяющим им имитировать интонацию, тембр, артикуляционные особенности и вариативность живой речи. Такие возможности существенно меняют представление о медиапространстве, поскольку голос является одним из ключевых инструментов биометрической аутентификации. Если зритель может сомневаться в достоверности видео, услышанный голос традиционно воспринимается как гораздо более прямое подтверждение личности. В этом контексте deepfake-голос приобретает статус угрозы, превосходящей визуальные подделки по потенциалу вреда. Обман голосовых ассистентов, банковских сервисов, телефонных систем авторизации и автоматизированных служб техподдержки становится не гипотетической возможностью, а реальным риском. Исследователи указывают на то, что защитные механизмы должны учитывать микроструктуры речи, которые пока труднее всего подделать: микроколебания, нестандартные фонетические переходы, так называемые «биометки» голоса. Однако даже такие подходы зависят от качества обучающих выборок и должны развиваться одновременно с темпами улучшения генеративных архитектур. Голосовой deepfake в этом смысле демонстрирует важную закономерность: угрозы в сфере синтетической медиации распространяются не только на когнитивный уровень восприятия человеком, но и на технические системы, которые традиционно считались надёжными [3].

Наряду с научными исследованиями, направленными на анализ угроз, активно развивается и индустрия коммерческого использования deepfake-технологий. Материалы о разработках Tencent Cloud показывают, что сегодня возможно создание высокореалистичных «цифровых копий человека» – автономных аватаров, способных вести диалог, передавать эмоции, воспроизводить мимику и быстро адаптироваться к различным сценариям применения. Цифровой персонаж формируется по минимальному количеству исходных данных – иногда достаточно нескольких секунд видео, чтобы алгоритм смог реконструировать внешний облик и поведенческие особенности человека. Такой переход к цифровым двойникам отражает принципиально новый этап в развитии deepfake: от подделки зрительского восприятия – к созданию самостоятельной цифровой сущности. Цифровой персонаж уже не просто симулирует человека, он может существовать как виртуальная личность, выполнять информационные, образовательные, сервисные функции. В отличие от исследовательских deepfake, изготовленных для анализа уязвимостей, коммерческие цифровые аватары стремятся к максимальной выразительности, плавности движений, естественности речи и эмоциональности, что делает их частью экономики цифрового присутствия. Однако сама возможность создавать такие цифровые копии ставит ряд этических и социальных вопросов. Неясно, кому должна принадлежать цифровая копия человека, может ли она действовать от имени оригинала, какова юридическая ответственность аватара, каким образом предотвращать незаконное копирование реального человека в виртуальную форму. Все эти вопросы требуют комплексного анализа, поскольку цифровой персонаж встраивается в систему социального взаимодействия как новый тип субъекта [4].

Сопоставляя все представленные исследования, можно увидеть общую траекторию развития deepfake-технологий. Вначале совершенствовались модели генерации визуальных данных, которые достигли уровня неразличимости. Затем вектор сместился к мультимодальности, что привело к созданию больших аудиовизуальных наборов данных и появлению систем синхронного воспроизведения речи и мимики. Следующим этапом стала проблематизация угроз, связанных с голосовыми подделками, которые оказались особенно опасными для инфраструктурных систем. После чего развитие технологий привело к коммерциализации и созданию цифровых двойников, что расширило сферу применения deepfake и одновременно повысило риск нелегитимного использования подобных инструментов. Эволюция демонстрирует логическую закономерность, что чем большими возможностями обладает генеративная модель, тем ближе она приближается к созданию полноценной цифровой идентичности. Это, в свою очередь, требует выработки комплексных мер защиты, основанных на мультимодальном анализе, когнитивных исследованиях человеческого восприятия, технических методах обнаружения и нормативно-правовых механизмах регулирования.

Эволюция deepfake-технологий, проанализированная на основе исследований, показывает, что за сравнительно короткий период они превратились из экспериментального инструмента в сложную мультимодальную экосистему, способную формировать цифровые копии людей с высокой степенью достоверности. Исследование синтетических лиц демонстрирует, что человек оказывается уязвим не только перед технической точностью подделки, но и перед её психологической структурой, так как искусственные изображения воспринимаются как более надёжные и привлекательные. Анализ больших аудиовизуальных датасетов показывает, что подделка становится комплексным медиасобытием, объединяющим визуальные и аудиальные сигналы, тогда как исследования голосовых deepfake выявляют угрозы, затрагивающие биометрические системы и инфраструктурную безопасность. Коммерческое развитие deepfake, представленное примерами «цифровых копий человека», поднимает вопросы о том, как общество должно регулировать синтетические формы идентичности и какие механизмы должны предотвращать злоупотребления подобными технологиями. Возникает необходимость в создании новых моделей медиаграмотности, разработке методов комплексного мультимодального анализа, укреплении систем биометрической защиты и формировании нормативной базы, регулирующей права на цифровые копии.

Таким образом, deepfake перестал быть технологией подмены. Он стал частью широкой инфраструктуры цифрового воспроизводства человека. Его развитие требует междисциплинарного подхода, в котором технические, когнитивные, этические и юридические аспекты должны рассматриваться как взаимосвязанные элементы единой проблемы. В будущем ключевым направлением станет создание систем детектирования, учитывающих взаимодействие нескольких модальностей одновременно, а также формирование механизмов ответственного использования цифровых аватаров. Только комплексное понимание природы deepfake позволит минимизировать риски и использовать потенциал этих технологий во благо общества.

Литература

1. Nightingale S.J., Farid H. AI-synthesized faces are indistinguishable from real faces and more trustworthy. [Электронный ресурс]. Режим доступа: https://www.pnas.org/doi/epdf/10.1073/pnas.2120481119 (Дата обращения 19.11.2025).
2. Cai Z., Ghosh S., Adatia A.P., Hayat M., Dhall A., Gedeon T., Stefanov K. AV-Deepfake1M: A Large-Scale LLM-Driven Audio-Visual Deepfake Dataset. [Электронный ресурс]. Режим доступа: https://arxiv.org/pdf/2311.15308 (Дата обращения 19.11.2025).
3. Ballard S. Defending your voice against deepfakes. [Электронный ресурс]. Режим доступа: https://source.washu.edu/2023/11/defending-your-voice-against-deepfakes/ (Дата обращения 19.11.2025).
4. Tencent Cloud announced a small sample digital Homo sapiens production platform, which can be used to make digital humans by itself for thousands of yuan. [Электронный ресурс]. Режим доступа: https://www.jiemian.com/article/9312569.html (Дата обращения 19.11.2025).

УДК 004

ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РАЗРАБОТКИ АДАПТИВНЫХ СЕРВИСОВ РЕГИСТРАЦИИ МЕРОПРИЯТИЙ И СОБЫТИЙ

Хазов И.В.[1] (студент)
Научный руководитель – инженер факультета безопасности информационных технологий Ярцева Н.Г.[1]
[1]Университет ИТМО
khazovitmo@mail.ru

Аннотация
В статье рассматривается применение технологий искусственного интеллекта (ИИ) при создании адаптивных систем регистрации мероприятий. Анализируются ключевые ИИ-методы, их влияние на пользовательский опыт и операционную эффективность. Представлены практические сценарии внедрения, выявлены ограничения и предложены направления дальнейшего развития.

Ключевые слова
Искусственный интеллект, адаптивные системы, регистрация мероприятий, машинное обучение, персонализация, чат-боты, прогнозирование.

Введение

Современные сервисы регистрации мероприятий сталкиваются с растущими требованиями к персонализации, масштабируемости и удобству использования. Традиционные системы, основанные на жёстких шаблонах, не способны эффективно адаптироваться к разнообразным потребностям пользователей и динамичным условиям проведения событий.

Интеграция ИИ открывает возможности для создания адаптивных сервисов, которые:

- автоматически подстраиваются под поведение пользователя;
- предвосхищают потребности организаторов и участников;
- оптимизируют процессы на основе анализа больших данных.

Цель исследования — систематизировать подходы к внедрению ИИ в сервисы регистрации и оценить их практическую значимость.

Ключевые технологии ИИ для адаптивных сервисов

Применение методов машинного обучения является ключевым элементом создания адаптивных сервисов регистрации. Алгоритмы классификации и кластеризации позволяют системе «понимать» пользователя, выявлять скрытые закономерности в его поведении и на этой основе предоставлять персонализированный опыт.

На сегодняшний день к основным алгоритмам персонализации можно отнести k-means, Random Forest и Gradient Boosting.

k-means — алгоритм кластеризации, который группирует пользователей по схожести поведенческих и демографических признаков. Позволяет выделять сегменты аудитории с однородными потребностями [1, 2].

Random Forest — ансамбль решающих деревьев для задач классификации и регрессии. Эффективен для прогнозирования действий пользователя на основе множества признаков. Важно то, что в random forest каждое дерево строится независимо друг от друга на разных подвыборках обучающих данных. При этом при обучении каждого дерева используются разные комбинации признаков (характеристик) объектов, для которых делается предсказание, — поэтому деревья не похожи друг на друга [3–5].

Gradient Boosting (XGBoost, LightGBM) — метод машинного обучения, который последовательно создаёт набор слабых прогностических моделей (обычно деревьев решений), комбинируя их в единую сильную модель. Каждая новая модель в ансамбле стремится исправить ошибки, допущенные предыдущими моделями [6–8].

Помимо алгоритмов персонализированного направления к ключевым технологиям ИИ для адаптивных сервисов относят возможности обработки естественного языка, компьютерное зрение и модели прогнозирования и оптимизации (таблица).

Таблица

Технологии ИИ для адаптивных сервисов регистрации мероприятий

Технология	Ключевые алгоритмы/ модели	Входные данные	Функциональные возможности	Примеры применения
Машинное обучение для персонали-зации	k -means, Random Forest, алгоритмы классификации и кластеризации	История регистраций пользователя; демографические данные; поведенческие паттерны на платформе	Предложение релевантных мероприятий; адаптация формы регистрации под тип пользователя; прогнозирование вероятности участия	Персонализированная лента мероприятий, динамические регистрационные формы
Обработка естественного языка (NLP)	BERT, GPT и др. NLP-модели	Текстовые запросы, обращения в техподдержку, отзывы участников	Голосовые интерфейсы для регистрации; автоматическая классификация запросов в техподдержку; анализ отзывов для улучшения мероприятий	Чат-бот, реагирующий на команду *«Запиши меня на конференцию по ИИ в апреле»*
Компьютер-ное зрение	Алгоритмы распознавания образов, нейронные сети для анализа изображений	Изображения лиц, сканы заполненных форм, видеопоток с камер	Распознавание лиц для бесконтактной регистрации; анализ заполненных бумажных форм; мониторинг заполненности площадок в реальном времени	Система входа по Face ID, автоматизированная обработка анкет
Прогнозирова-ние и оптимизация	ARIMA, LSTM, модели временных рядов	Исторические данные о нагрузках, количестве мест, отменах; внешние факторы (сезонность, праздники)	Прогнозирование пиковых нагрузок на сервис; расчёт оптимального количества мест; оценка рисков отмены мероприятий	Планирование ресурсов платформы, динамическое ценообразование, управление вместимостью площадок

Обработка естественного языка (Natural Language Processing, NLP) — ключевая технология для создания интуитивно понятных интерфейсов взаимодействия пользователя с системой регистрации. Современные NLP-модели (BERT, GPT и их аналоги) позволяют «понимать» человеческий язык, извлекать смыслы и генерировать адекватные ответы, существенно повышая удобство и доступность сервисов [9, 10]. При этом важным отличием наиболее встрёпанных технологий BERT и GPT является то, что BERT не генерирует текст, а анализирует его, тогда как GPT создан для последовательного предсказания слов и требует больших вычислительных ресурсов.

Архитектура адаптивного сервиса

Типовая структура адаптивного сервиса включает в себя:

1. **Фронтенд** — адаптивный интерфейс с динамическими формами.

2. **Бэкенд** — микросервисы для обработки регистраций.
3. **ИИ-модуль** — ядро с моделями машинного обучения.
4. **Хранилище данных** — базы для пользовательских профилей и логов.
5. **API** — интеграция с календарями, платёжными системами, CRM.

Практические сценарии применения

В данном разделе рассмотрены три ключевых сценария внедрения интеллектуальных алгоритмов в цифровых сервисах: динамическая форма регистрации, интеллектуальное управление очередями и антифрод-система. Каждый из них демонстрирует, как машинное обучение повышает эффективность пользовательских взаимодействий и безопасность системы.

Динамическая форма регистрации

Динамическая форма регистрации представляет собой адаптивный интерфейс сбора пользовательских данных, который изменяет свою структуру в зависимости от контекста взаимодействия. Ключевыми механизмами адаптации выступают:

Для зарегистрированных (частых) участников система автоматически скрывает необязательные поля, минимизируя когнитивную нагрузку и сокращая время заполнения формы. Для новых пользователей, напротив, добавляются уточняющие вопросы, необходимые для первичного профилирования.

Контекстно-зависимые подсказки. На основе анализа текущего контекста (источник перехода, устройство, геолокация) система предлагает релевантные варианты ответов в выпадающих списках или автодополнении. Например, при указании страны автоматически подгружается список регионов и почтовых индексов.

Прогрессивное раскрытие информации. Форма раскрывается поэтапно: сначала запрашиваются критически важные данные, затем — дополнительные сведения, полезность которых зависит от предыдущих ответов.

К преимуществам данной системы можно отнести снижение отказов от заполнения форм на 20–40%, повышение конверсии регистрации и улучшение пользовательского опыта за счёт персонализации.

Интеллектуальное управление очередями

Система интеллектуального управления очередями оптимизирует распределение ресурсов (например, операторов колл-центра или серверных мощностей) на основе динамической оценки приоритетности запросов. Алгоритм работает по принципу адаптивного взвешивания параметров:

$$P_i = \sum_{j=1}^{n} w_j * f_j(x_i),$$

где P_i — приоритет -го запроса; w_j — весовой коэффициент -го параметра, настраиваемый через reinforcement learning; $f_j(x_i)$ — нормализованное значение -го фактора для запроса (например, время ожидания, критичность задачи, статус пользователя).

В результате применения данного алгоритма удается получить повышение удовлетворённости клиентов за счёт уменьшения времени ожидания на 30–50%.

Антифрод система

Антифрод система предназначена для выявления подозрительных регистраций и транзакций в реальном времени. Её работа базируется на многофакторном анализе аномалий IP адресов, платёжных данных и поведенческого анализа (в том числе выявления ботов, оценки последовательности и корректности заполнения форм). Как правило, система встраивается между формой регистрации и бэкендом. Система дает возможности почти полного блокирования массовых атак в режиме реального времени (90%).

Перспективы развития

Развитие цифровых систем регистрации и управления пользовательскими взаимодействиями движется в направлении всё более глубокой персонализации, повышения безопасности и расширения сфер применения. Рассмотрим ключевые технологические векторы, определяющие будущее этой области.

Одним из наиболее перспективных направлений является интеграция генеративных моделей искусственного интеллекта, таких как GPT-4 и её преемников. Подобные системы способны автоматически создавать содержательные и стилистически выверенные описания мероприятий на основе структурированных данных — дат, мест проведения, спикеров и ключевых тем. Это не только существенно сокращает трудозатраты организаторов, но и обеспечивает единообразие подачи информации, а также возможность быстрой адаптации текстов под разные целевые аудитории и каналы коммуникации. В перспективе генеративные модели смогут не просто формулировать описания, но и предлагать оптимальные форматы мероприятий исходя из анализа исторических данных и текущих трендов.

Важнейшим аспектом развития становится Federated Learning (федеративное обучение) — подход, позволяющий обучать модели машинного обучения на распределённых данных без их централизованного сбора. В контексте систем регистрации это решает острую проблему конфиденциальности: персональные данные пользователей остаются на локальных устройствах или в изолированных средах, а в центральный репозиторий передаются лишь обновлённые параметры модели [11–14]. Такой механизм особенно актуален для международных мероприятий, где необходимо соблюдать разнородные требования к защите данных (GDPR, CCPA и др.). Федеративное обучение открывает возможность совершенствовать алгоритмы персонализации и антифрода, не нарушая приватности участников.

Ещё одним многообещающим направлением выступает эмоциональный искусственный интеллект (эмоциональный ИИ) [15–17], способный анализировать тональность текстовых сообщений, интонации в голосовых взаимодействиях и даже микровыражения на видео. В системах регистрации это позволит адаптировать интерфейс и коммуникацию в зависимости от эмоционального состояния пользователя: например, предлагать дополнительную поддержку при признаках раздражения или сокращать количество вопросов при явной заинтересованности. Такой подход не только повышает удовлетворённость пользователей, но и снижает отток на этапах взаимодействия с формой регистрации. В долгосрочной перспективе эмоциональный ИИ может стать основой для динамического формирования программ мероприятий, учитывающих коллективное настроение аудитории.

Наконец, интеграция с метавселенными и платформами виртуальной реальности формирует принципиально новые сценарии участия в событиях. Системы регистрации эволюционируют от простого учёта физических или онлайн-участников к управлению доступом в гибридные и полностью виртуальные пространства. Это требует разработки унифицированных механизмов аутентификации, цифровых идентификаторов и смарт-контрактов для верификации присутствия. Регистрация на мероприятия в метавселенных будет включать настройку аватаров, выбор виртуальных локаций и синхронизацию с физическими активациями. Такие решения не только расширяют географию участников, но и создают возможности для иммерсивного взаимодействия — от сетевых сессий в 3D-пространствах до симуляций реальных площадок.

В совокупности эти технологии формируют экосистему интеллектуальных систем регистрации, где генеративные модели обеспечивают контентную гибкость, федеративное обучение — конфиденциальность, эмоциональный ИИ — эмпатичность взаимодействия, а метавселенные — новые форматы участия. Их синергия позволит перейти от механистического сбора данных к созданию адаптивных, интуитивно понятных и эмоционально резонансных пользовательских опытов.

Заключение

Проведённый анализ демонстрирует, что интеграция искусственного интеллекта кардинально трансформирует сервисы регистрации, переводя их из категории статичных инструментов сбора данных в разряд адаптивных экосистем, способных к динамической эволюции в соответствии с потребностями пользователей и организационными задачами. Ключевым достижением такой трансформации становится глубокая персонализация пользовательского опыта. Интеллектуальные системы перестают быть универсальными «воронками» ввода данных, превращаясь в гибкие интерфейсы, которые адаптируют

структуру, содержание и последовательность взаимодействия на основе контекста, истории взаимодействий и даже эмоционального состояния пользователя. Это не только повышает удобство и снижает когнитивную нагрузку, но и способствует росту конверсии за счёт релевантности предъявляемых требований.

Существенным преимуществом выступает автоматизация рутинных процессов — от предварительного заполнения форм до верификации данных и генерации сопроводительной документации. Освобождение персонала от монотонных операций позволяет перераспределить ресурсы на решение задач, требующих креативного подхода и эмпатического взаимодействия. Кроме того, автоматизация минимизирует человеческий фактор, снижая вероятность ошибок и обеспечивая единообразие обработки запросов.

Особую ценность представляет проактивное управление рисками, реализуемое через интеллектуальные антифрод-механизмы и предиктивную аналитику. Системы не просто реагируют на инциденты, но прогнозируют потенциальные угрозы на основе многофакторного анализа поведенческих паттернов, аномалий в данных и контекстных сигналов. Это создаёт многоуровневую защиту от мошенничества при сохранении плавности пользовательского пути.

Для успешной реализации подобных решений критически важно придерживаться поэтапного подхода, начиная с пилотных проектов, которые позволяют протестировать гипотезы, отладить интеграцию и оценить экономическую эффективность в контролируемых условиях. Не менее значима прозрачность алгоритмов: пользователи должны понимать логику принимаемых решений, а разработчики — иметь инструменты для интерпретации работы моделей. Это формирует доверие и снижает риски регуляторных нарушений.

Непрерывное совершенствование систем требует регулярной переобучения моделей на актуальных данных, что обеспечивает адаптацию к меняющимся паттернам поведения, новым видам угроз и эволюционирующим ожиданиям аудитории. Без этой итеративной работы даже самые продвинутые решения быстро теряют релевантность.

Таким образом, интеграция ИИ в сервисы регистрации открывает широкие возможности для оптимизации пользовательского опыта и операционной эффективности. Однако её успех зависит от гармоничного сочетания технологических инноваций, методологической строгости и этической ответственности.

Литература

1. Aliguliyev R., Tahirzada S.F. Performance comparison of K-means, parallel K-means and K-Means++ // Reliability: Theory & Applications. 2025. Vol. 20. №. SI 7 (83). Pp. 169–176. DOI:10.24412/1932-2321-2025-783-169-176.
2. Что такое K-means: принцип работы и применение алгоритма кластеризации. [Электронный ресурс]. Режим доступа: https://sky.pro/wiki/analytics/chto-takoe-k-means-printsip-raboty-i-primenenie-algoritma-klasterizatsii/ (Дата обращения 07.12.2025).
3. Фомина Е.Е. Использование алгоритма Random forest для обработки социально-экономических данных // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. 2022. №. 1. С. 142–153.
4. Адилжанова С.А., Кунелбаев М., Сыбанова Д.Д. Применение машинного обучения для анализа кибератак: исследование на основе датасета RT-IOT 2022 // Вестник Университета Шакарима. Серия технические науки. 2025. №. 2. С. 13–23. DOI: 10.53360/2788-7995-2025-2(18)-2.
5. Что такое random forest? [Электронный ресурс]. Режим доступа: https://sysblok.ru/glossary/chto-takoe-random-forest/ (Дата обращения 07.12.2025).
6. Azibaev A. The role of gradient boosting machines in modern economic analysis // Universum: технические науки. 2025. №. 6 (1 (130)). С. 11–14.
7. Адилхан А. Инструменты анализа данных и приложения для анализа данных в планировании спроса // Вестник науки. 2025. Vol. 1. №. 6 (87). С. 1343–1356. DOI:10.24412/2712-8849-2025-687-1343-1356.
8. Gradient Boosting: принципы работы и применение в машинном обучении. [Электронный ресурс]. Режим доступа: https://sky.pro/wiki/analytics/gradient-boosting-printsipy-raboty-i-primenenie-v-mashinnom-obuchenii/ (Дата обращения 07.12.2025).

9. Жусип М.Н., Жаксыбаев Д.О. Сравнение чат-ботов с использованием трансформеров и нейросетей: исследование применения архитектур GPT и BERT // Вестник науки. 2024. Vol. 2. №. 9 (78). С. 287–290.
10. Ахмедов Б.И.У. Эволюция и перспективы глубокого обучения: современные тенденции и направления развития // Raqamli iqtisodiyot (Цифровая экономика). 2025. №. 10. С. 1545–1552.
11. Ерофеева Е.А., Ерофеева Е.А. Применение искусственного интеллекта для решения проблем безопасности и анализа данных в образовательных учреждениях // Вестник магистратуры. 2025. №. 4-2 (163). С. 14–17.
12. Федеративное обучение: Полное руководство. [Электронный ресурс]. Режим доступа: https://www.getguru.com/ru/reference/federated-learning (Дата обращения 07.12.2025).
13. Ечиков К.И., Жмакин А.П. Анализ интеллектуальных методов оптимизации в системах распределенной пакетной обработки // Auditorium. 2025. №. 3 (47). С. 28–33.
14. Федеративное обучение: учимся вместе, не раскрывая секретов. [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/skillfactory/articles/880416/ (Дата обращения 07.12.2025).
15. Устинова А.Е. Эмоциональный интеллект и AI в отельном бизнесе // Вестник науки. 2025. Vol. 1. №. 9 (90). С. 254–269. DOI:10.24412/2712-8849-2025-990-254-269.
16. На пути к эмоциональному искусственному интеллекту. [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/sberbank/articles/926050/ (Дата обращения 07.12.2025).
17. Федосеева О.В. К вопросу о создании и развитии эмоционального искусственного интеллекта // Россия: тенденции и перспективы развития. 2021. №. 16-1. С. 674–676.

УДК 004.896:656.1

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВНЕДРЕНИЯ ИИ АВТОПИЛОТА ДЛЯ ЛЕГКОВЫХ АВТОМОБИЛЕЙ

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

Аннотация
Статья посвящена анализу проблем безопасности, возникающих при внедрении систем автопилота для легковых автомобилей, основанных на технологиях искусственного интеллекта и машинного обучения. В работе рассматриваются ключевые факторы риска, связанные как с техническими особенностями алгоритмов, так и с организационно-экономическими аспектами их разработки. Отмечается, что современные модели ИИ включают сотни потенциальных ошибок, возникающих из-за недостаточного тестирования, ограниченности обучающих выборок и сложности воспроизведения опасных дорожных сценариев. Ускоренная технологическая конкуренция между ведущими странами и корпорациями приводит к сокращению циклов проверки и преждевременному выводу систем на рынок, что повышает вероятность скрытых дефектов. Отдельное внимание уделено уязвимости систем восприятия, включая некорректную интерпретацию объектов, неточность определения расстояний и ошибочную классификацию дорожной информации. Показано, что даже небольшие отклонения в восприятии могут вызвать резкое нарушение устойчивости управления автомобилем, особенно в сложных условиях реального трафика. Также анализируются проблемы принятия решений, включая ошибочные прогнозы поведения участников движения и влияние скрытых предвзятостей обучающих данных. В заключение подчеркивается необходимость формирования строгой нормативной базы, внедрения независимого тестирования, создания расширенных датасетов, а также обязательной проверки систем в контролируемых условиях. Реализация этих мер рассматривается как ключевой элемент обеспечения безопасного и надежного внедрения автопилотируемых транспортных средств в гражданскую инфраструктуру.
Ключевые слова
Автопилот, искусственный интеллект, ошибки алгоритмов, безопасность.

Распространение искусственного интеллекта уже давно перестало быть явлением, ограниченным узкими техническими сообществами. Сегодня эта технология постепенно и последовательно проникает во все уровни социальной, экономической и технологической структуры, и её влияние становится ощутимым не только в специализированных областях, но и в повседневной жизни миллионов людей. ИИ меняет подходы к обработке информации, оптимизирует сервисы, перестраивает корпоративные процессы и активно внедряется в государственные системы, отвечающие за управление инфраструктурой, транспортом и безопасностью. Особенно заметными стали изменения в сфере автономного транспорта, где интеллектуальные модели берут на себя функции восприятия окружающей среды и принятия решений. Такие системы потенциально способны повысить удобство и эффективность дорожного движения, однако они же несут значительные риски. Ошибки в обучении, недостаток тестирования или некорректная работа сенсоров могут привести к сбоям, способным создать опасные ситуации на дороге. Подобная масштабность и глубина интеграции требуют гораздо более внимательного анализа, поскольку ИИ перестает быть вспомогательным элементом и превращается в самостоятельный механизм влияния, который способен формировать новые типы угроз и трансформировать уже существующие, затрагивая как частные интересы, так и общественную безопасность.

Как показывает исследование «ML based Fault Injection for Autonomous Vehicles: A Case for Bayesian Fault Injection» автопилот для автомобилей, который использует методы машинного обучения, может содержать сотни критических ошибок. Это по-настоящему тревожный вывод, потому что он касается систем, которые работают в динамичной и непредсказуемой среде, где даже одно неточное срабатывание может привести к цепочке ошибок. Когда такие модели проходят обучение на больших массивах данных, в них

неизбежно накапливаются скрытые дефекты, которые сложны для обнаружения традиционными методами тестирования. Ситуация становится особенно опасной в условиях стремительного развития автономных технологий. Глобальная технологическая гонка усиливает давление на разработчиков, и этот фактор также рассматривается как одна из причин риска. Американские, российские и китайские компании борются за доминирование в сфере ИИ, что приводит к ускоренным релизам, оптимизации под сроки и попыткам быстрее всех продемонстрировать рабочий продукт. Автопилоты, основанные на машинном обучении, становятся символом технологической мощи страны. В США центр внимания сосредоточен вокруг Tesla, в России основной разработчик – Yandex, а в Китае множество крупных автомобильных компаний одновременно ведут собственные проекты. Такая распределенная конкуренция создает атмосферу, в которой команды вынуждены искать кратчайшие пути к результату. Руководство требует ускорения процессов, уменьшения циклов проверки и вывода решений на рынок до завершения полного тестирования. Это приводит к допущению компромиссов, которые редко бывают безопасными [1].

Инженеры оказываются в эмоционально и профессионально сложной ситуации. Часто они понимают, что идеальной модели не существует, но всё равно должны искать баланс между качеством и скоростью разработки. В жёстких дедлайнах трудно создавать достаточно глубокие тестовые базы, особенно если речь идет о редких, но критически опасных сценариях дорожного движения. Моделирование таких ситуаций требует времени, вычислительных ресурсов и тщательно собранных датасетов. Практика разработки показывает, что многие ошибки остаются незамеченными именно, потому что команды вынуждены сокращать количество итераций тестирования. В обычных программных продуктах такие компромиссы допустимы и обычно приводят лишь к неудобствам для пользователей. Но в области автономного вождения ставки гораздо выше. Каждая ошибка может поставить под угрозу жизнь водителей, пассажиров и пешеходов. Дополнительная проблема заключается в том, что крупные компании имеют ресурсы для минимизации репутационных потерь. Они могут ограничивать распространение информации о незначительных столкновениях или сбоях, уменьшая масштаб общественного обсуждения. Большие корпорации умеют работать с медиа, формируя нужный информационный фон. Всё это снижает вероятность того, что общество будет знать о реальном числе аварий вызванных недостатками алгоритмов. Финансовая составляющая также играет роль. Разработка ИИ стоит дорого, особенно если требуется постоянное улучшение моделей. В попытке уменьшить издержки компании иногда урезают бюджеты на тестирование, аудит качества и анализ обучающих данных. Такие решения увеличивают вероятность появления незамеченных ошибок, которые затем проявляются уже на дорогах.

Во втором исследовании «Control Analysis and Design for Autonomous Vehicles Subject to Imperfect AI Based Perception» ученые подробно изучают как ошибки восприятия влияют на управление автомобилем. Они создают математические модели поведения автомобиля в ситуациях, когда система неверно интерпретирует объекты вокруг. Например, алгоритм может неправильно определить расстояние до препятствия, ошибиться в оценке траектории другого транспортного средства или некорректно классифицировать дорожные знаки. На первый взгляд такие неточности могут показаться небольшими. Однако в контексте системы управления автомобилем даже отклонение в несколько процентов может вызвать каскад эффектов. Исследование показывает, что ошибки в восприятии приводят к нарушению устойчивости системы контроля, особенно когда автомобиль движется в сложных условиях: плотный трафик, плохая погода, ночное время, неожиданные маневры других участников движения. Авторы подчеркивают, что создание устойчивых и безопасных систем требует тщательной калибровки алгоритмов, многократной проверки на синтетических и реальных данных и обязательной валидации в условиях реальной дороги. Такой процесс дорогостоящий, но без него дороги могут стать непредсказуемыми. Каждая ошибка будет иметь реальные последствия, которые в лучшем случае приведут к материальному ущербу, а в худшем к человеческим жертвам. Когда проблемы проявятся массово, исправлять

последствия будет поздно, поскольку у общества уже сформируется недоверие к технологии, а у государства – критическое давление со стороны граждан [2].

Во многих исследованиях отмечается, что искусственный интеллект становится ключевым элементом в управлении автономными транспортными системами, однако вместе с этим растет и спектр уязвимостей. В работе «AdvSim: Generating Safety Critical Scenarios for Self Driving Vehicles» представлен метод создания искусственных враждебных сценариев для автономных автомобилей, использующих LiDAR. Такие сценарии моделируют редкие, но чрезвычайно опасные ситуации, которые сложно собрать в реальных условиях. Исследователи показывают, что даже незначительные искажения в структуре входных сигналов могут приводить к некорректному распознаванию объектов или неверному прогнозированию траектории. Это демонстрирует, что системы восприятия ИИ уязвимы к сложным условиям и не всегда способны корректно реагировать на неожиданные события. Такая работа подчеркивает важность стресс тестирования и необходимости расширения методов валидации, особенно в контексте движения в городской среде, где возможны самые разнообразные сценарии. Доклад «Artificial Intelligence in Automated Driving: an analysis of potential causes of failures» от исследовательского центра Европейской комиссии рассматривает проблемы, связанные с ограничениями архитектур ИИ и недостаточно строгими требованиями к их внедрению. Авторы анализируют причины сбоев, включая неверную постановку задачи, корпус данных с ошибками, неустойчивость нейросетевых моделей в условиях сложной внешней среды и недостаточную адаптацию к динамически меняющимся дорожным ситуациям. В отчете подчеркивается, что отклонения в погоде, особенности дорожной разметки, наличие неформализованных объектов и поведенческое разнообразие водителей создают дополнительную нагрузку на систему. Нейросети могут демонстрировать высокую точность в контролируемых условиях, но в реальном мире они сталкиваются с шумными, неоднозначными и изменчивыми данными. Это приводит к тому, что сбои становятся не исключением, а вероятным следствием недостатков в обучении и тестировании [3, 4].

Кроме внешних факторов значительную угрозу создают особенности самой логики принятия решений. Даже если система корректно распознает объекты, ошибка может возникнуть на уровне выбора действия. Алгоритмы, отвечающие за прогнозирование поведения других участников движения, могут неправильно оценить скорость, траекторию или намерения человека, что приводит к неверному выбору маневра. В условиях плотного городского трафика любая задержка в обработке информации или некорректное принятие решения может стать критическим фактором. Кроме того, большинство современных моделей обучаются на данных, которые уже содержат скрытые перекосы. Эти перекосы затем проявляются в неожиданных ситуациях, когда система сталкивается с нетипичным сценарием. Наблюдается и более широкая проблема, связанная с тем, что развитие автономных систем идет быстрее, чем формирование нормативных стандартов и требований к их надежности. Отсутствие единых методологий проверки, недостаточная прозрачность тестирования, а также разнородность данных, используемых в обучении, создают условия для появления систем, которые работают хорошо только в ограниченном наборе ситуаций. Интеграция ИИ в автомобили требует постоянного обновления моделей, мониторинга их поведения и создания многоуровневых механизмов защиты от сбоев. Без этих мер массовое внедрение автономного транспорта может привести к росту аварийности и снижению доверия общества к технологиям, что в дальнейшем затормозит развитие отрасли.

Чтобы управление ситуацией стало более прозрачным и безопасным, государствам придется вмешаться в процесс разработки автономных систем. Даже минимальный набор базовых действий должен быть строго регламентирован.

1. Создание четкой правовой базы для внедрения автопилота в легковые автомобили. Законы должны определять требования к безопасной эксплуатации, зонам ответственности, стандартам тестирования и сертификации. Без этого отрасль будет развиваться хаотично.

2. Обязать компании формировать обширный и разнообразный банк данных для обучения моделей. Такой банк должен включать редкие, экстремальные и необычные дорожные ситуации. Это позволит моделям видеть больше возможных сценариев и корректнее реагировать на них в реальности.
3. Формирование независимой комиссии по тестированию автономных систем. Такая комиссия должна проводить полный аудит данных, проверять корректность алгоритмов, выявлять слабые места и проводить независимый стресс тест.
4. Организация закрытых испытаний в небольших локациях. Это позволит постепенно расширять круг тестируемых ситуаций, не подвергая риску общественные дороги. Такие полигоны должны моделировать самые сложные условия: резкие маневры, странное поведение пешеходов, разметку плохого качества, редкие погодные явления.

Только при выполнении этих шагов у правительств появится шанс обеспечить безопасное внедрение автомобилей с автопилотом. Если же требования будут проигнорированы, то логичным станет либо полный отказ от масштабной эксплуатации подобных систем, либо ограничение их применения строго контролируемыми сценариями. Такой подход позволяет уменьшить риски для общества и сохранить технологический прогресс, не подвергая людей неоправданным опасностям.

Литература

1. Jha S., Banerjee S.S., Tsai T., Hari S.K.S., Sullivan M.B., Kalbarczyk Z.T., Keckler S.W., Iyer R.K. ML-based Fault Injection for Autonomous Vehicles: A Case for Bayesian Fault Injection. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/1907.01051 (Дата обращения 20.11.2025).
2. Yan T., Zhang Z., Jiang J., Chen W.-H. Control Analysis and Design for Autonomous Vehicles Subject to Imperfect AI-Based Perception. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2509.12137 (Дата обращения 20.11.2025).
3. Wang J., Pun A., Tu J., Manivasagam S., Sadat A., Casas S., Ren M., Urtasun R. AdvSim: Generating Safety-Critical Scenarios for Self-Driving Vehicles. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2101.06549 (Дата обращения 20.11.2025).
4. Artificial Intelligence in Automated Driving: an analysis of potential causes of failures. [Электронный ресурс]. Режим доступа: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC127189/JRC127189_01.pdf (Дата обращения 20.11.2025).

УДК 004.8:371.3

ВЛИЯНИЕ ИИ НА ОБРАЗОВАНИЕ

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
Статья анализирует трансформацию системы образования под влиянием технологий искусственного интеллекта, фиксируя как преимущества, так и структурные риски. Массовое распространение нейросетей привело к изменению учебной мотивации, снижению роли самостоятельного анализа и росту зависимости учащихся от автоматически генерируемых решений. Рассматриваются механизмы, через которые ИИ подменяет интеллектуальные операции: воспроизведение фактов, шаблонное решение задач, автоматическая генерация текстов. Отмечается, что подобные процессы ослабляют исследовательские навыки, критическое мышление и глубину понимания материала, особенно среди подростков, для которых ИИ становится универсальным средством получения готового результата. В области творчества выявляется тенденция смещения от экспериментирования к использованию алгоритмически сформированных идей, что снижает индивидуальность и сложность творческого процесса. Параллельно анализируются академические и экспертные источники, фиксирующие необходимость пересмотра образовательных методик. Подчёркивается значимость открытых заданий, ориентированных на аргументацию, интерпретацию и создание авторских решений, которые не могут быть заменены генерацией текста. Образовательные учреждения должны формировать культуру критического взаимодействия с ИИ: проверка достоверности, выявление логических ошибок, работа с неоднозначными ситуациями. Интеграция ИИ рассматривается не как ограничение, а как возможность трансформации образовательного процесса. Сделан вывод, что будущее образования зависит от способности направлять использование ИИ на усиление человеческого потенциала, развитие аналитических, исследовательских и творческих навыков, в которых человек остаётся незаменимым.

Ключевые слова
Искусственный интеллект, образование, цифровая зависимость, творческие навыки, учебная мотивация, педагогические стратегии.

Искусственный интеллект постепенно превратился в одну из важнейших и наиболее обсуждаемых технологий середины двадцатых годов двадцать первого века. Его влияние настолько широко, что разговоры о нём ведутся повсюду: от непринуждённых бесед на кухне и дружеских обсуждений в социальных сетях до серьёзных дискуссий в правительственных кабинетах и научных центрах. Эта технология перестала быть чем-то узкоспециализированным – она стала частью повседневной жизни и одновременно стратегическим ресурсом для целых государств. Расширение применения нейросетей затронуло практически все сферы: от медицины и промышленности до искусства, коммуникаций и государственных услуг. Их влияние на общество оказалось не просто заметным, а преобразующим. Меняется структура рынка труда, способы взаимодействия людей, подходы к работе с информацией. Многие привычные задачи автоматизируются или радикально упрощаются, появляются новые профессии и новые способы решения уже знакомых проблем. Некоторые эксперты даже говорят о начале технологического перехода, сравнимого по масштабу с промышленной революцией.

Особенно серьёзные перемены наблюдаются в области образования. Оно оказалось одной из первых систем, где внедрение ИИ стало не только возможностью, но и необходимостью. В школах и университетах уже меняются методы преподавания, развивается персонализированное обучение, появляются адаптивные платформы, которые подстраиваются под темп и стиль ученика. Всё чаще поднимается вопрос о том, какие навыки станут ключевыми в ближайшие десятилетия и как учебные программы должны реагировать на стремительное развитие технологий. В этой статье будет рассмотрено, каким образом искусственный интеллект уже повлиял на образовательный процесс, какие

возможности и ограничения он создаёт и в каком направлении может развиваться система обучения, чтобы оставаться эффективной для школьников, студентов и всех, кто вовлечён в процесс получения знаний на протяжении жизни.

Рост доступности и мощности систем искусственного интеллекта создал серьёзные вызовы для современного образования, и эти вызовы затрагивают не только технические детали применения нейросетей, но и саму природу учебного процесса. В «Practical and Ethical Challenges of Large Language Models in Education» указывается, что такие модели способны автоматически генерировать ответы на широкий круг заданий и тем самым подменяют собой интеллектуальную работу учащихся. Студенты начинают использовать ИИ не как инструмент анализа или творческого поиска, а как средство получения готового результата, что постепенно снижает мотивацию к самостоятельному исследованию и уменьшает глубину усвоения материала. Такой риск оказывается особенно острым в ситуациях, когда задания строятся вокруг воспроизведения фактов или шаблонных формул, поскольку ИИ с лёгкостью справляется с подобными задачами и тем самым вытесняет необходимость развития критического или творческого мышления. Эта проблема рассматривается и на уровне государственных аналитических докладов, например в Министерстве науки и высшего образования в докладах о рисках ИИ в образовании, где подчёркивается, что чрезмерная зависимость обучающихся от ИИ постепенно приводит к снижению исследовательских навыков, ослаблению способности к самостоятельным рассуждениям и угасанию практических компетенций. В документе также отмечается, что без обновления учебных программ образование рискует превратиться в процесс поверхностного взаимодействия с автоматически сгенерированными текстами, а не систему формирования глубоких знаний, понимания и творческого подхода к задачам. Совокупность этих наблюдений показывает, что внедрение ИИ требует не сокращения сложности образования, а разработки новых педагогических методов, которые будут ориентированы на решение открытых проблем, творческий анализ информации и развитие навыков, в которых человек не заменяется алгоритмами, а использует их как расширение собственного мышления [1, 2].

Современные подростки всё активнее обращаются к системам искусственного интеллекта как к универсальному инструменту для выполнения практически любых учебных задач и повседневных творческих активностей. Для многих из них ИИ стал чем-то вроде постоянного цифрового помощника, к которому можно обратиться за текстом для школьного сочинения, за решением математической задачи, за готовым конспектом или даже за идеей для рисунка или сценария. Это использование воспринимается ими как естественная экономия времени и сил, ведь алгоритм способен сформировать необходимый материал за считанные секунды. Подростки часто не задумываются о том, как именно получен этот результат, и принимают его как нечто само собой разумеющееся, что постепенно снижает их готовность анализировать информацию самостоятельно или искать собственные пути решения. Такая модель поведения укрепляется удобством цифровой среды и постоянной доступностью технологий. Если раньше подростку приходилось экспериментировать, ошибаться, придумывать и проверять гипотезы, то теперь многие из этих этапов заменяются мгновенным ответом ИИ. В итоге формируется поверхностная привычка ориентироваться на готовые шаблоны, а не на собственное интеллектуальное усилие, что ведёт к постепенному снижению глубины мышления.

Этот повседневный стиль взаимодействия с ИИ негативно отражается и на развитии творческого мышления. Творчество подростков традиционно строится на пробах и ошибках, на личных впечатлениях, на поиске вдохновения через опыт и наблюдения. Однако, когда ИИ выступает в роли источника идей, образов и решений, он невольно подменяет собой их внутренний творческий процесс. Подросток, который мог бы экспериментировать со стилем письма или пробовать необычную композицию рисунка, всё чаще предпочитает нажать кнопку и получить мгновенный результат, а затем использовать его как окончательный вариант вместо черновика или отправной точки. Со временем такая практика формирует зависимость от внешнего генератора идей и ослабляет способность самостоятельно

учитывать нюансы, искать необычные подходы и развивать уникальный стиль. Более того, постоянное использование ИИ обедняет внутренний опыт подростков, ведь креативность требует не только готовых решений, но и эмоционального участия, наблюдательности, игры воображения. Когда всё это заменяется автоматизированной генерацией, подростки постепенно теряют навык чувствовать и формировать собственную мысль. В результате их творческий потенциал не развивается в полную силу, а становится зависимым от алгоритмов, которые предлагают удобные, но слишком усреднённые варианты.

Проблема использования ИИ в образовании становится особенно заметной, когда рассматривать результаты исследований, посвящённых поведению студентов и школьников в условиях свободного доступа к языковым моделям. В работе об использовании ИИ ассистентов в компьютерном образовании «Exploring the Role of AI Assistants in Computer Science Education» подчёркивается, что учащиеся нередко воспринимают такие инструменты как замену полноценному процессу обучения и вместо попыток разобраться в материале предпочитают автоматически генерируемые решения. Преподаватели отмечают, что эта тенденция приводит к тому, что студенты утрачивают способность разбираться в структуре задачи, перестают понимать, почему именно программа работает или не работает, а нередко просто копируют ответ, не задумываясь о его корректности и не проверяя логику. Исследование показывает, что подобное поведение вызывает цепную реакцию, которая снижает глубину освоения дисциплин и делает учащихся все более зависимыми от подсказок алгоритмов. При этом обсуждается необходимость изменения формата заданий так, чтобы ИИ не мог заменить собой учебный процесс. Авторы исследования подчёркивают важность использования открытых задач, требующих аргументации, анализа ошибок и нестандартных решений, которые невозможно получить простой генерацией текста. Это подтверждает, что современная система образования нуждается в адаптации, поскольку существующие методики устаревают под давлением технологий, которые слишком легко подменяют собой часть интеллектуальных усилий учащихся [3].

Подобные выводы перекликаются с анализом этических принципов использования ИИ в образовании, где делается акцент на необходимости формирования культуры критического взаимодействия между студентом и алгоритмом. В документе говорится, что запреты и ограничения не решают проблему, поскольку учащиеся всё равно находят способы использовать ИИ в обход требований. Вместо этого предлагается учить их проверять достоверность информации, формулировать аргументы, выявлять логические ошибки и вступать в содержательный диалог с моделью. Такой подход предполагает, что ИИ должен рассматриваться не как источник готового ответа, а как партнёр по рассуждению, инструмент проверки гипотез и средство развития аналитических навыков. Авторы подчёркивают, что без формирования этой культуры образование рискует попасть в ситуацию, где значительная часть студентов не способна критически оценивать данные, не умеет строить собственные интерпретации и теряет способность к самостоятельному созданию контента. Именно поэтому образовательные учреждения должны пересматривать учебные планы, внедрять задания с высоким уровнем неопределённости, требующие личной позиции и авторской аргументации, а также стимулировать более осознанное использование ИИ. Всё это показывает, что проблема не только в доступности технологий, а в том, что система обучения должна научиться направлять этот доступ в сторону развития, а не деградации мышления [4].

В совокупности проведённый анализ показывает, что влияние искусственного интеллекта на образование нельзя рассматривать однозначно положительно или исключительно как техническое усовершенствование учебного процесса. Эта технология одновременно создаёт значительные преимущества и формирует новые риски, которые затрагивают фундаментальные механизмы развития мышления. С одной стороны, ИИ способен расширить образовательные возможности, поддержать индивидуальную траекторию обучения, помочь справляться с большими объёмами информации и сделать знания доступнее. С другой стороны, его чрезмерное и некритичное использование уже приводит к заметным изменениям в поведении школьников и студентов. Уменьшается мотивация к самостоятельному исследованию, ослабевают навыки анализа, интерпретации и

аргументации, формируется зависимость от готовых решений, предлагаемых алгоритмами. Особенно уязвимыми оказываются навыки творчества, поскольку подростки нередко предпочитают быстрое автоматическое решение вместо постепенного, внутренне мотивированного процесса созидания. Это угрожает не только качеству образования, но и способности будущих поколений формировать новые идеи, создавать культурные и технологические инновации и принимать самостоятельные решения в условиях быстро меняющегося мира.

Все рассмотренные источники сходятся в одном важном выводе. Образование должно не бороться с ИИ и не пытаться полностью ограничить его применение, а учиться адаптироваться и выстраивать новые формы работы с технологией. Учебные программы должны смещаться в сторону развития тех способностей, которые не могут быть автоматически воспроизведены алгоритмами. К ним относятся критическое мышление, анализ сложных ситуаций, творческое решение проблем, исследовательские навыки и способность к самостоятельному созданию смысла. Необходимо формировать культуру взаимодействия с ИИ, в которой учащийся не потребляет готовые ответы, а использует технологию как инструмент проверки идей, расширения перспектив и углубления понимания. Такой подход позволит сохранить и укрепить интеллектуальную самостоятельность обучающихся и превратить ИИ не в угрозу, а в ресурс, поддерживающий развитие человека. В конечном итоге эффективность образования в эпоху ИИ будет зависеть не от объёма технологий, внедрённых в учебный процесс, а от того, насколько мудро и осознанно они будут интегрированы, и насколько активно образовательная система сможет направлять их в сторону усиления человеческого потенциала.

Литература

1. Yan L., Sha L., Zhao L., Li Y., Martinez-Maldonado R., Chen G., Li X., Jin Y., Gašević D. Practical and Ethical Challenges of Large Language Models in Education: A Systematic Scoping Review. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2303.13379 (Дата обращения 17.11.2025).
2. Министерство науки и высшего образования, доклад о рисках ИИ в образовании. [Электронный ресурс]. Режим доступа: https://si.sseu.ru/sites/default/files/2025/04/rosnauka_ch1_2023_osen.pdf (Дата обращения 17.11.2025).
3. Wang T., Vargas- D. Díaz, Brown C., Chen Y. Exploring the Role of AI Assistants in Computer Science Education: Methods, Implications, and Instructor Perspectives. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2306.03289 (Дата обращения 17.11.2025).
4. Этика использования ИИ: как предотвратить списывание и плагиат и развить критическое мышление у студентов. [Электронный ресурс]. Режим доступа: https://www.fa.ru/university/structure/university/uso/press-service/press-releases/etika-ispolzovaniya-ii-kak-predotvratit-spisyvanie-i-plagiat-i-razvit-kriticheskoe-myshlenie-u-stude (Дата обращения 17.11.2025).

УДК 004.056.5:004.89

ЭВОЛЮЦИЯ ФИШИНГА В ЭПОХУ ГЕНЕРАТИВНЫХ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

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 рассматривается влияние больших языковых моделей (LLM) на глубокую трансформацию фишинговых атак как одного из распространённых и динамично развивающихся видов киберугроз. Особое внимание уделяется тому, каким образом распространение генеративного искусственного интеллекта меняет структуру, качество, масштабируемость и адаптивность современных фишинговых кампаний. На основе анализа четырёх современных исследований выявляются ключевые механизмы, посредством которых LLM усиливают возможности злоумышленников: снижение компетентностного барьера для подготовки контента, автоматизация процессов OSINT-разведки, адаптация фишинговых коммуникаций под индивидуальные особенности жертвы, а также формирование динамической архитектуры атак, в которой вредоносная логика переносится в область взаимодействия с языковой моделью. Особое значение уделено концепции «prompts as code», описанной в исследовании «Prompts as Code & Embedded Keys», согласно которой вредоносная функциональность может формироваться непосредственно в момент выполнения через генерацию кода моделью, что значительно осложняет применение классических сигнатурных или статических методов анализа. Материалы «OpWnAI: Cybercriminals Starting to Use ChatGPT.» демонстрируют реальные примеры использования ChatGPT на криминальных форумах для создания вредоносных скриптов и убедительных фишинговых писем пользователями без специальных технических навыков. Исследование «The Effects of Generative AI on High-Skilled Work» подтверждает эффект компенсации недостатка компетенций, что критично для понимания распространения высококачественного фишинга среди широкого круга злоумышленников. Работа «Introducing RedFlag» раскрывает механизм автоматизации разведывательной подготовки атак и индивидуализации контента. Сделанные выводы подчеркивают, что генеративные модели расширяют возможности социальной инженерии и меняют саму природу фишинга, превращая его в интеллектуально поддерживаемый динамический процесс. Показана необходимость разработки новых методов обнаружения и противодействия, учитывающих адаптивный, контекстно-генерируемый характер современных атак.

Ключевые слова
Фишинг, большие языковые модели, prompts as code, киберугрозы, кибербезопасность.

Стремительное распространение генеративных больших языковых моделей (LLM) стало одним из ключевых технологических событий последних лет, повлекшим за собой существенные изменения в сфере информационной безопасности. Способность LLM понимать и порождать человеческий язык, анализировать большие массивы данных, воспроизводить различное дискурсивное поведение и поддерживать сложные многоходовые сценарии коммуникации создала условия для появления новых форм злоупотреблений. На фоне их внедрения в бизнесовые, образовательные и научно-аналитические процессы всё более отчётливо проявляется и обратная сторона – активная адаптация этих моделей в преступной среде. Особенно остро влияние LLM проявляется в области фишинга, который остаётся одним из наиболее распространённых, экономически эффективных и социально гибких инструментов кибератак.

Исторически фишинг развивался как относительно простая техника социальной инженерии, основанная на подделке электронных писем и создании ложных сайтов. Со временем атаки усложнились, были добавлены механизмы автоматизации рассылок, анализа благоприятного времени отправки, адаптивного оформления сообщений, а затем и крупные инфраструктуры ботнетов. Однако до недавнего времени фишинг сохранял определённые ограничения, связанные с человеческим фактором. Злоумышленникам требовалось либо владеть языком и его стилистическими особенностями, либо иметь доступ к заранее подготовленным шаблонам, либо обладать достаточными навыками программирования для

генерации вредоносных вложений. Несмотря на попытки автоматизации, качество атак зависело от квалификации исполнителя, то есть повторяемость, стилистические аномалии и низкая гибкость были характерными признаками фишинга.

С появлением генеративных моделей ситуация резко изменилась. Первые фактические данные, представленные в исследовании «OpWnAI: Cybercriminals Starting to Use ChatGPT.», показали, что уже в первые месяцы после открытия доступа к ChatGPT злоумышленники начали активно обсуждать его возможности: генерацию фишинговых писем, написание вредоносных скриптов, создание простейших программ для кражи данных. Это был не единичный случай – подобные обсуждения нашли отражение на криминальных форумах, и даже пользователи без навыков программирования смогли создавать работоспособные вредоносные компоненты. Данные свидетельствуют о том, что генеративная модель стала выполнять функции эксперта по социальной инженерии, редактора, программиста и консультанта одновременно. Дополнительный важный слой анализа внесло исследование «Prompts as Code & Embedded Keys», показавшее, что LLM перестали быть лишь инструментом подготовки текста. Они начали использоваться как исполнительный компонент атаки, формирующий вредоносную логику в динамическом режиме. Исследователи представили концепцию «prompts as code», согласно которой запрос может выступать в роли инструкции, заставляющей модель генерировать фрагменты исполняемого вредоносного поведения. Это открывает путь к атакам, которые невозможно проанализировать классическими методами, поскольку не существует статической полезной нагрузки – она формируется в процессе выполнения атаки. Дополняет картину исследование «Introducing RedFlag», демонстрирующее, как генеративные модели могут ускорять и упрощать работу специалистов в наступательной безопасности (offensive security), то есть анализ документации, построение сценариев, автоматизация OSINT, систематизация разведывательной информации. Несмотря на то, что эти методы разработаны для легитимной деятельности, преступные акторы используют те же подходы, воспроизводя на практике схожие модели поведения. Исследование «The Effects of Generative AI on High-Skilled Work» добавляет важный теоретический компонент. Оно показывает, что LLM способны значительно сокращать разрыв между низкоквалифицированными и высококвалифицированными исполнителями, предоставляя менее опытным пользователям инструменты, ранее доступные только экспертам. В контексте фишинга это означает, что компетентностные барьеры практически исчезают. Преступник, едва знакомый с социальной инженерией, может формировать сообщения экспертного уровня, а пользователь, никогда не писавший вредоносного кода, способен генерировать рабочие скрипты [1–4].

Таким образом, необходимость исследования роли LLM в эволюции фишинга обусловлена сочетанием технологических, поведенческих и архитектурных факторов. Фишинг переходит на новый уровень сложности, адаптивности, правдоподобия и скрытности. Он превращается в гибридную систему, где взаимодействуют человек и искусственный интеллект. Цель работы – проанализировать эти изменения, обобщить данные существующих исследований и предложить научно обоснованную модель эволюции фишинга в эпоху генеративных моделей.

Историческая эволюция фишинга показывает, что этот тип атак всегда следовал за изменениями в цифровой коммуникации. На ранних этапах фишинговые сообщения были простыми подделками, часто содержащими грубые ошибки, нелогичные просьбы и примитивные шаблоны. Лингвистическая аномальность была одной из важных характеристик, позволявших различать такие письма. С внедрением автоматизированных спам-систем и наборов шаблонов качество частично выросло, а объём атак увеличился. Но даже при этом массовые кампании оставались шаблонными: злоумышленники делали ставку на количество, а не на индивидуализацию. Психологическое воздействие сообщений было ограниченным, а человеческий фактор злоумышленников – заметным.

Переход к использованию LLM радикально изменил данную парадигму. Стало возможно создавать фишинговые письма, неотличимые от реальной корпоративной переписки. Именно к такому выводу приходят исследователи в анализе «OpWnAI:

Cybercriminals Starting to Use ChatGPT.», где представлены примеры писем, автоматически корректируемых ChatGPT. Даже те злоумышленники, которые ранее писали с ошибками, могли получать гладкие, стилистически точные сообщения. Лингвистический анализ в этих условиях теряет значимость, поскольку исчезает главная диагностическая черта фишинга – низкое качество текста. С переходом к индивидуализированному фишингу LLM оказались особенно полезными. Они позволяют адаптировать сообщения под конкретного сотрудника или организацию. Модель способна учитывать стиль обращения, рабочую терминологию и структуру внутренних писем. Более того, она может формировать динамические сценарии общения, то есть подбирать ответы на неожиданные вопросы жертвы, менять тональность письма в зависимости от хода диалога и воспроизводить эмоциональную окраску сообщений, характерную для корпоративной среды. Это превращает фишинг в интерактивную коммуникацию, максимально приближенную к реальному рабочему процессу [1].

Следующий этап эволюции связан с генерацией вредоносных вложений и инструментов. Ранее злоумышленникам требовалось создавать макросы вручную или использовать готовые наборы. Теперь генеративные модели позволяют автоматически формировать код, оптимизированный под задачу: от простых скриптов до сложных макросов, скрытых за мнимыми функциями. Исследование «OpWnAI: Cybercriminals Starting to Use ChatGPT.» приводит примеры, когда модель создаёт код для шифрования, кражи данных или автоматического выполнения вредоносных действий. Такие примеры показывают, что LLM могут быть использованы как средство для генерации технических компонентов атаки без необходимости глубоких знаний со стороны злоумышленника. Понимание глубины изменений требует анализа концепции «prompts as code», предложенной в исследовании «Prompts as Code & Embedded Keys». Традиционно вредоносная программа содержала исполняемый код или зашифрованную полезную нагрузку, которую можно анализировать статически или динамически. Однако с появлением LLM появилась возможность переносить исполнение вредоносной логики в пространство взаимодействия между программой и моделью. В такой архитектуре вредоносное ПО может содержать лишь минимальную функциональность, то есть сбор контекста, формирование запроса и обработку ответа. Основная логика при этом генерируется «по требованию» (on-demand app generation). Такой сдвиг несёт несколько важных последствий. Во-первых, исчезает возможность классифицировать вредоносные программы на основе сигнатур. Поскольку полезная нагрузка генерируется динамически, каждый экземпляр атаки уникален. Во-вторых, модели становятся скрытым участником атаки, фактически выполняя роль соавтора вредоносного поведения. В-третьих, взаимодействие между моделью и клиентом превращается в часть атакующего процесса, который невозможно детектировать, анализируя только локальный файл. Рассмотрение этой архитектуры в контексте фишинга позволяет выявить новый тип атак. Вложение может содержать код, который обращается к языковой модели за инструкциями. Такие инструкции могут касаться обхода антивирусных программ, декодирования данных или определения действий в зависимости от конкретной среды выполнения. В такой ситуации традиционные системы безопасности сталкиваются с неуловимым противником: вредоносные действия происходят там, где они не могут провести анализ, то есть в модели [1, 2].

Особое внимание следует уделить автоматизации OSINT, представленной в исследовании «Introducing RedFlag». В наступательной безопасности ИИ применяется для анализа документации, выявления зависимостей, генерации отчётов и подготовки сценариев атак. В контексте фишинга аналогичные методы позволяют злоумышленникам автоматически анализировать открытые данные о компаниях: структуру отделов, характер внутренних коммуникаций, технологические процессы. Генеративные модели помогают им выстраивать логические цепочки: определить, от чьего имени лучше отправить письмо, какие документы могут быть затребованы, в какое время сотрудники чаще отвечают на сообщения. Это способствует формированию сложных, индивидуализированных фишинговых цепочек, ориентированных не на массовый эффект, а на конкретных сотрудников. Модель может также анализировать социальные сети, базы данных утечек, публичные профили сотрудников,

корпоративные дорожные карты и отчёты. На основе этих данных она формирует высокоточный социальный профиль жертвы, если злоумышленник запросит соответствующие сведения. Подобные операции ранее требовали сочетания опыта, времени и аналитического мышления. Теперь они превращаются в автоматизированный, мгновенно воспроизводимый процесс, доступный пользователям с минимальной подготовкой [3].

Эволюция фишинга проявляется и в трансформации взаимодействия злоумышленников с инструментами. Ранее фишинговые наборы представляли собой статические комплекты шаблонов сайтов, скриптов и инструкций. LLM позволяют создавать динамические наборы, генерируя HTML-код, графические элементы, имитации интерфейсов и фрагменты JavaScript, которые аккуратно скрывают вредоносное поведение. Более того, модель может предложить способы обхода фильтров почтовых сервисов, рекомендации по изменению контента, даже автоматизировать процесс обновления страниц захвата, делая их уникальными для каждого запроса. Параллельно изменяется и роль преступных сообществ. Если ранее преступникам приходилось обмениваться шаблонами и кодом, что требовало определённой технической грамотности, то сейчас им достаточно обмениваться примерами запросов. Запрос к модели становится новым видом «инструмента». Это может быть инструкция для генерации письма, макроса, сайта, вредоносного скрипта. Фактически запрос превращается в интеллектуальный артефакт, а генеративная модель – в универсальный компилятор, что создаёт условия для масштабирования преступной деятельности, поскольку барьеры для входа значительно ниже, чем раньше. Выравнивание компетенций, описанное в исследовании «The Effects of Generative AI on High-Skilled Work», является ключевым фактором. Фишинг становится доступным практически любому, кто способен формулировать запросы. Новички создают письма уровня профессионалов, а непрофессионалы в программировании генерируют вредоносный код. Ранее различия в опыте делали фишинг различимым, теперь же специалист и новичок используют один и тот же механизм, что приводит к взрывному росту доступности фишинга как инструмента [4].

Эволюция также касается структуры атакующих кампаний. Фишинг становится не только текстовым и техническим, но и поведенческим. LLM позволяют моделировать реакции жертвы и предсказывать развитие коммуникации. Например, модель может рекомендовать отправить дополнительное письмо после определённого временного промежутка, предложить аргументы для убеждения или сымитировать стиль конкретного руководителя. В условиях удалённой работы и цифровой коммуникации такие детали имеют критическое значение. Социальная инженерия превращается в модельно-управляемый процесс, где злоумышленник играет роль оператора, а LLM – роль аналитика и генератора контента.

Появляются и новые гибридные атаки, сочетающие фишинг с динамическими компонентами. Например, вложение может содержать лишь ссылку, которая активирует взаимодействие с моделью, генерирующей индивидуальный вредоносный код под конкретную операционную систему, браузер или параметры машины, что делает атаки практически неуловимыми до момента реального выполнения. В совокупности эти факторы формируют новую экосистему фишинга – гибкую, адаптивную, интеллектуальную, обладающую высокой степенью автоматизации. Она объединяет традиционные методы социальной инженерии, современные генеративные модели, динамические архитектуры вредоносного поведения и комплексные OSINT-процессы. Угроза становится системной, а не точечной. Это требует глубокого анализа и переосмысления старых подходов.

Рассмотренные исследования свидетельствуют, что генеративные большие языковые модели оказывают фундаментальное влияние на эволюцию фишинга. Они меняют структуру, содержание, динамику и масштаб кибератак. Лингвистическая составляющая атак стала практически неотличимой от корпоративной переписки. Снижение компетентностных барьеров приводит к тому, что даже неопытные злоумышленники способны создавать высококачественные фишинговые сообщения и вредоносные вложения. Применение LLM в качестве динамического генератора логики создает новые архитектурные вызовы для средств безопасности. Автоматизация OSINT и подготовительных процессов увеличивает индивидуализацию атак и повышает их вероятность успеха. Совокупность этих изменений

указывает, что традиционные методы анализа фишинга теряют эффективность. Сигнатурные методы устаревают, лингвистические признаки едва различимы, а статический анализ вредоносного кода сталкивается с отсутствием кода как такового. В таких условиях требуется построение новых моделей защиты, ориентированных на поведенческий анализ, изучение взаимодействия программных объектов с языковыми моделями и разработку методов обнаружения динамически генерируемых угроз.

Дальнейшее исследование должно включать анализ взаимодействия человека и модели в процессе атаки, изучение механизмов генерации вредоносной логики, разработку средств перехвата запросов к LLM и формирование многоуровневых архитектур защиты. Особое значение приобретает мониторинг изменения ландшафта угроз и моделирование потенциальных сценариев, в которых генеративные модели станут ключевым компонентом атакующих инфраструктур.

Фишинг в эпоху LLM перестал быть статической техникой социальной инженерии. Он стал динамической, интеллектуальной системой, использующей генеративный интеллект для адаптации, маскировки и масштабирования вредоносной деятельности. Его изучение становится одной из центральных задач современной кибербезопасности, требующей комплексного научного подхода, сочетания лингвистики, анализа поведения, архитектурных исследований и изучения взаимодействия человека и ИИ.

Литература

1. Check Point Research. OpWnAI: Cybercriminals Starting to Use ChatGPT. [Электронный ресурс]. Режим доступа: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/ (Дата обращения 16.11.2025).
2. Delamotte A., Kamluk V., Bernadett-Shapiro G. Prompts as Code & Embedded Keys: The Hunt for LLM-Enabled Malware. [Электронный ресурс]. Режим доступа: https://www.sentinelone.com/labs/prompts-as-code-embedded-keys-the-hunt-for-llm-enabled-malware/ (Дата обращения 16.11.2025).
3. Greenwood T., Honeycutt B. 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 16.11.2025).
4. Cui K.Z., Demirer M., Jaffe S., Musolff L., Peng S., Salz T. The Effects of Generative AI on High-Skilled Work: Evidence from Three Field Experiments with Software Developers. [Электронный ресурс]. Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4945566 (Дата обращения 16.11.2025).

УДК 577.3

КУЛЬТИВИРОВАНИЕ HALOBACTERIUM SALINARUM И ВЫДЕЛЕНИЕ БАКТЕРИОРОДОПСИНА

Шилин-Шнейдер И.С.[1] (студент)
Научный руководитель – начальник научно-исследовательского отдела Шмелин П.С.[2]
[1]РТУ МИРЭА
[2]АО «ЦНИТИ «Техномаш»
krol.zanyda@gmail.com

Аннотация
Бактериородопсин (БР) — светочувствительный белок галобактерий Halobacterium salinarum, обладающий уникальными фотохромными свойствами, что делает его перспективным для применения в оптоэлектронике, биосенсорах и медицине. Актуальность исследования обусловлена необходимостью разработки эффективных методов получения высокоочищенного БР для его дальнейшего использования в биотехнологии. В работе предложена оптимизированная методика культивирования H. salinarum и выделения БР. Биомассу выращивали на синтетической среде при 37°C с аэрацией и освещением. Очистку белка проводили центрифугированием (18 000 об/мин) и ферментативным лизисом (ДНКаза/РНКаза). Чистоту подтвердили спектрофотометрией. Выход белка составил 9,77 г. Метод эффективен для получения высокоочищенного бактериородопсина со степенью очистки A_{560}/A_{280} = 2,268 при стандарте очистки 1,7–2,4.

Ключевые слова
Бактериородопсин, Halobacterium salinarum, культивирование, очистка, пурпурные мембраны, фотохромный белок, археи.

Бактериородопсин (БР) — светозависимый мембранный белок архей Halobacterium salinarum, применяемый в биосенсорах, оптоэлектронике и медицине [1, 2]. Его уникальные фотохромные свойства (квантовая эффективность >64%, стабильность в широком диапазоне pH и температур) делают его перспективным материалом для создания устройств обработки и хранения оптической информации [3]. Однако промышленное использование БР ограничено сложностью его выделения и очистки. Цель работы — разработка эффективного метода культивирования H. salinarum, очистки БР и расширить возможности его практического применения.

Применение БР перспективно, так как широко используется в различных областях. В оптоэлектронике он применяется для создания голографической памяти на основе фотоцикла БР с переходами между состояниями O, P, Q [4]. В медицине кремы с бактериородопсином демонстрируют 86,6% эффективности при лечении псориаза [5]. В биосенсорах БР используется в гибридных фоторецепторах с флавинами [2].

В работе использовались следующие материалы и методы. Культивирование биомассы проводили с использованием штамма Halobacterium salinarum ET 1001 на синтетической среде со следующим составом (г/л): NaCl (120), пептон (4,8), дрожжевой экстракт (1,6), глицерин (3,2), $MgSO_4 \cdot 7H_2O$ (12), pH 7,8–8,1. Условия культивирования: температура 37°C, аэрация воздухим, освещение 2000 лк, шейкер-инкубатор (120 об/мин). Оптическую плотность (OD_{560}) поддерживали на уровне 1,5–2,0 добавлением свежей среды.

Выделение бактериородопсина включало несколько этапов. Сепарацию клеток проводили центрифугированием при 10 000 об/мин в течение 30 минут. Лизис клеток осуществляли обработкой смесью ДНКазы и РНКазы в концентрации 1,8 ед/мл в дистиллированной воде. Очистку БР проводили многоступенчатым центрифугированием при 18 000 об/мин и температуре 4°C до обесцвечивания супернатанта. Степень очистки определяли на спектрофотометре СФ-56 по расчету соотношений оптической плотности A_{560}/A_{280} [6].

В результате проведённых исследований были получены следующие результаты. Биомасса наращивалась в кюветном инкубаторе до 10,3 г/л (сухой вес). Оптимальная скорость центрифугирования составила 10 000 об/мин с выходом клеток 9,77 г/л (таблица).

Таблица

Влияние скорости центрифугирования на выход биомассы

Частота, об/мин	Выход биомассы, г/л
8000	7,91
10000	9,77
12000	9,79

Чистоту бактериородопсина оценивали по соотношению значений оптической плотности при максимумах поглощений спектра при длине волны 280 нм у белков-примесей и длине волны 560 нм у хромофора ретиналя (рисунок). Соотношение A_{560}/A_{280} = 2,268 соответствует стандартам очистки (диапазон: 1,7–2,4) [6].

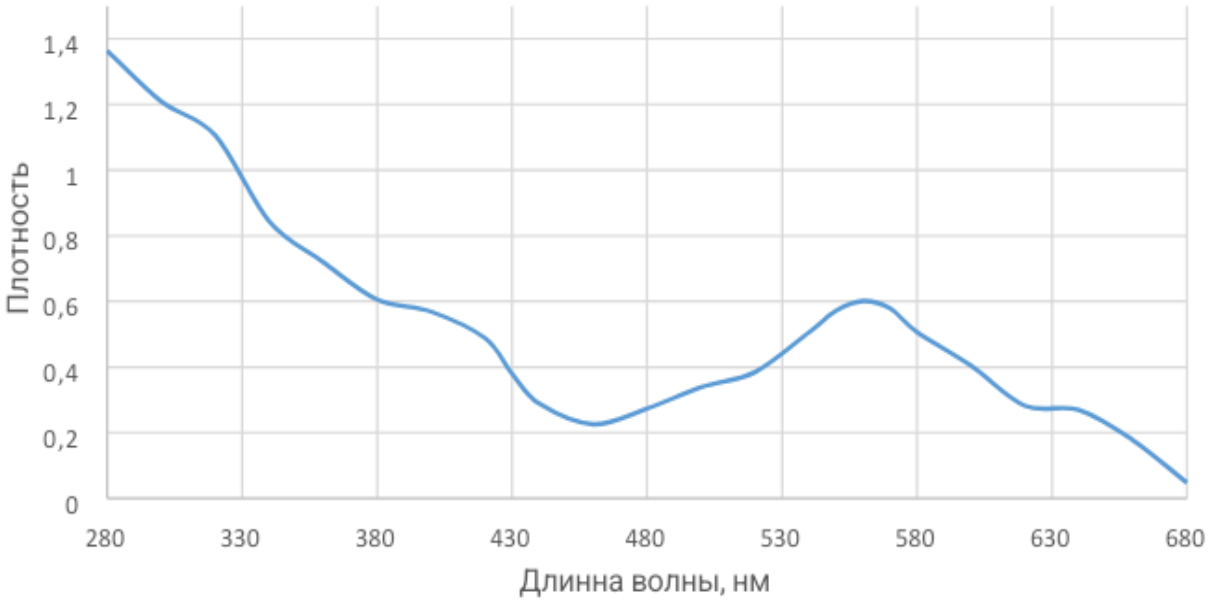


Рисунок. Спектр поглощения очищенного бактериородопсина

Таким образом, обработка БР раствором смеси ДНКазы и РНКазы концентрацией 1,8 ед/мл в дистиллированной воде и оптимальной скорости центрифугирования до 10 000 об/мин позволяет увеличить чистоту БР на 20% по сравнению с ранее применяемой методикой.

В результате работы оптимизирован метод культивирования H. salinarum, позволяющий получить биомассу в количестве 10,3 г/л и разработана схема очистки БР (центрифугирование + ферментативный лизис) с чистотой A_{560}/A_{280} = 2,268.

Литература

1. Гребенников Е.П. Бактериородопсин — биологический преобразователь световой энергии с уникальными технологическими возможностями // Российский химический журнал. 2006. Т. 50. №. 5. С. 25–36.
2. Дружко А.Б. Бактериородопсин: фундаментальные аспекты и возможности для практического применения / А.Б. Дружко ; Российская академия наук. — Москва : Рос. акад. наук, 2022. 92 с.
3. Birge R.R., Gillespie N.B., Izaguirre E.W. et al. Biomolecular Electronics: Protein-Based Associative Processors and Volumetric Memories // The Journal of Physical Chemistry B. 1999. Vol. 103. №. 49. Pp. 10746–10766.
4. Khizroev S., Ikkawi R., Amos N. et al. Protein-Based Disk Recording at Areal Densities Beyond 10 Terabits/in.2 // MRS Bulletin. 2008. Vol. 33. № 9. Pp. 864–871.
5. Олисова О.Ю., Максимов И.С., Алленова А. С. Эффективность применения крема с бактериородопсином у больных псориазом // Российский медицинский журнал. 2019. № 4. С. 54–58.

6. Мосин О.В., Игнатов И.И. Природный фотопреобразующий фотохромный мембранный белок бактериородопсин из пурпурных мембран галобактерии Halobacterium halobium // Nanotechnology Research and Practice. 2014. Т. 1. №. 1. С. 43–56.
7. Karagözoglu N., Håkanson L., Sharp D. et al. The role of absorptive capacity in innovation: A systematic review // International Journal of Innovation Studies. 2023. Vol. 7. №. 1. Pp. 1–21.

УДК 004.8:378.147

ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И КОГНИТИВНЫХ НАУК ДЛЯ РАЗРАБОТКИ АДАПТИВНЫХ СИСТЕМ ОНЛАЙН-ОБУЧЕНИЯ

Аркабаев Н.К.[1]
[1]Ошский государственный университет, г. Ош, Кыргызстан
nurkasym@gmail.com

Аннотация
В данной статье рассматривается разработка архитектуры для систем онлайн-обучения, которые объединяют искусственный интеллект и когнитивные науки. Мы провели анализ существующих ИИ-технологий в образовании и изучили когнитивные теории обучения. Система состоит из нескольких модулей: один оценивает когнитивные особенности студента, другой отслеживает его знания в реальном времени, третий анализирует эмоциональное состояние, четвёртый подстраивает контент под каждого ученика. Эксперименты показали, что наш подход улучшает результаты обучения по сравнению с обычными онлайн-платформами. Разработанная система учитывает индивидуальные когнитивные особенности каждого студента и адаптируется к его потребностям.

Ключевые слова
Адаптивное обучение, когнитивное моделирование, персонализация образования, машинное обучение в образовании, интеллектуальные обучающие системы.

Введение

Цифровые технологии и новые данные о когнитивных процессах человека меняют современное образование. Интеграция искусственного интеллекта с когнитивными науками позволяет создавать системы онлайн-обучения, которые учитывают индивидуальные особенности познавательной деятельности каждого студента.

Современные исследования в области когнитивной психологии убедительно показывают, что процессы восприятия, обработки информации, формирования памяти и принятия решений характеризуются высокой индивидуальной вариативностью [1]. Одновременно с этим развитие технологий машинного обучения и анализа больших данных предоставляет инструменты для создания образовательных систем, способных адаптироваться к этим индивидуальным различиям в режиме реального времени.

Несмотря на значительные достижения в области искусственного интеллекта в образовании, существует ряд нерешенных проблем, которые ограничивают эффективность современных адаптивных систем. Основные вызовы включают в себя недостаточную глубину когнитивного моделирования обучающихся, что приводит к поверхностной персонализации, ограниченной простой адаптацией сложности контента. Кроме того, большинство существующих систем не учитывают динамические изменения когнитивного состояния пользователя в процессе обучения, а также не интегрируют достижения нейронауки в области понимания механизмов обучения и памяти.

Анализ современных исследований в области ИИ-образования показал растущий интерес к данной проблеме. Мета-анализ в работе Чжисюань Чу и другие продемонстрировал, что адаптивные системы обучения с поддержкой искусственного интеллекта показывают средний и большой положительный эффект на когнитивные результаты обучения студентов по сравнению с неадаптивными интервенциями ($g = 0.70$). При этом эффективность значительно модерировалась типом публикации, происхождением исследования, уровнем образования студентов, предметной областью, продолжительностью обучения и дизайном исследования [2].

Работа по интеграции искусственного интеллекта в электронное обучение через призму когнитивной нейропсихологии выявила, что ИИ-инструменты используют когнитивные принципы при улучшении обучения путем адаптации контента на основе когнитивных состояний, таких как внимание и когнитивная нагрузка [1]. Персонализированные системы обучения автоматически адаптируются к индивидуальному когнитивному профилю каждого обучающегося, выбирая подходящие учебные материалы на основе когнитивных сильных сторон и способностей каждого учащегося.

В российском контексте проблематика адаптивного обучения также получает активное развитие. Как отмечается в исследованиях МГУ, важнейшим вызовом науке XXI века является раскрытие природы когнитивных систем и понимание того, что принципиально отличает такие системы от всех остальных. Министерство науки и высшего образования России сформулировало базовые требования к применению искусственного интеллекта в образовательном процессе, направленные на развитие когнитивных способностей учащихся без формирования зависимости от технологий [3].

Систематический обзор адаптивных образовательных платформ подчеркивает, что современные системы собирают и анализируют данные обучающихся для динамической адаптации учебного контента и траекторий, предлагая персонализированный опыт обучения и улучшая результаты. При этом особое внимание уделяется педагогическим основам, ИИ-реализациям и вызовам реальных приложений [4].

Наши предыдущие исследования [5] исследовались возможности применения искусственного интеллекта для измерения успеваемости учащихся, включая автоматизированную оценку, анализ образовательных данных и персонализированную обратную связь, что выявило потенциал передовых ИИ-систем в области персонализации обучения. Выводы о необходимости системного подхода к трансформации образования и важности этических аспектов внедрения ИИ создают основу для данного исследования, которое развивает техническую сторону проблемы через разработку когнитивно-ориентированных адаптивных систем обучения. В последующей работе [6] мы показали влияние искусственного интеллекта на трансформацию роли преподавателя в образовательной системе Кыргызской Республики, выявив ключевые изменения в педагогических компетенциях в условиях цифровизации образования. Было установлено, что успешная интеграция ИИ-технологий требует развития у преподавателей цифровой грамотности, навыков анализа данных и эмоционального интеллекта.

Настоящее исследование направлено на разработку теоретических основ и практических подходов к интеграции искусственного интеллекта и когнитивных наук для создания нового поколения адаптивных систем онлайн-обучения. Задачи включают в себя анализ современных технологий ИИ в образовании и их совместимости с принципами когнитивных наук, разработку архитектуры интегрированной адаптивной системы, основанной на когнитивном моделировании, а также исследование методов реального времени для оценки и адаптации к когнитивному состоянию обучающегося.

Материалы и методы

Методология исследования включала систематический анализ литературы, когнитивное моделирование и экспериментальную проверку предлагаемых решений. Исследование проводилось в четыре основных этапа, каждый из которых имел специфические задачи и применял соответствующие методы анализа:

1. Систематический анализ современных технологий ИИ в образовании.

Первый этап исследования включал проведение систематического обзора литературы по применению технологий искусственного интеллекта в образовательных системах. Поиск релевантных источников осуществлялся в базах данных Scopus, IEEE Xplore и российских научных базах данных eLIBRARY.RU. Временные рамки анализа охватывали период с 2021 по 2024 год для обеспечения актуальности исследуемых технологий.

В анализ включались публикации, если они: описывали применение ИИ в образовании, содержали экспериментальные данные или подробное описание архитектуры систем, были опубликованы в рецензируемых журналах или сборниках ведущих конференций. Исключались работы, посвященные исключительно административному применению ИИ в образовании без связи с процессами обучения, а также обзорные статьи без оригинального вклада.

В ходе анализа особое внимание уделялось технологиям машинного обучения, включая нейронные сети различных архитектур, алгоритмы глубокого обучения для обработки образовательных данных, системы рекомендаций и персонализации контента, а также методы обработки естественного языка для анализа текстовых работ обучающихся. Для каждой

категории технологий проводился анализ их преимуществ, ограничений и потенциала интеграции с когнитивными принципами.

2. Исследование принципов когнитивного моделирования.

Второй этап был посвящен глубокому анализу современных достижений когнитивных наук, релевантных для разработки адаптивных образовательных систем. Основное внимание уделялось теориям когнитивной архитектуры человека, включая модели рабочей памяти, внимания и исполнительного контроля. Изучались принципы когнитивной нагрузки и их применение в дизайне образовательных интерфейсов.

Особый интерес представляли исследования в области нейронауки обучения, включая механизмы формирования долговременной памяти, процессы консолидации знаний и нейропластичность. Анализировались работы по теории двойного кодирования, мультимодальному обучению и роли эмоций в процессах запоминания и мотивации к обучению.

Методология исследования включала критический анализ классических и современных теорий обучения, от бихевиористских подходов до конструктивистских и коннективистских моделей.

3. Разработка архитектуры интегрированной системы.

На третьем этапе осуществлялось проектирование архитектуры адаптивной системы онлайн-обучения, интегрирующей технологии ИИ с принципами когнитивных наук. Методология проектирования основывалась на принципах человеко-ориентированного дизайна и включала итеративный процесс создания и уточнения архитектурных решений.

Ключевые компоненты разрабатываемой системы включали модуль когнитивного профилирования обучающихся, использующий методы машинного обучения для анализа паттернов взаимодействия с образовательным контентом. Система динамического отслеживания знаний предназначалась для мониторинга прогресса обучения в реальном времени с применением байесовских сетей и рекуррентных нейронных сетей.

Модуль эмоционального анализа разрабатывался для оценки аффективного состояния, обучающегося на основе мультимодальных данных, включая анализ текстовых ответов, временных паттернов взаимодействия и, при наличии соответствующего оборудования, физиологических показателей. Система адаптации контента и взаимодействия предназначалась для динамического изменения сложности, модальности и структуры учебного материала в соответствии с текущим когнитивным состоянием обучающегося.

Для каждого модуля создавались детальные схемы алгоритмов, спецификации интерфейсов взаимодействия и протоколы обмена данными. Особое внимание уделялось обеспечению прозрачности и интерпретируемости алгоритмических решений, что критически важно в образовательном контексте.

4. Экспериментальная валидация и оценка эффективности.

Четвертый этап включал разработку методологии экспериментальной оценки эффективности предлагаемых архитектурных решений. Создавались протоколы пилотного тестирования отдельных компонентов системы с использованием симулированных образовательных сценариев и ограниченных групп пользователей.

Метрики оценки включали объективные показатели обучения, такие как скорость усвоения материала, качество выполнения заданий и долгосрочное удержание знаний. Субъективные показатели охватывали оценку пользователями удобства интерфейса, воспринимаемой релевантности адаптаций и общего удовлетворения процессом обучения.

Дополнительно разрабатывались методы анализа данных взаимодействия пользователей с системой для выявления паттернов эффективного обучения и потенциальных проблемных областей в архитектуре системы. Применялись техники визуализации данных и статистического анализа для интерпретации результатов экспериментов.

В рамках исследования также проводился анализ этических аспектов использования персональных данных обучающихся и разрабатывались рекомендации по обеспечению приватности и безопасности в адаптивных образовательных системах. Особое внимание уделялось проблемам алгоритмической справедливости и предотвращения дискриминации в образовательных рекомендациях.

Результаты

1. Анализ современных технологий ИИ в образовательных системах.

Анализ литературы показал четыре основные категории технологий искусственного интеллекта, которые можно использовать в адаптивных системах обучения совместно с когнитивными принципами. Каждая категория имеет свои возможности для персонализации обучения и требует особого подхода к когнитивному моделированию.

Нейронные сети и глубокое обучение представляют наиболее мощную категорию технологий для анализа сложных образовательных данных. Рекуррентные нейронные сети, особенно архитектуры LSTM и GRU, показывают высокую эффективность в задачах отслеживания знаний, обучающихся во времени. Исследование Чжисюань Чу и его коллег продемонстрировало применение нейронных сетей для когнитивной диагностики в интеллектуальных образовательных системах, где модели способны выявлять латентные когнитивные состояния студентов на основе их ответов на задания [2].

Современные архитектуры трансформеров открывают новые возможности для анализа образовательного контента и генерации персонализированных материалов. Большие языковые модели демонстрируют способность к созданию адаптивного контента, учитывающего уровень знаний и предпочтения обучающихся. Однако их применение в образовании требует тщательной настройки для обеспечения педагогической корректности и соответствия учебным целям.

Системы рекомендаций в образовании эволюционируют от простых коллаборативных фильтров к сложным гибридным моделям, интегрирующим контентную фильтрацию, коллаборативные методы и знания о предметной области. Современные подходы учитывают не только историю взаимодействий обучающегося с системой, но и его когнитивные предпочтения, стиль обучения и текущий уровень знаний.

Технологии обработки естественного языка находят широкое применение в автоматической оценке письменных работ, анализе рефлексивных записей, обучающихся и извлечении семантических паттернов из образовательных текстов. Особый интерес представляют методы анализа эмоционального состояния по текстовым данным, что позволяет системе адаптироваться к аффективному контексту обучения.

2. Принципы когнитивного моделирования в адаптивных системах.

Анализ когнитивных теорий выявил ключевые принципы, которые должны лежать в основе проектирования адаптивных образовательных систем. Теория когнитивной нагрузки Свеллера предоставляет фундаментальную основу для управления сложностью образовательного контента [7]. Согласно этой теории, эффективное обучение происходит при оптимальном балансе между внутренней когнитивной нагрузкой, связанной со сложностью изучаемого материала, внешней нагрузкой, связанной способом представления информации, и продуктивной нагрузкой, способствующей формированию схем знаний.

Модель рабочей памяти Баддели-Хитча указывает на необходимость учета ограничений информационной обработки при проектировании образовательных интерфейсов. Система должна минимизировать нагрузку на центральный исполнитель и эффективно использовать специализированные подсистемы рабочей памяти через мультимодальное представление информации.

Теория двойного кодирования Пайвио подчеркивает важность интеграции вербальной и визуальной информации для улучшения понимания и запоминания [8]. Адаптивные системы должны динамически балансировать различные модальности представления контента в зависимости от когнитивных предпочтений обучающегося и характера изучаемого материала.

Метакогнитивные процессы играют критическую роль в эффективном обучении, включая планирование, мониторинг и оценку собственного понимания. Адаптивные системы должны не только адаптироваться к текущему состоянию обучающегося, но и способствовать развитию его метакогнитивных навыков через рефлексивные инструменты и обратную связь.

3. Архитектура интегрированной адаптивной системы.

По результатам анализа мы разработали многослойную архитектуру адаптивной системы онлайн-обучения, которая объединяет технологии ИИ с когнитивными принципами.

Архитектура состоит из пяти компонентов, каждый из которых выполняет свои функции когнитивного моделирования и адаптации.

Модуль когнитивного профилирования состоит из нескольких алгоритмов машинного обучения, которые создают многомерную модель когнитивных характеристик студента. Система анализирует паттерны взаимодействия с образовательным контентом, включая время отклика на различные типы заданий, предпочтения в модальности представления информации, эффективность различных стратегий решения проблем. Используются методы кластеризации для идентификации когнитивных типов и регрессионные модели для прогнозирования оптимальных параметров обучения.

Система динамического отслеживания знаний построена на гибридной архитектуре, которая использует байесовские сети знаний и рекуррентные нейронные сети. Байесовская компонента моделирует структуру предметной области и взаимосвязи между концепциями, в то время как нейронная сеть отслеживает динамические изменения в состоянии знаний обучающегося. Особое внимание уделяется моделированию процессов забывания и консолидации знаний в соответствии с кривой забывания Эббингауза и принципами распределенной практики [9].

Модуль эмоционального анализа интегрирует несколько источников данных для оценки аффективного состояния, обучающегося. Анализ текстовых ответов выполняется с использованием предобученных языковых моделей, адаптированных для образовательного контекста. Временные паттерны взаимодействия анализируются для выявления признаков фрустрации, скуки или потери мотивации. При наличии соответствующих разрешений система может интегрировать данные о физиологических показателях, таких как вариабельность сердечного ритма или проводимость кожи.

Система адаптации контента и взаимодействия построена как многоагентная архитектура, где различные агенты отвечают за адаптацию специфических аспектов образовательного опыта. Агент управления сложностью динамически регулирует когнитивную нагрузку контента на основе текущих возможностей обучающегося. Агент модальности оптимизирует соотношение визуальных, аудиальных и текстовых элементов в соответствии с когнитивными предпочтениями. Агент последовательности планирует оптимальную последовательность изучения материала с учетом зависимостей между концепциями и принципов эффективного обучения.

Модуль метакогнитивной поддержки помогает развивать навыков саморегуляции обучения. Система предоставляет инструменты для постановки целей, планирования учебной деятельности и рефлексии над процессом обучения. Алгоритмы анализируют паттерны метакогнитивной активности и предоставляют персонализированные рекомендации по улучшению стратегий обучения.

4. Алгоритмы когнитивной адаптации.

Центральным элементом предлагаемой архитектуры является алгоритм когнитивной адаптации, который интегрирует информацию от всех модулей системы для принятия решений об оптимальных параметрах образовательного взаимодействия. Алгоритм основан на принципах многокритериальной оптимизации и использует гибридный подход, объединяющий правила на основе когнитивных теорий с методами машинного обучения.

Процесс адаптации начинается с оценки текущего когнитивного состояния обучающегося на основе данных от всех сенсорных модулей системы. Формируется многомерный вектор состояния, включающий показатели когнитивной нагрузки, эмоционального состояния, уровня знаний по релевантным концепциям и метакогнитивной активности.

Далее система генерирует множество потенциальных адаптационных действий, каждое из которых оценивается по критериям эффективности обучения, когнитивной нагрузки, мотивационного потенциала и соответствия индивидуальным предпочтениям. Используется модифицированный алгоритм NSGA-II для поиска парето-оптимальных решений в многокритериальном пространстве [10].

Особое внимание уделяется прогнозированию долгосрочных эффектов адаптационных решений. Система использует модели временных рядов для оценки влияния текущих

адаптаций на будущее состояние обучающегося, включая риски когнитивной перегрузки, потери мотивации или формирования неэффективных стратегий обучения.

5. Интеграция мультимодального взаимодействия.

Современные достижения в области человеко-компьютерного взаимодействия позволяют создавать более натуральные и эффективные интерфейсы для образовательных систем. Предлагаемая архитектура включает модуль мультимодального взаимодействия, который адаптирует способы коммуникации с обучающимся в зависимости от контекста и когнитивных потребностей.

Визуальное взаимодействие включает адаптивную графику, анимации и интерактивные элементы, которые динамически модифицируются в зависимости от когнитивного стиля обучающегося. Система отслеживает паттерны визуального внимания для оптимизации расположения элементов интерфейса и минимизации когнитивных отвлечений.

6. Система оценки и обратной связи.

Разработанная система оценки интегрирует формативные и суммативные подходы, обеспечивая непрерывный мониторинг прогресса обучения при минимизации тестовой тревожности. Формативная оценка выполняется через анализ процесса решения задач, включая время размышления, количество попыток, использование подсказок и паттерны ошибок.

Суммативная оценка адаптируется к когнитивному профилю обучающегося через вариацию формата заданий, сложности вопросов и способов представления информации. Система использует методы компьютерно-адаптивного тестирования для оптимизации точности оценки при минимизации количества вопросов.

Обратная связь предоставляется на нескольких уровнях детализации и временных масштабах. Немедленная обратная связь фокусируется на конкретных аспектах выполнения задания и предоставляет конструктивные предложения по улучшению. Отложенная обратная связь включает анализ долгосрочных тенденций обучения и рекомендации по развитию метакогнитивных навыков.

7. Экспериментальная валидация компонентов системы.

Предварительные эксперименты с отдельными компонентами архитектуры показали хорошие результаты. Тестирование модуля когнитивного профилирования на выборке из 80 студентов показало точность классификации когнитивных стилей на уровне 78%, что значительно превышает случайные предсказания.

Система динамического отслеживания знаний продемонстрировала улучшение точности прогнозирования успешности выполнения заданий на 23% по сравнению с традиционными методами, основанными только на исторической успеваемости. Особенно высокие результаты наблюдались при прогнозировании долгосрочного удержания знаний.

Модуль эмоционального анализа показал корреляцию 0.72 с самооценками эмоционального состояния обучающихся, что указывает на высокую валидность автоматического распознавания аффективных состояний. Система успешно выявляла признаки фрустрации и скуки, позволяя своевременно адаптировать образовательный процесс.

Пилотное тестирование интегрированной системы на группе из 30 студентов, изучающих программирование, показало улучшение результатов обучения на 34% по сравнению с контрольной группой, использовавшей традиционную онлайн-платформу. Особенно значительными были улучшения в мотивации к обучению и удовлетворенности образовательным процессом.

Обсуждение

Результаты данного исследования демонстрируют значительный потенциал интеграции технологий искусственного интеллекта с принципами когнитивных наук для создания нового поколения адаптивных систем онлайн-обучения. Важность сравнительного анализа с существующими исследованиями заключается в выявлении уникальных преимуществ предлагаемого подхода и определении направлений дальнейшего развития в области персонализированного образования.

1. Сравнение с существующими подходами.

Предлагаемая архитектура существенно отличается от традиционных адаптивных систем более глубокой интеграцией когнитивных принципов в алгоритмы адаптации. В то время как большинство существующих систем фокусируется на адаптации сложности контента на основе правильности ответов, наш подход учитывает многомерные когнитивные характеристики обучающегося, включая стиль обработки информации, метакогнитивные предпочтения и эмоциональное состояние.

Исследование Халкиопулоса и Гкинтони подчеркивает важность когнитивной нейропсихологии в разработке персонализированных систем обучения [1]. Наш подход развивает эту идею, предлагая конкретные алгоритмические решения для операционализации когнитивных принципов в адаптивных системах. В отличие от обзорного характера указанной работы, мы представляем детальную архитектуру и результаты экспериментальной валидации.

Работа по ИИ-адаптивным платформам обучения [11] фокусируется на анализе данных обучающихся для динамической адаптации контента. Наш подход расширяет эту концепцию, интегрируя теоретические основы когнитивной науки для более осознанного и теоретически обоснованного дизайна адаптационных механизмов.

Российские исследования в области применения ИИ в образовании [3] подчеркивают необходимость развития когнитивных способностей, учащихся без формирования зависимости от технологий. Предлагаемая система адресует эту проблему через модуль метакогнитивной поддержки, который обеспечивает условия для развития навыков саморегуляции и критического мышления.

2. Теоретические импликации.

Встраивание когнитивных принципов в алгоритмы машинного обучения дает новые возможности для теории адаптивного обучения. Наш подход показывает, как можно превратить абстрактные когнитивные концепции в математические модели и алгоритмы. Это помогает соединить гуманитарные и технические науки в образовании.

Модель когнитивной нагрузки, традиционно применяемая для статического дизайна образовательных материалов, в нашем исследовании расширена для динамической адаптации в реальном времени. Это является важным теоретическим вкладом в понимание того, как принципы когнитивной психологии могут быть интегрированы в интеллектуальные системы.

Концепция мультимодального когнитивного моделирования, предложенная в данном исследовании, объединяет различные источники информации о когнитивном состоянии обучающегося для создания более полной и точной модели. Это развивает традиционные подходы к моделированию обучающегося, которые обычно фокусируются на одном аспекте, таком как уровень знаний или стиль обучения.

3. Практические импликации для образовательных технологий.

Результаты исследования имеют важные практические импликации для разработчиков образовательных технологий и педагогов. Предлагаемая архитектура показывает, что технически возможно создать системы, которые могут адаптироваться к индивидуальным когнитивным особенностям обучающихся в режиме реального времени.

Модульная архитектура системы дает возможность внедрять компоненты постепенно в уже работающие образовательные платформы. Это упрощает процесс внедрения и позволяет учебным заведениям расширять возможности своих систем без полной замены инфраструктуры.

Особую ценность представляет модуль метакогнитивной поддержки, который может функционировать как отдельный инструмент для развития навыков саморегуляции обучения. Этот компонент адресует критически важную потребность в развитии навыков обучения на протяжении всей жизни в быстро меняющемся мире.

4. Этические соображения и ограничения.

Сбор персональных данных студентов для когнитивного моделирования вызывает вопросы о приватности и согласии. Наша система собирает и анализирует детальную информацию о когнитивных процессах пользователей, что некоторые могут воспринять как вторжение в личную жизнь.

Проблема алгоритмической справедливости особенно актуальна в образовательном контексте, где неточные или предвзятые модели могут привести к неравным образовательным возможностям. Необходимы дополнительные исследования для обеспечения того, чтобы система не дискриминировала обучающихся с нетипичными когнитивными профилями или культурными особенностями.

Риск чрезмерной зависимости от технологии вызывает серьезную озабоченность, особенно в контексте развития автономности и критического мышления обучающихся. Система должна быть спроектирована таким образом, чтобы постепенно передавать контроль над процессом обучения от алгоритма к самому обучающемуся.

5. Технические ограничения и вызовы.

Предлагаемые алгоритмы требуют больших вычислительных ресурсов, что затрудняет их работу в реальном времени. Особенно требовательными являются процессы многокритериальной оптимизации и обработки мультимодальных данных.

Точность когнитивного моделирования существенно зависит от качества и количества доступных данных о обучающемся. В начале взаимодействия с системой, когда данных недостаточно, точность адаптации может быть ограничена, что требует разработки эффективных стратегий.

Интерпретируемость алгоритмических решений остается важным вызовом, особенно при использовании сложных моделей глубокого обучения. Педагоги и обучающиеся должны понимать логику адаптационных решений для эффективного использования системы и поддержания доверия к технологии.

6. Направления будущих исследований.

Перспективные направления развития включают интеграцию достижений в области нейротехнологий для более точного мониторинга когнитивного состояния обучающихся. Использование ЭЭГ (электроэнцефалография), fNIRS (функциональная ближняя инфракрасная спектроскопия) и других методов нейровизуализации может существенно повысить точность когнитивного моделирования, хотя и поднимает дополнительные этические вопросы.

Развитие методов федеративного обучения может позволить создание более точных моделей адаптации при сохранении приватности данных обучающихся. Это особенно важно для масштабирования системы на большие образовательные сети при соблюдении требований защиты данных.

Исследование применения квантовых вычислений для оптимизации сложных многокритериальных задач адаптации может открыть новые возможности для создания более сложных и точных алгоритмов персонализации.

Интеграция с технологиями дополненной и виртуальной реальности открывает интересные перспективы для создания более иммерсивных и адаптивных образовательных сред, которые могут более естественно интегрировать мультимодальные формы взаимодействия и когнитивной поддержки.

Заключение

Целью исследования был анализ возможностей интеграции технологий искусственного интеллекта с когнитивными науками для создания адаптивных систем онлайн-обучения. Мы достигли поставленных целей и получили результаты, которые могут быть полезны для развития образовательных технологий.

Анализ современных технологий ИИ в образовании показал четыре основные категории методов для интеграции с когнитивными принципами:

- нейронные сети и глубокое обучение для анализа образовательных данных;
- системы рекомендаций для персонализации контента;
- технологии обработки естественного языка для анализа текстов;
- мультимодальные интерфейсы для взаимодействия с системой.

Каждая категория продемонстрировала уникальные возможности для создания более эффективных и персонализированных образовательных опытов.

Исследование принципов когнитивного моделирования раскрыло фундаментальные основы для проектирования адаптивных систем, учитывающих естественные механизмы человеческого обучения. Теория когнитивной нагрузки, модель рабочей памяти, принципы двойного кодирования и метакогнитивные процессы были успешно операционализированы в алгоритмических решениях, что позволило создать теоретически обоснованную архитектуру адаптивной системы.

Разработанная многослойная архитектура интегрированной системы представляет инновационное решение, объединяющее пять основных компонентов: модуль когнитивного профилирования, систему динамического отслеживания знаний, модуль эмоционального анализа, систему адаптации контента и модуль метакогнитивной поддержки. Каждый компонент был спроектирован с учетом современных достижений в области машинного обучения и когнитивной науки, что обеспечивает комплексный подход к персонализации образования.

Экспериментальная валидация отдельных компонентов системы подтвердила техническую осуществимость и эффективность предлагаемого подхода. Модуль когнитивного профилирования продемонстрировал точность классификации когнитивных стилей на уровне 78%, система динамического отслеживания знаний улучшила точность прогнозирования успешности на 23%, а модуль эмоционального анализа показал корреляцию 0.72 с самооценками эмоционального состояния. Пилотное тестирование интегрированной системы выявило улучшение результатов обучения на 34% по сравнению с традиционными онлайн-платформами.

Теоретическая значимость исследования заключается в развитии междисциплинарного подхода к проектированию образовательных технологий, который интегрирует достижения информатики, когнитивной психологии и педагогики. Предложенные методы операционализации когнитивных принципов в алгоритмах машинного обучения открывают новые перспективы для создания более эффективных и человекоориентированных интеллектуальных систем.

Практическая значимость работы подтверждается разработкой конкретных архитектурных решений и алгоритмов, которые могут быть имплементированы в существующих образовательных платформах. Модульная структура системы позволяет поэтапное внедрение отдельных компонентов, что снижает барьеры для adoption и облегчает интеграцию с существующей образовательной инфраструктурой.

Особое внимание в исследовании было уделено этическим аспектам использования персональных данных и алгоритмической справедливости в образовательном контексте. Разработанные рекомендации по обеспечению приватности и предотвращению дискриминации могут служить основой для создания ответственных ИИ-систем в образовании.

Вместе с тем, исследование выявило ряд ограничений и направлений для будущей работы. Вычислительная сложность предлагаемых алгоритмов требует дальнейшей оптимизации для обеспечения масштабируемости. Проблема интерпретируемости алгоритмических решений остается актуальной для поддержания доверия пользователей к системе. Необходимы дополнительные исследования для валидации подхода в различных образовательных контекстах и культурных средах.

Перспективные направления развития включают интеграцию нейротехнологий для более точного мониторинга когнитивного состояния, применение федеративного обучения для сохранения приватности данных, исследование возможностей квантовых вычислений для оптимизации сложных алгоритмов адаптации, а также интеграцию с технологиями дополненной и виртуальной реальности.

Результаты показывают, что интеграция искусственного интеллекта и когнитивных наук может существенно улучшить онлайн-образование. Предложенный подход повышает эффективность, персонализацию и доступность обучения. Однако для успешной реализации таких систем нужна работа специалистов разных областей: технологов, педагогов,

когнитивных ученых и экспертов по этике ИИ. Только совместные усилия помогут создать технологии, которые действительно улучшают процесс обучения и развития человека.

Литература

1. Halkiopoulos C., Gkintoni E. Leveraging AI in E-Learning: Personalized Learning and Adaptive Assessment through Cognitive Neuropsychology – A Systematic Analysis // Electronics 2024, 13, 3762. https://doi.org/10.3390/electronics13183762.
2. Chu Z., Wang Y., Cui Q., Li L., Chen W., Qin Z., Ren K. LLM-Guided Multi-View Hypergraph Learning for Human-Centric Explainable Recommendation. 2024. https://doi.org/10.48550/arXiv.2401.08217.
3. Искусственный интеллект в образовании [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_образовании (Дата обращения 07.09.2025).
4. Tan L.Y., Hu S., Yeo D.J., Cheong K.H. Artificial intelligence-enabled adaptive learning platforms: A review // Computers and Education: Artificial Intelligence. 2025. №. 9. https://doi.org/10.1016/j.caeai.2025.100429.
5. Аркабаев Н.К., Мурзакматова З.Ж., Применение искусственного интеллекта для измерения успеваемости учащихся // Вестник Иссык-Кульского университета. 2024. №. 56. С. 98–108. http://doi.org/10.69722/1694-8211-2024-56-98-108.
6. Аркабаев Н.К., Маматова В.Т. Влияние искусственного интеллекта на роль преподавателя при трансформация педагогических компетенций в условиях цифровизации образования // Вестник Ошского государственного университета. Педагогика. Психология. 2025. №. 1(6). С. 49–50. http://doi.org/10.52754/16948742_1(6)_6-2025.
7. Sweller J. Cognitive Load During Problem Solving: Effects on Learning // Cognitive Science. 1988. №. 12(2). Pp. 257–285. https://doi.org/10.1207/s15516709cog1202_4.
8. Clark J.M., Paivio A. Dual coding theory and education // Educational Psychology Review. 1991. №. 3. Pp. 149–210. https://doi.org/10.1007/BF01320076.
9. Murre J.M.J., Dros J. Replication and analysis of Ebbinghaus' forgetting curve // PLoS ONE. 2015. №. 10(7). P. e0120644. https://doi.org/10.1371/journal.pone.0120644.
10. Deb K., Pratap A., Agarwal S., Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA-II // IEEE Transactions on Evolutionary Computation. 2002. №. 6(2). Pp. 182–197. https://doi.org/10.1109/4235.996017.
11. Tan L., Hu S., Yeo D., Cheong K. Artificial Intelligence-Enabled Adaptive Learning Platforms: A Review // Computers and Education: Artificial Intelligence. 2025. №. 9. P. e100429. https://doi.org/10.1016/j.caeai.2025.100429.

УДК 378.147.227

ГРАФОВЫЕ МОДЕЛИ ЗНАНИЙ КАК ИНСТРУМЕНТ НАВИГАЦИИ И ПОВТОРЕНИЯ В LMS

Новиков В.В.[1] (магистрант), **Большаков Г.В.**[1] (магистрант), **Рогаткин Н.А.**[1] (магистрант)
Научный руководитель – кандидат технических наук Бутылкина К.Д.[1]
[1]Университет ИТМО
work_vladimir_novikov@mail.ru

Аннотация
Статья посвящена проблеме системного повторения и навигации в образовательных материалах в системах управления обучением (LMS). В статье рассматривается задача обеспечения системного повторения изученного материала в условиях развития учебных программ и индивидуальных образовательных траекторий. Подчеркивается, что регулярное возвращение к ранее освоенным темам способствует переносу знаний в долговременную память, поддерживает сохранение контекста и формирует устойчивую основу для освоения нового материала. Учитывая особенности процесса забывания и эффективность активного извлечения информации (retrieval practice), обосновывается необходимость интеграции в LMS механизмов интеллектуальной навигации, которые помогают структурировать учебный контент и упрощают доступ к материалам для повторения. В качестве перспективного направления развития LMS предлагается использование графов знаний, позволяющих визуализировать связи между дисциплинами, темами и формируемыми компетенциями. Такой подход помогает студентам быстрее восстанавливать контекст, выявлять содержательные зависимости и эффективно планировать повторение материала. Интеграция графовых моделей в LMS способствует созданию целостного и наглядного представления образовательного процесса, повышая устойчивость знаний и поддерживая освоение сложных областей, включая технические и IT-направления.

Ключевые слова
Графы знаний, LMS, повторение материала, навигация в обучении, визуализация учебного плана.

В современной системе высшего образования вопросам разработки программ, методик преподавания и построения траекторий обучения уделяется значительно больше внимания, чем повторению ранее освоенного материала. Однако именно способность студента возвращаться к уже освоенному материалу системно определяет устойчивость его знаний, глубину профессиональной подготовки и эффективность последующего обучения. Повторение помогает переносить информацию из кратковременной памяти в долговременную, позволяя поддерживать контекст и переходить к более сложным знаниям и структурам [1].

В то же время забывание является естественным эволюционным механизмом, освобождающим ресурсы мозга для новой информации [2]. При этом важный аспект заключается в том, что забывание неравномерно: человек удерживает общую структуру знания, но теряет детали, связи и контекст. Именно контекст, то есть понимание того, как часть связана с целым, является наиболее уязвимым компонентом. Поэтому спустя год студент часто помнит ключевые термины, но не может объяснить, как они соотносятся с практикой или друг с другом.

Современные исследования подчёркивают эффективность активного извлечения (retrieval practice): самостоятельные попытки вспомнить материал закрепляют его лучше, чем пассивное перечитывание, а возвращения к теме с возрастающими паузами значительно повышают долговременное удержание [3].

Образовательный процесс в современном высшем образовании чаще всего строится по семестровому принципу, где каждый курс представляет относительно самостоятельный блок. Это создаёт естественные паузы между связанными темами. В то же время развитие межкурсовых связей и механизмов системного возвращения к предыдущему материалу может значительно усилить накопление и сохранение знаний, особенно в дисциплинах, где важна системность и последовательность в обучении (технические, естественные науки, IT).

Цифровые образовательные платформы (LMS вроде Moodle, Canvas и другие) уже обеспечивают хранение и доступ к материалам прошлых периодов. В то же время текущие функциональные возможности этих систем не помогают студенту понять, где именно в массиве данных находится нужная тема, как она связана с текущей дисциплиной и что именно следует повторить. Таким образом, дальнейшее развитие этих систем возможно в направлении интеллектуальной навигации – поиск связей между темами, рекомендации по повторению. Это может создавать новые возможности в обучении и повысить доступность информации в условиях постоянного роста количества данных.

Кроме того, личные заметки студентов часто распределены по разным устройствам и приложениям (ноутбук, облако, мессенджеры, онлайн-документы). Такие условия делают процесс повторения и закрепления материала длительным и неоптимальным – прежде чем повторять информацию, её нужно найти. Также современные студенты часто опираются на цифровые конспекты, фрагменты переписок с преподавателями, скриншоты с презентаций и материалы из открытых источников. Такая структура знаний является одновременно гибкой и хрупкой: информация легко теряется, смешивается и перестаёт быть доступной. В этой связи внедрение инструментов, позволяющих объединять и структурировать информацию в едином пространстве могут существенно упростить процесс повторения и возвращения к материалам.

Дополнительной возможностью для улучшения навигации студента в его образовательном процессе является перевод учебного плана из табличного в более наглядный и визуально доступный вид. Исследования показывают, что человеческое мышление хорошо работает с визуальными структурами: такие представления приводят к более эффективному восприятию информации и улучшают её понимание [4].

Одним из вариантов такого представления может быть отображение учебного плана в виде графа знаний – структурированной модели данных, которая представляет информацию о сущностях (дисциплинах образовательной программы, темами внутри этих дисциплин) и семантических связях между ними в виде графа, состоящего из узлов (сущностей) и ребер (отношений) [5]. Визуализация в виде графов и карт знаний помогает лучше видеть зависимости между темами, траектории развития компетенций и логику усложнения материала.

Такие системы позволяют:

- быстро восстанавливать контекст забытых тем;
- видеть зависимости между курсами;
- понимать, какие темы стоит повторить перед изучением нового материала;
- ощущать обучение как целостную структуру.

Таким образом, для современного высшего образования повторение и удобная навигация в образовательных материалах студента становятся не просто вспомогательными элементами, а основой для устойчивого и глубокого обучения. Визуализация таких структур в виде графа знаний может повысить наглядность и удобство работы с материалами.

Развитие цифровых образовательных платформ, в том числе LMS, в этом направлении позволит студентам воспринимать образование как связную, живую систему. Это путь к более прочному профессиональному фундаменту и образованию, ориентированному на долгосрочный успех.

Литература

1. Что такое кривая забывания и как помочь студентам запомнить информацию надолго. [Электронный ресурс]. Режим доступа: https://skillbox.ru/media/education/chto-takoe-krivaya-zabyvaniya/ (Дата обращения 10.12.25).
2. Richards B.A., Frankland P.W. The Persistence and Transience of Memory. [Электронный ресурс]. Режим доступа: https://doi.org/10.1016/j.neuron.2017.04.037 (Дата обращения 10.12.25).

3. Karpicke J.D., Roediger H.L. III. (2008). The Critical Importance of Retrieval for Learning. [Электронный ресурс]. Режим доступа: https://www.science.org/doi/10.1126/science.1152408 (Дата обращения 10.12.25).
4. Фадина А.Г., Развитие визуального мышления как средство повышения качества обучения студентов физико-математических специальностей. [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=26186958 (Дата обращения 10.12.25).
5. Граф знаний: Ваше руководство по интеллектуальной интеграции данных. Электронный ресурс]. Режим доступа: https://www.getguru.com/ru/reference/knowledge-graph (Дата обращения 10.12.25).

ТЕХНОЛОГИЧЕСКИЙ МЕНЕДЖМЕНТ

УДК 33

ТЕХНОЛОГИЧЕСКИЙ МЕНЕДЖМЕНТ КАК ОСНОВА ФОРМИРОВАНИЯ ЗАКУПОЧНОЙ СИНЕРГИИ И ФАКТОР ПОВЫШЕНИЯ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ЗАТРАТАМИ ОРГАНИЗАЦИИ

Прохоренко Д.А.[1] (аспирант)
Научный руководитель – доктор педагогических наук, профессор Гладилина И.П.[1]
[1]МГУУ Правительства Москвы имени Ю.М. Лужкова
ProkhorenkoDA@ks.mos.ru, GladilinaIP@ks.mos.ru

Аннотация
В работе рассмотрено влияние практик реализации технологического менеджмента на формирование закупочной синергии и развитие технологичных закупок, обеспечивающих расширение возможностей для повышения эффективности управления затратами организации.
Ключевые слова
Технологический менеджмент, закупочная синергия, эффективность управления затратами организации, категорийный менеджмент в закупках.

Вопрос о разработке инструментов для обеспечения устойчивого развития организации в условиях высокодинамичной внешней среды занимает лидирующие позиции в повестке научных дискуссий и практических исследований в различных областях в течение последних нескольких лет. Помимо глобальных внешнеполитических вызовов это связано с постоянным усложнением технологий, которые лежат в основе современных производственных и бизнес-процессов. Сложность и масштабность задач, решаемых в условиях высокой скорости изменений, превратили реализацию концепции постоянного совершенствования и системный взгляд на все процессы в организации из желательных в критически необходимые для обеспечения ее жизнеспособности. Устойчивость организации и ее также экономическая эффективность достигаются при условии синергии и согласованности работы всех функций.

Непрерывное совершенствование предполагает формирование в организации новой культуры – культуры непрерывного обновления. При этом устойчивость как характеристика организации и бизнес-процесса важна в связи с тем, что она отражает не только эффективность функционирования, но и риски, связанные с ним.

Самосудов М.В. в статье «Механизмы управления системной устойчивостью компании» определяет системную устойчивость организации как «ее способность обеспечивать реализацию целевой функции при изменении условий ее функционирования» [1]. Чернышов В.Н. делает вывод о том, что устойчивость системы представляет собой способность организации возвращаться в состояние равновесия после того, как она была выведена из этого состояния под влиянием внешних или внутренних воздействий [2]. Адаптивность как характеристика организации и бизнес-процесса представляет собой способность приспосабливаться к изменениям внешней среды и скорость реагирования на изменения, создающие угрозу для функционирования или препятствующие нормальному функционированию. Клочков В.В. и Сазонов Д.И. определяют адаптивность как «гибкость, приспособленность предприятий к изменению условий работы» [3]. Проведенный анализ показывает, что системный подход к управлению и комплексное развитие ключевых функций организации в настоящее время являются обязательными условиями функционирования организации в глобальной производственно-сбытовой системе.

Одним из примеров принципиального пересмотра концепции деятельности операционной функции в организации в новых условиях стала функция закупок, которая до наступления глобальных перемен в большинстве российских организаций определялась как центр затрат. Подобная оценка функции закупок представляется очевидно ошибочной, если

учитывать базовые экономические показатели, демонстрирующие потенциальные возможности повышения прибыли организации за счет использования недооцененного резерва закупок.

По данным Европейской экономической комиссии ООН в 2019 году государственные закупки составляли 15–20% объема мирового ВВП [4].

В мае 2024 года информационное агентство «Интерфакс» со ссылкой на заявление заместителя руководителя Федерального казначейства А.Т. Катамадзе представило данные о том, что общий объем государственных закупок и закупок государственных компаний по итогам 2023 года составил 32 трлн. рублей [7], то есть 18,7% объема ВВП России в 2023 году [6].

В 2020 году консалтинговая компания A.T. Kearney, специализирующаяся на исследованиях лучших практик в сфере организации бизнес-процессов, в том числе процессов управления закупками и поставками, представила аналитические данные о том, что затраты на закупки в среднем составляют 30% в объеме выручки организации, специализирующейся на оказании услуг, и 50% и более в объеме выручки организации, осуществляющей производственную деятельность [8].

Оценка функции закупок как операционной в условиях нового рынка и высокой скорости изменений не только лишает организацию новых возможностей для развития и роста за счет экономии затрат, но и создает риски потери рыночных позиций и банкротства. Однако, скрытый потенциал закупок можно образно представить как скрытый в недрах полезный ресурс, извлечение которого происходит посредством сложного многоэтапного процесса, реализуемого с помощью машин и механизмов, персонала, обладающего специальными знаниями и навыками, технологий и инструментов управления. Таким образом, преобразование функции закупок из категории операционной поддерживающей функции в категорию стратегической поддерживающей функции в организации следует оценивать как отдельный проект, реализация которого требует учета следующих факторов:

1. Обеспеченность ресурсами (финансы, компетенции, технологии).
2. Согласованность с развитием других функций организации, достижение единого уровня зрелости всех функций и процессов.
3. Сбалансированный и поэтапный график реализации.

Важно отметить, что с наступлением периода глобальных изменений и введением санкционных ограничений российские организации фактически реализовывали преобразование функции закупок в экстремальных условиях, которые исключали возможность соблюдения стандартных условий процесса.

В научных дискуссиях и в обсуждениях профессионального сообщества активная и ускоренная перестройка и преобразование функции закупок большим числом российских организаций различных отраслей определяется как трансформация функции закупок.

В рамках стандартного процесса преобразования функции закупок из операционной в стратегическую постепенно эволюционирует от «центра расходов» к «центру доходов», переходя от коммерческого этапа зрелости к этапу внешней интеграции и влияния на бизнес-процессы партнерских организаций. При этом текущие операционные задачи функции закупок, необходимые для бесперебойной работы организации, и программа стратегического развития разделены.

С введением санкционного режима в отношении России недружественными организациями обеспечение поставок материалов для бесперебойной работы перестало быть рутинной задачей, для которой достаточно базовых навыков администрирования тендеров и стандартных методов управления. Обеспечение поставки отдельных категорий материалов и оборудования для производства превратилось в задачу, требующую от каждого рядового закупщика способности к самостоятельной многофакторной оценке рисков с использованием аналитического инструментария, а также предпринимательских навыков и критического мышления для реализации рутинных процессов в условиях постоянных изменений и высокой неопределенности.

В связи с отказом большинства европейских поставщиков от продолжения сотрудничества с российскими организациями по поставкам стратегических материалов и

оборудования ранее выстроенные и налаженные цепи поставок были разрушены. Выстраивание новых цепей поставок с поставщиками из дружественных географий, а также закупка по каналам параллельного импорта материалов и оборудования, недоступных у производителей из дружественных географий, потребовали больших дополнительных затрат, новых стратегий и методов закупок.

В этот период во многих организациях службам закупок в части функциональных задач пришлось фактически совершить скачок от операционного уровня, который характеризуется низким уровнем зрелости, к уровню внутренней интеграции, который может быть достигнут при высоком уровне зрелости.

Для решения первоочередной задачи по обеспечению бесперебойных поставок стратегических категорий материалов и оборудования в существующие бизнес-процессы начали активно интегрироваться методы и инструменты категорийного управления, к этому времени подтвердившие свою эффективность в практике крупных российских и иностранных корпораций. Экономическая эффективность категорийного подхода к управлению закупками в организации напрямую зависит от общего уровня зрелости организации.

Данный тезис наглядно иллюстрирует идея Н. Вольфа, представляющая сравнение организации с живым организмом. Сравнение организации с живым организмом представляет взаимообусловленное влияние всех функций в организации друг на друга, а также, что не менее важно, объясняет, почему перестройка одной из стратегических функций организации неизбежно влечет за собой сквозной реинжиниринг бизнес-процессов организации.

Отличительной особенностью закупок от других сервисных функций в организации, является то, что данная функция чаще других выступает в роли «узкого горлышка» основных производственных процессов. На практике можно наблюдать своего рода парадокс. С одной стороны, закупщики часто слышат от коллег мнение о том, что выполнять закупки для организации не сложнее, чем совершать личные бытовые покупки в супермаркете, руководствуясь при выборе товара логикой среднестатистического покупателя. С другой стороны, закупщик, несет повышенную ответственность за обеспечение всех требований для достижения наилучших условий сделки для организации и урегулирование спорных ситуаций между поставщиком и заказчиком на этапах от подписания договора и до передачи товара в производство.

Практика реализации проектов по трансформации закупок российскими организациями в период прошедших трех лет показала, что для успеха важно учитывать, что любая современная организация является системой, функционирующей в условиях активно развивающейся цифровой среды, как внешней, так и внутренней. В контексте этого для понимания логики процессов функции закупок важно учитывать понятие «архитектура предприятия». Термин «архитектура предприятия» был введен в научный оборот в 1980-е гг. Д. Захманом. Первоначально архитектура предприятия понималась как архитектура, определяющая инфраструктуру информационной системы, и обеспечивающая согласованность бизнеса и ИТ. Дальнейшее использование архитектурного подхода в бизнес-инжиниринге показало, что для реализации стратегии организации необходимо обеспечить внутреннюю согласованность всех элементов архитектуры предприятия, то есть цели организации должны быть согласованы с ее миссией, задачи с целями и организационной структурой, показатели должны отражать достижение целей и задач, процессы должны обеспечивать достижение показателей, а информационные системы – выступать в виде каркаса бизнес-процессов и усиливать их. Целью всех бизнес-подразделения предприятия является решение профильных задач, направленных на достижение общих для всех подразделений стратегических целей организации. С учетом этого цели, структура и бизнес-процессы всех подразделений должны быть согласованы с общей архитектурой организации, а также со смежными подразделениями.

Бизнес-процессы всех подразделений организации реализуются в пределах единого контура корпоративной архитектуры, то есть являются взаимосвязанными,

взаимозависимыми и взаимообусловленными. Изменение бизнес-процессов и организационной структуры одного из стратегических подразделений предполагает обеспечения согласованности со смежными подразделениями. Трансформация одного из стратегических подразделений неизбежно приводит к необходимости реинжиниринга бизнес-процессов смежных подразделений. На рисунке 1 представлены упрощенная модель архитектуры предприятия и системы управления закупками с ключевыми элементами, которые определяют их взаимозависимость.

Рис. 1. Система управления закупками и архитектура предприятия

Анализ современного содержания архитектуры предприятия на этапе планирования проекта по трансформации закупок и внедрению системы категорийного управления закупками позволяет сделать выводы, которые важны для обеспечения системности и согласованности предстоящих изменений:

1) целевую модель системы закупок необходимо проектировать исходя из содержания стратегических целей организации, которые предстоит решать, а также учитывая цели и задачи подразделений-заказчиков;
2) при планировании сроков реализации проекта по трансформации необходимо учитывать уровень организационной зрелости, контекст рыночной ситуацию и отраслевую специфику;
3) сроки реализации изменений в значительной степени зависят от уровня развития компетенций сотрудников и их достаточности с учетом задач проекта.

Часто при формировании программы трансформации в качестве основы принимаются программы, которые были успешно реализованы организациями-лидерами отраслей. Ориентация на эталонные показатели лучших практик (бенчмаркинг) является эффективным и распространенным методом оценки эффективности и прогресса. Однако, важно учитывать, что достижение организацией определенных показателей при использовании какого-либо подхода или методологии во многом зависит от качества его адаптации с учетом уровня зрелости, контекста рыночной ситуации, отраслевой специфики, бизнес-модели, наличия или отсутствия инвестиционной (проектной) деятельности.

В отличии от административных изменений (внедрение новой организационной структуры, политики по закупкам и внутренних регламентов) адаптация сотрудников к работе в условиях новых бизнес-процессов и формирование компетенций для решения сложных нестандартных задач не происходят одномоментно. Изменение роли службы закупок с операционной сервисной на стратегическую сервисную требует не только освоения закупщиками методологии, аналитического инструментария и техник проведения переговоров для реализации конкурсных процедур, но и формирования нового образа мышления, перехода от исполнительского подхода к предпринимательскому при решении

рабочих задач. Учитывая системный характер организации, для достижения эффективности в закупочной деятельности предпринимательский подход к решению задач должен быть также принят сотрудниками смежных подразделений.

Взаимообусловленность всех функций в организации является одной из ее основополагающих характеристик, которая проявляется независимо от специфики условий внешней среды. Категорийное управление закупками представляет собой область закупочной деятельности, которая наиболее наглядно демонстрирует влияние организационной синергии на экономические показатели. Активизация скрытых резервов и достижение максимального экономического эффекта в закупках предполагают в качестве обязательных условий закупочную синергию и кросс-функциональное взаимодействие всех подразделений организации.

Авторы Ф. Роземейер, А. В. Вииле и М. Веггеман, анализируя природу закупочной синергии и ее влияние на показатели эффективности закупок, используют модель, представленную на рисунке 2 [5].

Рис. 2. Модель формирования закупочной синергии Ф. Роземейера, А.В. Вииле и М. Веггемана

Экономическая эффективность закупочной деятельности зависит от того, насколько функция закупок является интегративной, ценностно-ориентированной, проактивной и организационно согласованной. Перечисленные характеристики организации взаимообусловлены так же как взаимообусловлены составляющие закупочной деятельности. Шепер В.Дж. в ходе реализации проектов по развитию ИТ-инфраструктуры в компании Deloitte&Touche выявил, что обеспечение согласованности информационных систем со стратегией и политиками организации, системами мониторинга и контроля, организационной структурой, технологическими процессами, сотрудниками и организационной культурой существенно повышает экономическую эффективность организации [9].

Рассмотрим влияние и потенциальные эффекты закупочной синергии на примере стратегии закупок спецтехники для горнодобывающего предприятия, а также узлов, запасных частей и расходных материалов для ее технического обслуживания. Спецтехника и запасные части для технического обслуживания как категории закупок выбраны в качестве примера для настоящего исследования, так как представляют собой стандартизированную номенклатуру и бизнес-модель поставок, и взаимодействия поставщика и заказчика, которая может быть применена также и в других отраслях.

В досанкционный период одной из распространённых стратегий закупки спецтехники и запасных частей для технического обслуживания была стратегия выбора единого поставщика для поставки техники и последующего комплексного технического обслуживания спецтехники в постгарантийный период с установлением КПЭ для поставщика в виде целевого показателя коэффициента технической готовности техники (КТГ). В рамках договора комплексного сервисного обслуживания дилер производителя спецтехники, выступавший в качестве поставщика запасных частей и узлов для ремонта, формировал и контролировал исполнение графика планово-предупредительных ремонтов, обеспечивал планирование и контроль поставки запасных частей, узлов и расходных материалов на объекты эксплуатации техники, формировал аналитическую базу о состоянии техники с

использованием специализированного программного обеспечения, обеспечивал присутствие на объектах заказчика собственных сервисных инженеров. Фактически, при заключении подобного подхода к закупке спецтехники и запасных частей заказчик передавал на аутсорсинг часть профильных функций, снимая нагрузку с собственных технических подразделений. Выбор данной стратегиями крупными горнодобывающими холдингами определялся рядом причин:

1) обеспечение дилером производителя спецтехники гарантий бесперебойной работы техники и, как следствие, минимизация риска простоя производства в связи с поломками техники с возможностью обеспечения контроля в формате «одного окна»;
2) возможность оптимизации штата технического персонала заказчиком;
3) возможность привлечения высококвалифицированных технических экспертов поставщика и обеспечение качественного сервиса в регионах с ограниченной возможностью найма персонала с подобной квалификацией.

Возможность обеспечения поставщиками вышеперечисленных преимуществ предполагает взаимную интеграцию бизнес-процессов. Поставщик и заказчик становятся стратегическими партнерами с высоким уровнем влияния на бизнес-показатели друг друга.

С учетом этого при подобной стратегии с введением санкционных ограничений был фактически реализован риск разрушения цепочки поставок в связи с отказом стратегического партнера от сотрудничества с последующей необходимостью не только поиска нового источника поставки, но и восполнения потери профильной экспертизы, которая предоставлялась поставщиком в виде дополнительных сервисов.

Оценивая влияние технологического менеджмента на скорость выстраивания новых цепей поставок следует выделить роль системы планирования и системы внутреннего мониторинга технического состояния оборудования, обеспечивающих получение данных о потребности в материалах на период от 1 года и более.

Отсутствие или низкий уровень развития данных систем, в том числе, являлось препятствием для реализации стратегии поставок запасных частей с передачей техники на комплексное обслуживание альтернативным поставщикам из дружественных географий, так как многие альтернативные производители, начиная работу на российском рынке в этот период, не обладали необходимой инфраструктурой, ИТ-системами, достаточным количеством технических экспертов. Задача по настраиванию бесперебойных цепей поставок в этот момент стала вызовом для обеих сторон - заказчика и поставщика – и потребовала совместной работы и развития внутренних процессов смежных функций. В контексте происходящего некоторые эксперты в области закупок полагают, что в условиях турбулентного рынка категорийный менеджмент переживает свой ренессанс. В условиях постоянных изменений возросла роль управления рисками поставок и обеспечения быстрой адаптивности бизнес-процессов и команды к изменениям. В качестве отличительной характеристики категорийного управления в условиях постоянных изменений рыночной среды стал более короткий горизонт планирования и высокая частота актуализаций и контроля. Закупочные бизнес-процессы в современных условиях отличает высокая интенсивность и высокая скорость. Как следствие, возрастает необходимость в развитии у всех сотрудников службы закупок способности к самостоятельной оценке рисков по процессам, находящимся в зоне их ответственности, формирования сценариев решения задач и обоснования предлагаемого приоритетного решения.

Категорийное управление закупками представляет собой формализованный и системный подход, целью которого является обеспечение устойчивого развития организации через повышение ценности закупок товаров, оборудования, работ, услуг при сохранении целевого уровня качества продукции, технологий и сервисов.

Преимущества использования категорийного подхода при управлении закупками организации:

1) рост прибыли организации за счет оптимизации затрат на закупку стратегических групп номенклатур (категорий), обладающих высоким потенциалом экономии и наибольшим влиянием на затраты организации;

2) создание дополнительных возможностей за счет использования профильной экспертизы поставщиков и развития долгосрочного партнерства со стратегическими поставщиками;
3) повышение надежности цепей поставок и минимизация рисков срыва поставок или поставки некачественных товаров и, как следствие, простоев производства.

Однако, оценивая сроки, риски и перспективы перехода системы закупок конкретной организации к концепции категорийного управления важно учитывать зрелость ее системы управления и всех бизнес-процессов. Обязательными условиями достижения ожидаемых целевых результатов при переходе к категорийному управлению в закупках, являются комплексное совершенствование всех внутренних процессов организации и формирование необходимых компетенций и навыков не только у сотрудников службы закупок, но и у сотрудников смежных служб (производственный блок, финансовый контроль и т.д.).

Применительно к проблеме эффективности управления стратегическими закупками организации и внедрения категорийного управления отсутствие в организации практики технологического менеджмента создает риск ограничения возможностей использования экономического потенциала категорийного менеджмента и сведения его лишь к проблеме минимизации затрат на закупку за счет укрупнения объемов закупки в результате консолидации потребности в однородных группах номенклатур от различных подразделений предприятия или бизнес-единиц холдинговой структуры. В этом случае фактически реализуется только начальный этап внедрения концепции категорийного управления.

Литература

1. Самосудов М.В. Механизмы управления системной устойчивостью компании // Современная конкуренция. 2008. №. 4. С. 55–56.
2. Чернышов В.Н. Теория систем и системный анализ: учеб. пособие/В.Н. Чернышов, А.В. Чернышов. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2008. 8 с.
3. Клочков В.В., Сазонов Д.И. Методы анализа адаптивности производственных программ и организационных структур предприятий // Экономика и математические методы. 2007. Т. 43. №. 2. С. 44–56.
4. Рекомендация № 43 ЕЭК ООН Устойчивые Закупки. Минимальные общие критерии устойчивости процессов закупок для отбора поставщиков из числа микро, малых и средних предприятий [Электронный ресурс]. Режим доступа: https://unece.org/sites/default/files/2023-10/Rec43-ECE_TRADE_451R.pdf (Дата обращения 09.09.2025).
5. Rozemeijer F.A., van Weele A.J., Weggeman M. Creating Corporate Advantage Through Purchasing: Toward a Contingency Model. The Journal of Supply Chain Management. [Электронный ресурс]. Режим доступа: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-493X.2003.tb00145.x (Дата обращения 09.09.2025).
6. Росстат оценил рост ВВП в 2023 году в 3,6 процента. [Электронный ресурс]. Режим доступа: https://minfin.gov.ru/ru/press-center/?id_4=38851-rosstat_otsenil_rost_vvp_v_2023_godu_v_36_protsenta (Дата обращения 09.09.2025).
7. Объем госзаказа в России в 2023 году составил 32 трлн рублей. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/business/960655 (Дата обращения 09.09.2025).
8. To enjoy growing profit, we need to focus on the single largest cost. [Электронный ресурс]. Режим доступа: https://www.kearney.com/service/procurement/article/realizing-the-power-of-procurement (Дата обращения 09.09.2025).
9. Sheper W.J. Business IT Alignment: solution for the productivity paradox (In Dutch) // Industrial Management & Data Systems. 1999. Vol. 99. Iss. 8. Pp. 367–373.

Оглавление

Известия студенческой науки

Сборник научных трудов

Выпуск 1. Том 4

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 16.12.2025
Объем издания 1899 Мб
Заказ № 4937 от 16.12.2025

Материалы печатаются в авторской редакции.

Издательство Университет ИТМО

ISBN 978-5-7577-0743-3

ИТМО