

Секция «Цифровые коммуникации и искусственный интеллект в государственном управлении»

## Искусственный интеллект как метод противодействия угрозам экономической безопасности

Научный руководитель – Олейник Наталья Михайловна

*Симонова Виктория Владиславовна*

*Студент (специалист)*

Северо-Западный институт управления - филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Факультет экономики и финансов, Кафедра экономики и управления бизнесом (базовая кафедра), Санкт-Петербург, Россия

*E-mail: vsimonova-22-01@ranepa.ru*

Интерес к применению технологий искусственного интеллекта (ИИ) связан с широкими возможностями, отрывающимися как перед государством, так и перед бизнесом. Необходимость рассмотрения возможности применения цифровых технологий, таких как ИИ, обусловлена их результативностью и эффективностью при решении широкого спектра задач в достижении целей, в том числе и задач управления экономической безопасностью на предприятиях, представляющих разные секторы российской экономики.

Современные российские предприятия сталкиваются с вызовами, обусловленными как внутренними, так и внешними условиями, что порождает разнообразные риски — экономические, финансовые, информационные, кадровые и пр., что может отрицательно сказаться на итогах хозяйственной деятельности. Связь между возникающими угрозами и результативностью бизнеса проявляется через их влияние на стабильность и защищенность экономической среды компании.

Экономическая безопасность (ЭБ) – это состояние защищенности экономики от внутренних и внешних угроз, обеспечивающее поступательное развитие и защиту интересов государства, бизнеса и общества. Понятие «экономическая безопасность» интерпретируется учеными по-разному, в зависимости от методологических подходов и уровня анализа, однако все определения объединяет идея защиты экономики от угроз и обеспечения условий для ее устойчивого развития. Отсутствие единого определения отражает сложность и многогранность понятия, что требует изучения понятий «угроза» и «риск».

Центральной задачей в области ЭБ организаций выступает ее поддержание в ситуации, когда на нее воздействуют угрозы как изнутри, так и извне. В наши дни особое значение приобретают вызовы, связанные с внешними условиями, которые несут в себе увеличенные риски для финансовой стабильности. В связи с этим возникает потребность в их эффективном регулировании. Формируемые в современной практике угрозы и риски приводят к необходимости совершенствования системы обеспечения ЭБ хозяйствующих субъектов. Одним из направлений обеспечения ЭБ является цифровизация с использованием высокоинтеллектуальных систем, построенных на базе информационных технологий. Такая приоритетность обусловлена текущими тенденциями цифровой трансформации социально-экономической сферы, появлением новых технологий и высокая степень их интеграции в различные направления хозяйственной деятельности. Вышеперечисленные тенденции обеспечивают рост доступности технологий и разработок, позволяя их применять в процессе совершенствования системы управления бизнесом.

Одним из способов преодоления возникших сложностей выступает применение разнообразных методов определения угроз, влияющих на экономическую стабильность предприятия. Первый метод связан с проведением внутреннего аудита, проверка и экспертиза

которого позволяет получить аудиторские доказательства для корректировки управленческих решений менеджера. Вторым методом является аналитическим, куда относится модель Маккинси, в рамках применения которой проводится оценка конкурентоспособности предприятия через анализ его внутренней среды по 7 категориям, 3 из которых «жесткие», а 4 «мягкие»; модель Адизеса, использование которой заключается в том, что все компании схожи с живыми организмами и проходят одинаковые стадии жизненного цикла; SWOT анализ, который представляет из себя классический инструмент оценки конкурентоспособности, базирующийся на анализе четырех сфер, среди которых сила, слабость возможности и угрозы компании. Связь этих методов с ИИ проявляется в том, что современные технологии способны значительно усилить их эффективность и глубину применения. Например, при проведении внутреннего аудита ИИ может использоваться для автоматизации анализа больших объемов данных, выявления скрытых закономерностей или аномалий, что позволяет быстрее и точнее получать аудиторские доказательства для корректировки управленческих решений. Что касается аналитических подходов, таких как модель Маккинси, ИИ может оптимизировать оценку внутренней среды предприятия, обрабатывая информацию по семи категориям с учетом множества переменных, включая как «жесткие», так и «мягкие» аспекты, и предоставляя более детализированные выводы. В случае модели Адизеса технологии ИИ способны прогнозировать этапы жизненного цикла компании, анализируя исторические данные и текущие показатели, что делает сравнение с биологическими организмами более точным и практически применимым. Для SWOT-анализа ИИ может расширить возможности классического подхода, автоматически собирая данные из внешних и внутренних источников, выявляя сильные и слабые стороны, а также потенциальные возможности и угрозы с учетом динамики рынка и поведения конкурентов. Таким образом, ИИ выступает как инструмент, который обогащает традиционные методы, ускоряя их выполнение, повышая точность и предоставляя новые аналитические возможности для управления экономической стабильностью предприятия.

Кроме того, способы противостояния угрозам ЭБ все активнее опираются на передовые цифровые решения, среди которых выделяется использование ИИ. Технологии ИИ – это цифровые технологии нового поколения, с помощью которых происходит информационно-аналитическая поддержка системы управления, предотвращение и защита периметра организации от внешних угроз. С помощью технологий ИИ мы получаем возможность быстро получить данные, прогнозировать будущее состояние, планировать, моделировать ЭБ. По данным Национального центра развития ИИ при Правительстве РФ, средний уровень внедрения технологий ИИ в отраслях экономики составляет 31,5%. Лидерами являются сфера финансовых услуг и сфера информационно-коммуникационных технологий: 55,3% и 54,3% соответственно [2].

Значение ИИ заключается в его способности поддерживать экономическую стабильность и защищать от рисков, возникающих в цифровой среде. По данным компании BI.ZONE в 2024 г. наибольшее количество атак пришлось на госструктуры (15%), финансовую отрасль (13%), транспорт и логистику (11%) [3].

Для обеспечения экономической безопасности субъектов хозяйствования применяются комплекс методов, направленных на предотвращение, минимизацию и нейтрализацию угроз. Это правовые (законы, распоряжения, стратегии, в первую очередь – развитие нормативной базы для ИИ), организационные (внутри предприятия: кадры и их обучение), инженерно-технические (выявление слабых мест в технологиях защиты информации), технологические или инновационные (обеспечение кибербезопасности, защита всех ресурсов), информационно-аналитические (биг дата, программное обеспечение, коммерческая тайна, защита от утечки информации и хищений, мониторинг рисков), экономические (минимизация рисков, финансовая устойчивость, ИИ сигнализируют о возможных

отклонениях в финансовых показателях). Эффективное противодействие угрозам угрозам экономической безопасности требует сочетания различных мер правового, организационного, инженерно-технического, технологического и информационно-аналитического характера, где ИИ становится одним из методов, благодаря способности анализировать базы данных, противодействовать киберугрозам и прогнозировать риски. Более того, ИИ не только фиксирует угрозы, но и предлагает конкретные меры по их устранению, оценивая их долгосрочное влияние на стабильность компании.

Максимальная защита достигается только при синергии всех этих подходов. Технические решения укрепляют инфраструктуру, аналитика обеспечивает мониторинг, правовая база создает условия для инноваций, а обучение персонала минимизирует ошибки. Искусственный интеллект выступает связующим звеном, усиливая каждый элемент системы: он прогнозирует риски, моделирует сценарии и помогает оперативно реагировать на изменения. Такой интегрированный подход позволяет организациям не только преодолевать текущие трудности, но и выстраивать долгосрочную стратегию защиты в условиях неопределенности и растущих угроз.

Процесс внедрения искусственного интеллекта в экономику и управление набирает обороты, и его эффективность уже очевидна. Тем не менее, есть факторы, которые тормозят этот прогресс. Среди них — недостаток цифровой инфраструктуры, необходимой для работы таких технологий, значительные затраты на их интеграцию и нехватка специалистов, которые могли бы грамотно управлять системами ИИ. Несмотря на это, искусственный интеллект остается мощным инструментом в борьбе с угрозами экономической безопасности. Он переводит управление рисками на новый уровень, делая процессы более структурированными и автоматизированными. При этом важно понимать, что ИИ не вытесняет человека из процесса принятия решений, а выступает как поддержка, дополняя человеческий опыт и интуицию.

Внедрение ИИ в различные бизнес-сферы начинается со сбора и обработки необходимых данных, трансформирования и систематизации их в нужный структурированный вид. Следующим шагом является разработка ИИ-алгоритмов, которые будут способны к самообучению. Здесь необходимы квалифицированные ИТ-специалисты, которые смогут научить систему ИИ всем необходимым для компании или бизнеса действиям. Сегодня на рынке создано достаточно большое количество готовых ИИ-решений, которые помогут настроить алгоритмы ИИ быстрее и качественнее. После получения необходимой информации от системы ИИ осуществляется перестройка всех технологических и бизнес-процессов, на которые оказывают влияние алгоритмы ИИ.

С целью обеспечения эффективного использования технологий ИИ при цифровой трансформации системы управления ЭБ организацией требуется развитие человеческих ресурсов, формирования цифровых навыков у сотрудников при работе с информационно-коммуникационными системами бизнеса [1]. В этих целях предлагается налаживать профессиональную подготовку непосредственно на предприятиях либо задействовать внешние компании, которые занимаются проведением бизнес-тренингов и программ обучения для специалистов, адаптированных к реалиям цифровой экономики. Итогом такой стратегии в работе с кадрами станет укрепление их конкурентных позиций, рост результативности и отдачи от труда, а также, что особенно значимо, совершенствование управленческих процессов, где ключевые решения будут приниматься опытными и квалифицированными сотрудниками.

Таким образом, противодействие угрозам ЭБ предприятий при помощи использования технологий ИИ в условиях современной экономики характеризуется наличием проблем и преимуществ, которые формирует реализация подобной стратегии развития. В нашем понимании, данный процесс имеет более положительное воздействие, формируя новые

конкурентные преимущества и создавая устойчивый фундамент для стратегического масштабирования бизнеса, выводя его на новые рынки (отраслевые и региональные). Поэтому предприятиям рекомендуется принимать дополнительные управленческие решения, которые позволят нивелировать угрозы, связанные с использованием ИИ, и, наоборот, усилить положительный эффект от реализации проектов, связанных с внедрением данных технологий в бизнес-процессы и систему управления.

Стоит отметить, что использование технологий ИИ в современной практике российских организаций различных отраслей может быть направлено на повышение эффективности управленческих процессов, что совершенствует практику управления, делая ее экономически и финансово результативнее. Поэтому приоритетной стратегией цифровизации бизнеса современных предприятий является интеграция данных технологий в системы управления ЭБ. Результатом таких мер является улучшение устойчивости и конкурентоспособности организации, несмотря на ухудшение условий внешней бизнес-среды.

Перспективы развития технологий ИИ связаны с возможностью их использования при повышении точности прогнозирования угроз, из-за которых снижается ЭБ организаций и целых отраслей. Благодаря внедрению ИИ создаются условия минимизации рисков путем предотвращения угроз, возможность спрогнозировать приблизительное время и место угроз. Результаты такого прогнозирования напрямую связаны с возможностью анализа базы больших данных, где рутинное участие человека замедляет процессы и точность прогнозов.

Таким образом, проведенное исследование показало, что методы применения ИИ способствуют противодействию угрозам ЭБ и создает устойчивые экономические системы.

### Источники и литература

- 1) Олейник Н.М. Текущие тенденции и проблемы внедрения технологий искусственного интеллекта в экономику и государственное управление // Первый экономический журнал. 2024. № 10 (352). С. 159-170.
- 2) Осадчук Е.В. Внедрение технологий искусственного интеллекта в отечественной экономике: взгляд практика // Управление наукой: теория и практика. 2024. Т. 6, № 1. С. 127-146.
- 3) Исследование ThreatZone 2025: представили годовую динамику российского ландшафта угроз // URL: <https://cisoclub.ru/issledovanie-threat-zone-2025-predstavili-godovuju-dinamiku-rossijskogo-landshafta-ugroz/> (дата обращения: 01.03.2025).