ISSN 2522-9613 (Print)
ISSN 2524-2822 (Online)

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

Том 32, № 1, 2026

Научный журнал издается с 1995 года

Учредитель
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Журнал включен в базы данных:
DOAJ, Google Scholar, Mendeley, Open Alex, РИНЦ и другие

СОДЕРЖАНИЕ

ЭКОНОМИЧЕСКИЕ НАУКИ, ОБРАЗОВАНИЕ

Издание перерегистрировано в Министерстве информации Республики Беларусь 10 июня 2022 г.
Регистрационный номер 662

Журнал включен в Перечень научных изданий Республики Беларусь для опубликования результатов диссертаций по следующим научным направлениям: технические (информатика, вычислительная техника и управление) и экономические науки

Подписано в печать 18.03.2026. Формат бумаги 60×84⅛. Бумага офисная. Отпечатано на ризографе. Гарнитура Таймс. Усл. печ. л. 7,21. Уч.-изд. л. 5,4. Тираж 52 экз. Заказ 37.

Адрес редакции: 220013, г. Минск, ул. П. Бровки, 6
Белорусский государственный университет информатики и радиоэлектроники
Тел.: +375 17 293-88-41.
dig.tr@bsuir.by; http://dt.bsuir.by

Отпечатано в БГУИР. ЛП № 02330/264 от 24.12.2020.
220013, г. Минск, ул. П. Бровки, 6

ISSN 2522-9613 (Print)
ISSN 2524-2822 (Online)

DIGITAL TRANSFORMATION

V. 32, No 1, 2026

The scientific journal is being published since 1995

Founder
Educational Establishment "Belarusian State University of Informatics and Radioelectronics"

The Journal is included in the following databases:
DOAJ, Google Scholar, Mendeley, Open Alex, RISC et. al.

CONTENTS

Publication is re-registered in the Ministry of Information of the Republic of Belarus in 2022, June, 10th
Reg. No 662

Signed for printing 18.03.2026. Format 60×84 ⅛. Office paper. Printed on a risograph. Type face Times.
Ed.-pr. l. 7,21. Ed.-ed. l. 5,4. Edition 52 copies. Order 37.

Address
Belarusian State University of Informatics and Radioelectronics
6, P. Brovki St., 220013, Minsk
Tel.: +375 17 293-88-41
dig.tr@bsuir.by; http://dt.bsuir.by

Printed in BSUIR. License LP No 02330/264 from 24.12.2020.
6, P. Brovki St., 220013, Minsk

http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11

УДК 338.2

ФАКТОРЫ ФОРМИРОВАНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВА В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ ТУРБУЛЕНТНОСТИ

Е. Ю. РАКОВА

Белорусский государственный экономический университет (Минск, Республика Беларусь)

Аннотация. По мере проникновения цифровых технологий в экономику, политику и повседневную жизнь концепция цифрового суверенитета приобретает все большее значение. Однако в литературе отсутствует универсальное определение. Научная новизна исследования заключается в систематизации основных концепций цифрового суверенитета и подходов различных стран к его реализации. Особый интерес представляет анализ внутренних и внешних факторов, определяющих степень стратегической цифровой автономии того или иного государства. Аргументы автора склоняются в пользу гибкой стратегии, направленной на достижение стратегической автономии в критических областях при одновременном использовании преимуществ международной технологической кооперации, а также усилении применения мягких образовательных и просветительных мер и инструментов.

Ключевые слова: цифровой суверенитет, цифровая безопасность, информационный суверенитет, информационная безопасность, интернет-суверенитет, суверенитет данных, информационно-коммуникационные технологии, искусственный интеллект.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Ракова, Е. Ю. Факторы формирования цифрового суверенитета государства в условиях геополитической турбулентности / Е. Ю. Ракова // Цифровая трансформация. 2026. Т. 32, № 1. С. 5–11. http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11.

FACTORS IN THE FORMATION OF STATE DIGITAL SOVEREIGNTY IN THE CONDITIONS OF GEOPOLITICAL TURBULENCE

ELENA RAKOVA

Belarus State Economic University (Minsk, Republic of Belarus)

Abstract. As digital technologies permeate the economy, politics, and everyday life, the concept of digital sovereignty is gaining increasing importance. However, a universal definition is lacking in the literature. The research's novelty lies in its systematization of the key concepts of digital sovereignty and the approaches various countries take to implementing it. Of particular interest is the analysis of the internal and external factors that determine the degree of strategic digital autonomy for each state. The author argues for the need for a flexible strategy aimed at achieving strategic autonomy in critical areas while simultaneously leveraging the benefits of international technological cooperation and strengthening the use of soft educational and awareness-raising measures and tools.

Keywords: digital sovereignty, digital security, information sovereignty, information security, internet sovereignty, data sovereignty, information and communication technologies, artificial intelligence.

Conflict of interests. The author declares that there is no conflict of interests.

For citation. Rakova E. (2026) Factors in the Formation of State Digital Sovereignty in the Conditions of Geopolitical Turbulence. *Digital Transformation.* 32 (1), 5–11. http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11 (in Russian).

Введение

Цифровой суверенитет определяется сложным балансом внутренних и внешних факторов. В настоящее время внешние факторы являются драйвером суверенизации и сегментации интернета. Однако важными представляются и внутренние факторы, на которые государство может и должно влиять.

Исходя из проведенного анализа, предложены некоторые меры государственной политики, которые будут способствовать развитию и укреплению цифрового суверенитета. Начало XXI в. было стартом деглобализации и распада мировых хозяйственных связей. По мере обострения экономических и политических противоречий набирает популярность концепция суверенитета как противоположность различным проявлениям гегемонизма, будь то гегемония США в международных отношениях или гегемония частных корпораций [1, с. 130]. Идеи суверенизации коснулись и цифровой сферы. По мере развития информационно-коммуникационных технологий (ИКТ) и глобального лидерства западных стран появляется интерес к защите собственного информационного пространства и суверенизации критической информационной инфраструктуры. Лидером становится Китай, первым начавший жестко и последовательно защищать свои «виртуальные» границы. Постепенно в научной литературе появляются концепции интернет-суверенитета, информационного и цифрового суверенитета.

Теоретические аспекты понятия «цифровой суверенитет»

Следует отметить, что хотя проблематика формулирования и реализации права государства на суверенитет в сфере ИКТ давно существует, в литературе отсутствует единое научное определение цифровой независимости или цифрового суверенитета. Каждый автор видит его по-разному, а суть понятия варьируется от цифрового до информационного суверенитета или безопасности, используя в определении комбинацию ключевых слов: суверенитет, технологии, инфраструктура и данные [1–6].

Представленные в статье концепции являются ответом на глобализацию и цифровизацию и направлены на усиление роли государства в управлении и контроле над различными аспектами цифрового пространства. Технологический суверенитет стоит в основании пирамиды, обеспечивая способность создавать «железо» и «софт». Суверенитет данных отвечает на вопрос «Что регулируется?». Информационный суверенитет отвечает на вопрос «Зачем?», а интернет-суверенитет – на вопрос «Как?». Обобщает все концепции понятие «цифровой суверенитет», включающее в себя все составляющие подлинной независимости: от верховенства права до контроля над данными и технологиями.

Рассмотрим более подробно различные виды концепций:

• технологический суверенитет – это способность государства проводить независимую политику в сфере высоких технологий [1, с. 90]. Он реализуется на базовом уровне, обеспечивающем физический контроль над сетями и инфраструктурой. Сюда относят владение ключевыми технологиями, которые считаются критически важными для обеспечения функционирования основных институтов государства и конкурентоспособности: контроль над магистральными каналами передачи данных, точками обмена интернет-трафиком (IXP), сетями мобильной связи (4G/5G); наличие и управление собственными дата-центрами; независимая работа энергосистем, финансовых сетей, транспорта, которые управляются цифровыми системами; национальные системы доменных имен (DNS), позволяющие интернету работать внутри страны, даже если связь с глобальными серверами прервана;

• суверенитет данных – контроль над хранением и обработкой данных, а также «рациональные действия национальных государств, направленные на установление контроля над потоками конфиденциальных данных внутри собственных границ и за их пределами» [8, с. 10]. Можно сказать, что это правовой принцип, согласно которому информация (особенно персональные данные) подчиняется законам и нормам страны, на территории которой она находится. Таким образом, объектом защиты являются данные, а инструментами защиты – законы о защите данных, требования локализации данных (хранения на территории страны), их шифрование. Этот подход зачастую является самым конкретным и юридически оформленным в национальных юрисдикциях. Ключевые элементы – рациональные действия национальных государств, направленные

на установление локализации и контроля над потоками, хранением и обработкой данных внутри собственных границ и за их пределами. Другими словами, суверенитет данных – это обеспечение юрисдикции государства над данными на своей территории, их защита от несанкционированного доступа иностранных государств и компаний. Негативным следствием сильного суверенитета данных может являться фрагментация интернета (распад единого информационного пространства на ряд самостоятельных подсистем), однако «сама по себе такая политика сопряжена со значительными издержками, возникающими вследствие цифровой и физической изоляции страны» [8, с. 10];

• информационный суверенитет. В этом подходе подчеркивается исключительное право государства на определение информационной политики, задается идеологическая и ценностная рамка регулирования. Фокус смещается на защиту информационного пространства от деструктивного влияния извне, ориентацию на национальные интересы, обеспечение доминирования национальной культуры и идеологии. Его инструменты – политические и правовые режимы обработки данных, суверенное право страны проводить собственную информационную политику, т. е. контроль не только над технологической инфраструктурой, но и над способами создания и передачи информации. Важность данной концепции можно подчеркнуть тезисом, что информационный суверенитет является разновидностью государственного суверенитета [7, с. 119];

• интернет-суверенитет, или суверенный интернет, – способность государства обеспечивать устойчивое и независимое функционирование национального сегмента сети интернет, включая управление его критической инфраструктурой даже в условиях разрыва соединений с глобальной сетью [3, с. 78]. Именно поэтому иногда встречается такое определение, как сетевой суверенитет. Объектами регулирования являются интернет-инфраструктура и трафик. Это самый технически ориентированный вид суверенитета. Он направлен непосредственно на архитектуру и управление сетью интернет. Его цели – обеспечивать права государства устанавливать собственные правила функционирования интернет-пространства, отвечающие национальным традициям и интересам, гарантировать устойчивость и управляемость национального сегмента интернета, его защиту от внешних отключений и угроз. Инструментами государственной политики в данном случае являются национальное законодательство, контроль за интернет-провайдерами, фильтрация контента, ограничение доступа к ресурсам;

• цифровой суверенитет – самое широкое понятие. Объект регулирования в данной концепции – цифровая экосистема в целом, т. е. государство осуществляет контроль над коммуникационной инфраструктурой и интернетом в пределах национальных границ, обеспечивает независимость программного обеспечения и платформенной экономики, в том числе через национальные поисковые системы, социальные сети, почтовые сервисы, а также суверенитет данных. Главная цель – достижение технологической автономии, способности самостоятельно развивать и поддерживать критически важные цифровые технологии.

Таким образом, «цифровой суверенитет представляет собой способность государства самостоятельно, без вмешательства извне, определять порядок использования цифровых технологий, регулировать процессы сбора и обработки данных, а также обеспечивать безопасность и устойчивое функционирование национального сегмента информационно-коммуникационной сети интернет» [5, с. 40]. Можно сказать, что цифровой суверенитет – это стратегическая цель государства, тогда как другие концепции будут являться тактиками по ее достижению.

Правовые аспекты реализации цифрового суверенитета

В современном турбулентном мире каждая страна в меру своих возможностей и ограничений реализует концепцию информационного и цифрового суверенитета. Так, технологические компании США обязаны передавать данные о телефонных звонках, текстовых сообщениях и электронных письмах разведывательным службам США, включая ФБР, ЦРУ и АНБ. Тенденция последних лет – защита лидерства США в области критических технологий. Промышленный протекционизм и система ограничительных мер (например, на поставки высокотехнологичного оборудования в Китай в области искусственного интеллекта и облачных вычислений), а также масштабные инвестиции во внутренние исследования и стимулирование производства полупроводников в США призваны стимулировать внутреннее производство. То есть формально США стоят на принципах свободного интернета, однако в реальности все больше используют те или иные ограничительные и запретительные меры.

Европейский союз активно применяет различные нормативно-регуляторные меры защиты цифрового суверенитета. Основными инструментами являются Общий регламент по защите данных (General Data Protection Regulation, GDPR), который определяет порядок сбора, обработки, хранения и распространения персональных данных в странах Евросоюза, и Закон о цифровых услугах (EC) (Digital Services Act). На социальные сети, поисковые системы и торговые площадки, такие как Apple, Google, TikTok и Amazon, возложены дополнительные обязательства по борьбе с распространением незаконного контента, разжиганием ненависти, с дезинформацией и коммерческим мошенничеством (неправильный контент необходимо мониторить и немедленно уничтожать). Закон стал предметом судебных разбирательств между Европейской комиссией и американскими цифровыми компаниями, а также причиной огромных штрафов. В целом используется широкий набор мер и инструментов, направленных на защиту собственного цифрового суверенитета, иногда даже в ущерб глобальной конкурентоспособности. Таким образом, на Западе под цифровым суверенитетом понимают государственный контроль над инфраструктурой, программным обеспечением и данными.

В Китае на смену Великой китайской стены пришел Великий китайский файрвол (The Great Firewall of China). Одна из особенностей китайского файрвола – специальное программное обеспечение, закрывающее проникновение западных сервисов и заменяющее их местными аналогами. Другая особенность – создание аналогов западных платформ и мессенджеров. Так, китайцы переписываются в WeChat вместо Telegram, ищут информацию в Baidu, а не в Google, заказывают товары на Taobao, а не на Amazon. Страна активно развивается, у нее есть выбор всех западных программ, платформ и технологий, но на собственном технологическом базисе, с закрытием внешнего контура.

В России и Китае большое значение уделяется контролю над трансграничным контентом [1, 5]. То есть на первый план выходит концепция информационного суверенитета. Национальное законодательство страны создает правовую базу для централизованного управления интернетом в государственных границах. Большое внимание Россия уделяет строительству собственной инфраструктуры и созданию национальных программных продуктов и решений.

Беларусь также активно развивается в поиске своего места и возможностей в цифровом мире. Согласно Концепции обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года, под суверенитетом в сфере цифрового развития понимается «неотъемлемое право государства управлять государственной информационно-коммуникационной инфраструктурой и информационными ресурсами, осуществлять над ними контроль, защищать свои интересы и проводить независимую внешнюю и внутреннюю государственную политику в сфере цифрового развития» [9]. В то же время Концепция не дает четкого и исчерпывающего определения цифрового суверенитета. Согласно Концепции, «суверенитет в сфере цифрового развития является частью обеспечения информационной безопасности Республики Беларусь». В числе приоритетов проекта стратегии – формирование в стране экономики данных, разработка цифровых сервисов, стимулирование разработки и перехода на собственные программные продукты и информационные технологии. Правительству и бизнесу предстоит большая работа по наполнению их конкретными проектами и программами.

Внутренние и внешние факторы, определяющие цифровой суверенитет

Цифровой суверенитет – это не статичное состояние, а динамический результат непрерывного взаимодействия различных факторов, определяющих амбиции и возможности страны. На уровень стратегической автономии в эпоху цифровых технологий оказывает влияние тонкий баланс между национальной безопасностью, экономической стабильностью и сохранением культурно-политической идентичности в условиях, когда большая часть жизни переместилась в онлайн, управляемый извне. Можно сказать, что цифровой суверенитет в глобальном мире – это возможность проводить сбалансированную экономическую политику, используя глобальные технологии и одновременно инвестируя в собственные технологии и образование, создавая гибкое законодательство и противодействуя внешним вызовам.

Факторы, влияющие на цифровой суверенитет, носят комплексный характер и охватывают технологическую, экономическую, правовую и геополитическую сферы. Их можно разделить на внутренние (зависящие от действий самого государства, на которые оно может влиять) и внешние (объективные вызовы и угрозы).

Внутренние факторы:

– технологические и инфраструктурные: уровень развития собственной IT-отрасли, состояние критической информационной инфраструктуры (КИИ – устойчивость сетей, энергосистем, финансового и банковского секторов к кибератакам и внешним воздействиям, зависимость от иностранного программного обеспечения и технологий, наличие и качество телекоммуникационных сетей);

– экономические (ВВП, объем инвестиций в НИОКР, конкурентоспособность IT-отрасли, доля электронного бизнеса и IT-технологий в ВВП);

– правовые и регуляторные: наличие и качество законодательства (законы о защите персональных данных, КИИ, о суверенном интернете, регулировании техкорпораций), качество и эффективность управления государства в цифровой среде (электронное правительство), борьба с киберпреступностью;

– кадровые и образовательные (качество и количество IT-специалистов, уровень цифровой грамотности населения, состояние системы образования);

– социокультурные (уровень доверия к государству в цифровой сфере, культурная, ментальная и языковая специфика, ценности).

Внешние факторы в настоящее время становятся главным драйвером фрагментации и суверенизации интернета, прочерчивая виртуальные национальные границы в ранее свободной и открытой сети. Именно они стимулируют государство к созданию замкнутых контролируемых цифровых систем. Среди основных внешних факторов можно отметить:

- геополитическую конкуренцию и санкционное давление;
- деятельность глобальных технологических корпораций (Big Tech);
- развитие ИКТ, под которыми понимаются весь спектр и комплекс объектов, действий и правил, связанных с подготовкой, переработкой, доставкой информации при персональной, массовой и производственной коммуникации, а также все технологии и отрасли, интегрально обеспечивающие перечисленные процессы. Следует подчеркнуть, что эти технологии могут как подрывать цифровой суверенитет (системы слежения, блокировки данных, использование параллельных транзакций и т. п.), так и, наоборот, помогать сохранять и шифровать данные, создавать альтернативные технологические решения и пр.

Таким образом, внешние факторы не просто ослабляют или усиливают цифровой суверенитет, они качественно его меняют. Во-первых, этому способствовали сами IT-гиганты, и в первую очередь – развитие цифровых платформ, которые стали использовать информацию и личные данные пользователей как собственный ресурс для генерации новых услуг и прибыли, тем самым вызывая на себя давление с целью защиты персональных данных. Во-вторых, активное развитие новых информационных технологий и нейросетей приводит к возможности реального вмешательства и манипулирования политическим выбором – от Румынии до Мадагаскара. В-третьих, существующие практики отмены и санкционирования программных продуктов и технологий ставят страны, не владеющие ими, в реально уязвимое положение. В результате происходит системная трансформация подходов к управлению в области цифрового суверенитета. Смещается фокус контроля: вместо контроля над каналами связи (сетями) нужен контроль над данными, алгоритмами и точками их обработки. Становятся важными новые компетенции, которые надо создавать. Государству для эффективного контроля критично важно иметь своих специалистов по искусственному интеллекту и алгоритмам нейросетей, анализу больших данных, криптографии и блокчейну. Все это требует значительных финансовых и человеческих ресурсов и специальной государственной политики.

В то же время в цифровую эпоху невозможно просто «закрыться». Стратегия полной автаркии не только не реалистична, но и контрпродуктивна. Цифровой суверенитет в современном мире – это не столько технологический, сколько управленческий вызов. Соответственно, каждой стране нужно быть гибкой и адаптивной, находить тонкий баланс между импортозамещением и использованием современных технологий, между запретами и экономической эффективностью, гибкостью, стимулированием, а не принуждением. Необходимо найти свое место в глобальной конкурентоспособности, обеспечивая суверенитет лишь в критически важных сегментах (КИИ, оборона, госуправление и т. п).

Заключение

1. Систематизированы и проанализированы различные концепции, лежащие в основе цифрового суверенитета, такие как суверенитет данных, информационный и технологический суверенитет. Рассмотрена их взаимная обусловленность и связанность. Выполнен анализ внутренних и внешних факторов, определяющих возможности и границы цифрового суверенитета каждой страны. Именно внешние факторы выступают основным драйвером фрагментации интернета во многих странах, не являющихся технологическими лидерами в IT-отрасли. В то же время государствам необходимо сосредоточить основные усилия на развитии внутренних факторов.

2. В настоящее время большинство регуляционных мер, обеспечивающих реализацию информационного или цифрового суверенитета, так или иначе касаются правовых и технологических рамок. Сюда относятся меры, обеспечивающие безопасность цифровой среды, а также меры запретов и контроля. Однако все они требуют колоссальных ресурсов и имеют отложенный эффект. Изменение подхода и смещение фокуса с регуляторных и контролирующих мер, которые могут только задавать направление и рамки, к более мягким образовательным и просветительным мерам и инструментам, создающим кадровый и технологический потенциал, качественный национальный контент, устойчивую культурную среду и медиаграммотность, позволят существенно укрепить как цифровой, так и общенациональный суверенитет.

Список литературы

1. Шитьков, С. В. Подходы к изучению цифрового суверенитета в современной политической науке / С. В. Шитьков // Международная жизнь. 2025. № 5. С. 90–100.
2. Антонов, Д. Е. Цифровой суверенитет современного государства: от контроля до коммуникации / Д. Е. Антонов // Полилог. 2022. Т. 6, № 2. С. 1–14.
3. Бухарин, В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности / В. В. Бухарин // Вестник МГИМО-Университета. 2016. Т. 6, № 51. С. 76–91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91.
4. Володенков, С. В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности / С. В. Володенков // Журнал политических исследований. 2020. Т. 4, № 4. С. 3–11. DOI: 10.12737/2587-6295-2020-3-11.
5. Зиновьева, Е. С. Цифровой суверенитет в публикации о международных отношениях / Е. С. Зиновьева, С. В. Шитьков // Международная жизнь. 2023. № 3. С. 38–51.
6. Кутюр, С. Что означает понятие «суверенитет» в цифровом мире? / С. Кутюр, С. Тоупин // Журнал исследований международных организаций. 2020. Т. 15, № 4. С. 48–69.
7. Шахновская, И. В. Информационный суверенитет государства и личности: опыт Республики Беларусь и зарубежных стран / И. В. Шахновская // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24, № 2. С. 117–123.
8. Creemers, R. China's Conception of Cyber Sovereignty: Rhetoric and Realization / R. Creemers // Governing Cyberspace. 2020. P. 107–142.
9. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. Режим доступа: https://pravo.by/document/?guid=12551&p0=C22401074. Дата доступа: 10.11.2025.

Поступила 22.12.2025 Принята в печать 22.01.2026 Доступна на сайте 10.04.2026

References

1. Shitkov S. V. (2025) Approaches to the Study of Digital Sovereignty in Modern Political Science. *The International Affairs*. (5), 90–100.
2. Antonov D. E. (2022) Digital Sovereignty of the Modern State: From Control to Communication. *Polylogos.* 6 (2), 1–14.
3. Bukharin V. V. (2016) The Russian's Digital Sovereignty as a Technical Basis of Information Security. *MGIMO Review of International Relations*. 6 (51), 76–91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91.
4. Volodenkov S. V. (2020) The Phenomenon of Contemporary State's Digital Sovereignty in the Context of Global Technological Transformations: Content and Features. *Journal of Political Research*. 4 (4), 3–11. DOI: 10.12737/2587-6295-2020-3-11.
5. Zinovieva E. S., Shitkov S. V. (2023) Digital Sovereignty in International Relations. *The International Affairs*. (3), 38–51.

6. Couture S., Toupin S. (2020) What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *International Organizations Research Journal*. 15 (4), 48–69.
7. Shakhnovskaya I. V. (2024) Information Sovereignty of the State and Individuals: The Experience of the Republic of Belarus and Foreign Countries. *Bulletin of the South Ural State University. Series "Law"*. 24 (2), 117–123.
8. Creemers R. (2020) China's Conception of Cyber Sovereignty: Rhetoric and Realization. *Governing Cyberspace*. 107–142.
9. *National Legal Internet Portal of the Republic of Belarus*. Available: https://pravo.by/document/?guid=12551&p0=C22401074 (Accessed 10 November 2025).

Received: 22 December 2025 Accepted: 22 January 2026 Available on the website: 10 April 2026

Сведения об авторе

Ракова Е. Ю., канд. экон. наук, доц. каф. коммерческой деятельности и управления недвижимостью, Белорусский государственный экономический университет

Адрес для корреспонденции

220038, Республика Беларусь,
Минск, ул. Свердлова, 7
Белорусский государственный
экономический университет
Тел.: 375 29 659-10-02
E-mail: rakova2025@gmail.com
Ракова Елена Юрьевна

Information about the author

Rakova E., Cand. Sci. (Econ.), Associate Professor at the Department of Commercial Activity and Real Estate Management, Belarus State Economic University

Address for correspondence

220038, Republic of Belarus,
Minsk, Sverdlova St., 7
Belarus State
Economic University
Tel.: 375 29 659-10-02
E-mail: rakova2025@gmail.com
Rakova Elena

http://dx.doi.org/10.35596/1729-7648-2026-32-1-12-18

УДК 339.138:004.738.5

КЛЮЧЕВЫЕ ФАКТОРЫ АЛГОРИТМОВ СОЦИАЛЬНЫХ СЕТЕЙ: КЛАССИФИКАЦИЯ И ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ ДЛЯ SMM

М. П. БАТУРА, И. В. МАРАХИНА, В. А. ПАРХИМЕНКО

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. В социальных сетях алгоритмические системы определяют, увидят ли пользователи тот или иной контент, что требует от маркетологов выявления и анализа ключевых параметров, определяющих логику работы таких алгоритмов. В статье представлены систематизация и комплексный анализ ключевых факторов, которые алгоритмы социальных сетей учитывают при отборе, ранжировании и демонстрации текстовых, фото- и видеоматериалов. На их основе сформированы обоснованные рекомендации по оптимизации стратегий маркетинга в социальных сетях. В результате анализа выделены такие ключевые факторы, как уровень вовлеченности потребителя контента, предпочтения пользователей, соответствие контента приоритетам платформы (социальной сети), новизна контента, предыдущий успех (положительный опыт) публикаций, длительность просмотра. Предложены методические рекомендации по продвижению компании в социальных сетях с учетом каждого фактора.

Ключевые слова: алгоритмы социальных сетей, факторы ранжирования, вовлеченность, SMM, видимость контента, персонализация, публикация, классификация.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Батура, М. П. Ключевые факторы алгоритмов социальных сетей: классификация и практическая значимость для SMM / М. П. Батура, И. В. Марахина, В. А. Пархименко // Цифровая трансформация. 2026. Т. 32, № 1. С. 12–18. http://dx.doi.org/10.35596/1729-7648-2026-32-1-12-18.

KEY FACTORS OF SOCIAL NETWORKS ALGORITHMS: CLASSIFICATION AND PRACTICAL SIGNIFICANCE FOR SMM

MIHAIL BATURA, INA MARAKHINA, ULADZIMIR PARKHIMENKO

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. On social networks, algorithms determine whether users see certain content, requiring marketers to identify and analyze the key parameters that govern the logic of these algorithms. This article presents a systematization and comprehensive analysis of the key factors that social networks algorithms consider when selecting, ranking, and displaying text, photo, and video content. Based on these factors, the recommendations for optimizing social networks marketing strategies have been developed. The analysis identified key factors such as consumer engagement, user preferences, content alignment with platform (social network) priorities, content novelty, previous success (positive experience) of publications, and viewership duration. Methodological recommendations for company promotion on social networks, taking each of these factors into account, are proposed.

Keywords: social networks algorithms, ranking factors, engagement, SMM, content visibility, personalization, publishing, classification.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Batura M., Marakhina I., Parkhimenko U. (2026) Key Factors of Social Networks Algorithms: Classification and Practical Significance for SMM. *Digital Transformation.* 32 (1), 12–18. http://dx.doi.org/10.35596/1729-7648-2026-32-1-12-18 (in Russian).

Введение

Алгоритмические системы ранжирования контента представляют собой центральный элемент архитектуры современных социальных медиа, определяющий видимость, охват и, в конечном счете, эффективность маркетинговых коммуникаций бизнеса. В условиях цифровой трансформации, когда соцсети становятся важным каналом взаимодействия с целевой аудиторией, понимание принципов работы этих алгоритмов необходимо для разработки успешных стратегий маркетинга в социальных сетях (SMM).

Актуальность исследования обусловлена следующим противоречием: с одной стороны, от алгоритмов напрямую зависит коммерческий успех продвижения конкретных товаров, услуг, брендов, компаний, с другой – внутренняя логика алгоритмов, набор конкретных факторов и их весовые коэффициенты остаются «черным ящиком» [1–3] для исследователей и практиков. Такое положение дел, конечно, не должно вызывать удивления, поскольку социальная сеть (как бизнес) не заинтересована в полной прозрачности своих алгоритмов. Особенности алгоритмов – это элемент конкурентоспособности и фактор успешности бизнеса социальной сети, своего рода ноу-хау и, соответственно, коммерческая тайна, тщательно охраняемая как от конкурентов, так и от пользователей. Несмотря на указанное противоречие, анализ официальных публикаций социальных сетей, научных исследований и эмпирических данных все-таки позволяет приоткрыть «черный ящик» и реконструировать ключевые факторы, влияющие на принятие алгоритмических решений.

Теоретическая значимость исследований заключается в структуризации знаний о функционировании «черного ящика» алгоритмов, а практическая – в формировании на этой основе обоснованных методических рекомендаций для оптимизации SMM-деятельности, позволяющих организациям целенаправленно влиять на видимость своего контента в социальной сети для пользователей и вовлеченность потребителей, учитывая «логику» цифровых платформ. Важно подчеркнуть, что критический анализ выявленных факторов работы алгоритмов не отрицает их влияния, а, напротив, раскрывает сущностные особенности. Это позволяет перейти от следования трендам к научному стратегическому управлению цифровым маркетингом. Понимание как возможностей, так и рисков для деятельности компании, заложенных в функционирование алгоритмов, становится основой для построения устойчивой и социально ответственной SMM-стратегии в условиях цифровой трансформации.

Факторы алгоритмов социальных сетей

В рамках исследования факторы алгоритмов социальных сетей определены как формализованные параметры (признаки, сигналы), количественно или качественно характеризующие контентные единицы (посты) и поведенческие реакции пользователей, которые используются алгоритмами социальной сети как входные параметры для проведения отбора и ранжирования публикаций для каждого пользователя. Исследования и официальные публикации соцсетей позволяют выделить следующие основные факторы алгоритмов, а также показатели, которые их характеризуют и которые будут важны для целей исследования, связанных с продвижением в социальных сетях [4, 5].

Уровень вовлеченности потребителя контента. Чем больше пользователей взаимодействует с определенным контентом, тем выше их уровень вовлеченности и тем больше вероятность, что эта публикация будет продвигаться в лентах социальных сетей. При этом может запускаться цикл, в котором популярный контент приобретает еще большую известность [6].

T. Burton [7] так описывает действие этого фактора в Facebook: «Если контент, которым делится ваша бизнес-страница, кажется некачественным и получает мало внимания, он будет сочтен нерелевантным и будет погребен под другими публикациями. Вам будет трудно быть увиденным, пока вы не докажете алгоритму, что ваши публикации заслуживают того, чтобы их видели. Взаимодействие с клиентами – это великая движущая сила большинства алгоритмов – это должно быть вашей целью. Чем больше людей взаимодействуют с вашей публикацией, тем большему количеству людей Facebook ее покажет». В качестве показателей вовлеченности пользователей обычно используются такие, как время пребывания в социальной сети (длительность сессии), клики на гиперссылки, репосты контента, сохранения, лайки и т. д. [8, 9].

Как отмечают некоторые исследователи, можно говорить о том, что социальные сети, реализуя описанные выше подходы, используют «мудрость толпы» [6]. Концепция «мудрости толпы»

предполагает, что использование сигналов от действий, мнений и предпочтений других людей в качестве руководства приведет к обоснованным решениям. Например, коллективные прогнозы обычно точнее индивидуальных. Коллективный интеллект используется для прогнозирования финансовых рынков, спорта, выборов и даже вспышек заболеваний [6].

Однако при этом отмечаются и недостатки реализации такого подхода в социальных сетях. Например, делаются предположения, что оптимизация для популярности не всегда обеспечивает качество предоставляемого пользователю контента [6, 10, 11]. Исследователи обнаружили, что пользователи чаще ставят отметки «Нравится» или делятся статьями из источников с низкой надежностью и качеством, когда видят, что многие другие пользователи взаимодействовали с этими статьями. Таким образом, ориентация на показатели вовлеченности в первую очередь приводит к продвижению контента, который соответствует субъективным социальным, аффективным и когнитивным предпочтениям и предубеждениям человека, а не объективно качественному контенту [12]. Метрики популярности (вовлеченности) также могут быть сфальсифицированы, например, с помощью ботов, фейковых аккаунтов, организованных троллей и сети фейковых аккаунтов.

Уровень вовлеченности, как отмечалось выше, измеряется через реакции на публикации, например, для видеороликов это лайки, репосты и пересылки, комментарии, а также длительность просмотра. Кроме таких частных показателей, активно используются обобщающие: комплексный показатель вовлеченности (Engagement Rate, ER, %), показатель удержания внимания (Engagement Persistence, EP), показатели конверсии (Click-Through Rate, CTR):

$$ER = \frac{\sum L + \sum S + \sum C + \sum R}{N} 100\ \%; \quad (1)$$

$$ER = \frac{\sum L + \sum S + \sum C + \sum R}{\sum P} 100\ \%; \quad (2)$$

$$EP = \frac{N_c}{N_s} 100\ \%; \quad (3)$$

$$CRT = \frac{V}{I} 100\ \%, \quad (4)$$

где ΣL, ΣS, ΣC, ΣR – суммарное количество лайков, сохранений, комментариев и репостов соответственно; N – общее число подписчиков аккаунта; ΣP – суммарное количество просмотров; N_c – суммарное количество пользователей, завершивших просмотр контента (просмотревших видео/пост до конца или до значимой точки завершения); N_s – общее количество пользователей, начавших просмотр; V – количество просмотров контента (например, запуск и просмотр видеоролика); I – общее количество показов контента.

Следует отметить, что в зависимости от социальной сети показатели в числителе в формулах (1) или (2) могут меняться.

С точки зрения эффективности работы соцсетей высокий уровень вовлеченности обеспечивают рост времени, которое пользователи проводят на платформе, рост лояльности и вовлечение новых пользователей через приглашения или пересылки во внешние ресурсы. Так, комментарии для платформы – это дополнительное время, которое пользователь проведет в социальной сети, когда пишет свои или читает чужие комментарии. Кроме того, это может увеличить и частоту посещений, так как социальная сеть информирует об ответе на комментарий и стимулирует пользователя зайти вновь. Для пользователя же комментарии – это частичная возможность переноса общения в виртуальное пространство. Также комментарии – это часто интересный для целевой аудитории контент, который могут читать дольше, чем просматривать пост, под которым находятся комментарии. Репосты тоже очень важны для социальной сети. Они позволяют не только активизировать аудиторию, увеличивать число просмотров постов, но и привлекать новых пользователей.

Предпочтения пользователей. Алгоритмы социальных сетей, как полагают исследователи, в качестве входных данных используют, помимо прочего, предпочтения – то, что нравится пользователю, что он просматривает, читает, в том числе и то, во что он вовлечен. То есть – что он комментирует и чем делится. Другими словами, – это контент, который пользователю интересен [6]. Такие предпочтения могут быть:

– реальными – совокупность информации, подтвержденная действиями пользователя, которые свидетельствуют о его интересе в определенном контенте;

– ожидаемыми – прогнозируемые на основе модели предпочтения, например, исходя из интересов и предпочтений, выявленных у других пользователей из того же кластера.

В то же время необходимо отметить, что ориентация исключительно на предпочтения пользователя может приводить к появлению эхо-камер и поляризации пользователей.

Соответствие контента приоритетам платформы. Ряд авторов указывают на то, что отдельные платформы (социальные сети) изначально отдают предпочтение определенному контенту (как по форме, так и по содержанию). Так, в [5] приведены примеры того, как различные платформы соцсетей относятся к контенту: «Facebook продвигает живое видео, Instagram отдает предпочтение изображениям и видео, LinkedIn отдает приоритет публикациям с лидерскими идеями…». Следует отметить, что это обосновывается позиционированием социальных сетей относительно своих конкурентов. В то же время нужно осторожно относиться к таким рекомендациям, которые зачастую не имеют научного обоснования и эмпирически сложно проверяемые (Как, например, объективно оценить, насколько лидерской идеей обладает конкретная публикация?)

Новизна контента. Как отмечает S. Graffius [5], «социальные сети процветают за счет оперативности. Новый контент часто имеет приоритет над старыми постами. Это заставляет бренды, влиятельных лиц (инфлюэнсеров) и других поддерживать подходящий график размещения публикаций (постинга)». При этом следует отметь, что, скорее всего, максимальный охват получат те новые посты, которые согласуются с позицией алгоритмов о популярных трендах. Такой подход несет ряд рисков, именно поэтому значительная часть компаний предпочитает стратегию «следования за лидером». В этом случае создаются публикации на очень схожие темы или даже с одинаковым сюжетом, музыкой, текстами, которые уже проявили свой вирусный потенциал.

Предыдущий успех (положительный опыт) публикаций. Можно ожидать от социальных сетей создания рейтинга каждого автора и ожидаемой успешности его поста исходя из предыдущего опыта. Например, в LinkedIn существует показатель Social Selling Index, характеризующий рейтинг каждого пользователя. При этом социальная сеть не дает пояснений, на что данный рейтинг влияет. Поэтому механизм работы и воздействия данного показателя имеет предполагаемый характер.

В то же время значимость числа подписчиков, как подтверждения предыдущего успеха, является очевидной. Зачастую алгоритмы в первую очередь показывают посты, на авторов которых подписано больше пользователей. И при значительном числе подписчиков даже «невирусные» посты увидит большое число людей, а учитывая лояльность подписчиков, число реакций также будет значительным. Следует отметить, что наличие большого числа подписчиков является дополнительным стимулом подписаться, влияющим на остальных пользователей, которые хотят примкнуть и которые прислушиваются к «коллективному опыту». Одновременно значительное число подписчиков может приводить ко все более консервативному выбору тем, так как автор с осторожностью и избирательностью будет относиться к новым темам, чтобы не лишиться поддержки. В некоторых социальных сетях, кроме числа подписчиков в профиле авторов, можно увидеть и значение совокупного числа реакций, что может воздействовать на результаты работы алгоритмов схожим с числом подписчиков образом.

Длительность просмотра. Данный фактор упоминался при описании показателя вовлеченности пользователя, однако для видеоматериалов он может рассматриваться и отдельно, самостоятельным образом. Для социальных сетей длительные просмотры будут приносить больше возможностей для монетизации. Так, YouTube встраивает рекламу в середину видео только при превышении определенной длительности. В то же время короткие видео могут быть более разнообразными и захватывающими, что труднее достигнуть в длинном видео.

Как указывает T. Burton [7], «Facebook вознаграждает вас видимостью [контента для пользователя], если вы можете управлять обсуждением и удерживать внимание зрителей. Один из способов сделать это – использовать длинный видеоконтент, который является «родным» для Facebook (другими словами, напрямую загруженный, а не распространенный с другого сайта). Цель любого сайта социальных сетей – удержать вас на своей платформе».

Прочие факторы. Следует выделить, например, такой фактор, как активность реакции в первые часы просмотра, который связан с оптимальным временем публикации при наличии определенной целевой аудитории. Время публикации в этом случае должно опережать на небольшой промежуток время максимальной активности целевой аудитории или совпадать с временем ее входа в социальную сеть.

Проведенный анализ факторов работы алгоритмов определяет возможность для формирования универсальных рекомендаций по продвижению компании в социальных сетях (рис. 1). Таким образом, не имея возможности влиять напрямую на алгоритмы, можно влиять на факторы или входные параметры, что позволяет усовершенствовать работу в соцсетях и является основой для формирования и развития SMM-стратегии и мероприятий.

Рис. 1. Универсальные методические рекомендации по оптимизации SMM на основе факторов алгоритмов социальных сетей (*источник – собственная разработка*)
Fig. 1. Universal guidelines for SMM optimization based on social networks algorithm factors (*source – proprietary development*)

Разработанные на основе анализа рекомендации (рис. 1) трансформируют критическое понимание факторов в конкретный практический инструментарий, позволяющий бизнесу системно «настраивать» коммуникации, превращая алгоритм из барьера в управляемый ресурс. Реализация методических рекомендаций включает:

– управление вовлеченностью на основе активного привлечения «доноров вовлеченности» (лидеров мнений, экспертов, лояльных клиентов и т. д.) для запуска первоначальных алгоритмических сигналов и целевое стимулирование качественных поведенческих реакций (комментариев, сохранений, репостов и т. д.), смещая фокус с пассивных лайков на глубокое взаимодействие;

– персонализацию и аналитику, реализуемые через глубокий анализ реальных и ожидаемых предпочтений аудитории, непрерывное отслеживание метрик и адаптацию SMM-стратегии, что создает цикл обратной связи для постоянной оптимизации;

– адаптацию к формальным требованиям платформы, включающую учет приоритетных форматов контента для соответствия текущим подходам к его ранжированию;

– балансировку инноваций и минимизацию рисков, достигаемых путем сочетания стратегии «следования за лидером» на проверенном контенте, развития микровирусности, управления рисками;

– наращивание органической аудитории за счет последовательного укрепления лояльности для повышения доверия и готовности аудитории к взаимодействию, формирование предсказуемого, позитивного пользовательского опыта и минимизация негативных реакций;

– обеспечение роста длительности просмотров и удержания пользователей за счет перманентного анализа коэффициентов удержания и экономики контента и внедрения целевых стратегий, стимулирующих длительное взаимодействие и создающих для алгоритма сигналы о высокой ценности и качестве материала;

– ускорение первоначальной реакции на контент, повышение активности пользователей в первые часы благодаря определению оптимального времени публикации для целевой аудитории.

Этот комплекс мер позволяет бизнесу не просто реагировать на алгоритмы, а воздействовать на них, где каждое действие – публикация, реакция, анализ – становится управляемым входным сигналом. Тем самым алгоритмическая система превращается из непрозрачного «черного ящика» в более предсказуемый и настраиваемый механизм повышения видимости и достижения маркетинговых целей в условиях цифровой трансформации.

Заключение

1. Анализ литературных источников позволяет констатировать, что алгоритмические системы ранжирования контента являются центральным элементом, опосредующим взаимодействие бизнеса и потребителей в социальных сетях. Работа таких алгоритмов, несмотря на внешнюю непрозрачность, при системном подходе все-таки поддается реконструкции и анализу на основе изучения официальных данных платформ, научных публикаций и эмпирических наблюдений.

2. Теоретическая значимость исследования заключается в структуризации знаний о работе алгоритмических систем и формализации набора ключевых факторов, что вносит вклад в развитие теории цифрового маркетинга. Практическая значимость и ценность исследования состоит в разработке универсальных методических рекомендаций для SMM-специалистов и маркетологов, в критическом осмыслении факторов алгоритмов социальных сетей.

3. Перспективы дальнейших исследований – в количественной верификации весовых коэффициентов выделенных факторов для различных платформ и тематических ниш, а также в изучении динамики изменения их значимости под влиянием обновлений алгоритмов и трансформации медиапотребления в обществе.

Список литературы

1. Gagrcin, E. Algorithmic Media Use and Algorithm Literacy: An Integrative Literature Review / E. Gagrcin, T. K. Naab, M. F. Grub // New Media & Society. 2024. DOI: 10.1177/14614448241291137.
2. Pasquale, F. The Black Box Society: The Secret Algorithms That Control Money and Information / F. Pasquale // Harvard University Press. 2015.
3. Kossow, N. Algorithmic Transparency and Accountability [Electronic resource] / N. Kossow, S. Windwehr, M. Jenkins // Transparency International. 2021. Mode of access: https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf. Date of access: 19.08.2025.
4. Никитин, А. Ю. Алгоритмы социальных сетей: вызовы и возможности для современного маркетолога / А. Ю. Никитин // Научный результат. Технологии бизнеса и сервиса. 2025. Т. 11, № 1. С. 123–138. DOI: 10.18413/2408-9346-2025-11-1-123–138.
5. Graffius, S. How Algorithms Shape the User Experience on Social Media Platforms [Electronic resource] / S. Graffius. Mode of access: https://scottgraffius.com/blog/files/tag-how-algorithms-shape-the-user-experience-on-social-media-platforms.html. Date of access: 19.08.2025. DOI: 10.13140/RG.2.2.29149.01767.
6. Menczer, F. Facebook Whistleblower Frances Haugen Testified That the Company's Algorithms Are Dangerous – Here's How They Can Manipulate You [Electronic resource] / F. Menczer // The Conversation. 2021. Mode of access: https://theconversation.com/facebook-whistleblower-frances-haugen-testified-that-the-companys-algorithms-are-dangerous-heres-how-they-can-manipulate-you-169420. Date of access: 11.09.2025.
7. Burton, T. Marketing: Is Facebook a Fit? [Electronic resource] / T. Burton // PBI. 2022. Mode of access: https://www.pbi.org/blog/social-media-marketing-is-facebook-a-fit/. Date of access: 19.08.2025.
8. Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media / S. Milli [et al.] // PNAS Nexus. 2025. Vol. 4, Iss. 3. DOI: 10.1093/pnasnexus/pgaf062.
9. Guide to Beating Social Media Algorithms [Electronic resource]. Mode of access: https://www.adobe.com/learn/express/web/increase-social-media-visibility. Date of access: 20.08.2025.
10. Metzler, H. Social Drivers and Algorithmic Mechanisms on Digital Media / H. Metzler, D. Garcia // Perspectives on Psychological Science. 2023. Vol. 19, No 5. P. 735–748.
11. How Algorithmic Popularity Bias Hinders or Promotes Quality / G. L. Ciampaglia [et al.] // Scientific Reports. 2018. Vol. 8, Iss. 1. DOI: 10.1038/s41598-018-34203-2.
12. Menczer, F. How "Engagement" Makes You Vulnerable to Manipulation and Misinformation on Social Media [Electronic resource] / F. Menczer // The Conversation. 2021. Mode of access: https://theconversation.com/how-engagement-makes-you-vulnerable-to-manipulation-and-misinformation-on-social-media-145375. Date of access: 11.09.2025.

Поступила 10.11.2025 Принята в печать 26.01.2026 Доступна на сайте 10.04.2026

References

1. Gagrcin E., Naab T. K., Grub M. F. (2024) Algorithmic Media Use and Algorithm Literacy: An Integrative Literature Review. *New Media & Society.* DOI: 10.1177/14614448241291137.
2. Pasquale F. (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. *Harvard University Press*.
3. Kossow N., Windwehr S., Jenkins M. (2021) Algorithmic Transparency and Accountability. *Transparency International.* Available: https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf (Accessed 19 August 2025).
4. Nikitin A. Y. (2025) Social Media Algorithms: Challenges and Opportunities for the Modern Marketer. *Scientific Result*. *Business and Service Technologies.* 11 (1), 123–138. DOI: 10.18413/2408-9346-2025-11-1-123–138 (in Russian).
5. Graffius S. (2024) *How Algorithms Shape the User Experience on Social Media Platforms.* Available: https://scottgraffius.com/blog/files/tag-how-algorithms-shape-the-user-experience-on-social-media-platforms.html (Accessed 19 August 2025). DOI: 10.13140/RG.2.2.29149.01767.
6. Menczer F. (2021) Facebook Whistleblower Frances Haugen Testified That the Company's Algorithms Are Dangerous – Here's How They Can Manipulate You. *The Conversation.* Available: https://theconversation.com/facebook-whistleblower-frances-haugen-testified-that-the-companys-algorithms-are-dangerous-heres-how-they-can-manipulate-you-169420 (Accessed 11 September 2025).
7. Burton T. (2022) Marketing: Is Facebook a Fit? *PBI.* Available: https://www.pbi.org/blog/social-media-marketing-is-facebook-a-fit/ (Accessed 19 August 2025).
8. Milli S., Carroll M., Wang Y., Pandey S., Zhao S., Dragan A. D. (2025) Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media. *PNAS Nexus.* 4 (3). DOI: 10.1093/pnasnexus/pgaf062.
9. *Guide to Beating Social Media Algorithms*. Available: https://www.adobe.com/learn/express/web/increase-social-media-visibility (Accessed 20 August 2025).
10. Metzler H., Garcia D. (2023) Social Drivers and Algorithmic Mechanisms on Digital Media. *Perspectives on Psychological Science.* 19 (5), 735–748.
11. Ciampaglia G. L., Nematzadeh A., Menczer F., Flammini A. (2018) How Algorithmic Popularity Bias Hinders or Promotes Quality. *Scientific Reports.* 8 (1). DOI: 10.1038/s41598-018-34203-2.
12. Menczer F. (2021) How "Engagement" Makes You Vulnerable to Manipulation and Misinformation on Social Media. *The Conversation.* Available: https://theconversation.com/how-engagement-makes-you-vulnerable-to-manipulation-and-misinformation-on-social-media-145375 (Accessed 11 September 2025).

Received: 10 November 2025 Accepted: 26 January 2026 Available on the website: 10 April 2026

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Батура М. П., д-р техн. наук, проф., зав. науч.-исслед. лаб. «Новые обучающие технологии», Белорусский государственный университет информатики и радиоэлектроники (БГУИР)

Марахина И. В., канд. экон. наук, доц., доц. каф. экономики, БГУИР

Пархименко В. А., канд. экон. наук, доц., зав. каф. экономики, БГУИР

Information about the authors

Batura M., Dr. Sci. (Tech.), Professor, Head of the R&D Lab "New Educational Technologies", Belarusian State University of Informatics and Radioelectronics (BSUIR)

Marakhina I., Cand. Sci. (Econ.), Associate Professor, Associate Professor at the Economics Department, BSUIR

Parkhimenko U., Cand. Sci. (Econ.), Associate Professor, Head of the Economics Department, BSUIR

Адрес для корреспонденции

220005, Республика Беларусь,
Минск, ул. Платонова, 39–809
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 29 380-59-99
E-mail: marahina@bsuir.by
Марахина Инна Викторовна

Address for correspondence

220005, Republic of Belarus,
Minsk, Platonova St., 39–809
Belarusian University
of Informatics and Radioelectronics
Tel.: +375 29 380-59-99
E-mail: inamarahina@gmail.com
Marakhina Ina

http://dx.doi.org/10.35596/1729-7648-2026-32-1-19-25

УДК 331.5:378:004.9

РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ПОДГОТОВКОЙ КОНКУРЕНТОСПОСОБНЫХ КАДРОВ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ НА ОСНОВЕ ИНТЕГРАЦИИ ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ И РЫНКА ТРУДА

Д. В. БАРАНКОВ

Московский финансово-промышленный университет «Синергия» (Москва, Российская Федерация)

Аннотация. Рассмотрено формирование комплексной модели управления подготовкой конкурентоспособных специалистов в условиях цифровой экономики с опорой на интеграцию образовательной системы и рынка труда. Актуальность исследования обусловлена недостаточной согласованностью обучения и запросов работодателей, что снижает эффективность кадровой политики. Разработана интегративно-адаптивная схема, объединяющая требования цифрового сектора, сетевые формы сотрудничества, цифровые инструменты и систему объективных показателей результативности. Представлены структурные элементы модели, механизмы координации организаций образования и предприятий, инструменты мониторинга карьерных траекторий и способы формирования индивидуальных образовательных маршрутов. Особое внимание уделено цифровым платформам и показателям эффективности, позволяющим уточнять программу подготовки на основе реальных данных. Методологическая основа исследования включала теоретический анализ, сопоставление практик и изучение современных публикаций.

Ключевые слова: цифровая экономика, управление, образование, предпринимательство, конкурентность, профессиональные компетенции, подготовка кадров, интеграция образования и рынка труда, модель управления, сетевое взаимодействие, цифровые платформы.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Баранков, Д. В. Разработка модели управления подготовкой конкурентоспособных кадров в условиях цифровой экономики на основе интеграции образовательных систем и рынка труда / Д. В. Баранков // Цифровая трансформация. 2026. Т. 32, № 1. С. 19–25. http://dx.doi.org/10.35596/1729-7648-2026-32-1-19-25.

DEVELOPING A MANAGEMENT MODEL FOR TRAINING COMPETITIVE PERSONNEL IN THE DIGITAL ECONOMY BASED ON THE INTEGRATION OF EDUCATIONAL SYSTEMS AND THE LABOR MARKET

DMITRY BARANKOV

Moscow Financial and Industrial University "Synergy" (Moscow, Russian Federation)

Abstract. This article examines the development of a comprehensive management model for training competitive specialists in the digital economy, based on the integration of the education system and the labor market. The relevance of the study stems from the insufficient alignment of training and employer demands, which reduces the effectiveness of HR policies. An integrative and adaptive framework has been developed that combines the requirements of the digital sector, networked forms of collaboration, digital tools, and a system of objective performance indicators. The article presents the structural elements of the model, mechanisms for coordinating educational organizations and enterprises, tools for monitoring career trajectories, and methods for creating individual educational paths. Particular attention is paid to digital platforms and performance indicators, which allow for the refinement of the training program based on real data. The methodological basis of the study included theoretical analysis, a comparison of practices, and a study of modern publications.

Keywords: digital economy, management, education, entrepreneurship, competitiveness, professional competencies, personnel training, integration of education and the labor market, management model, networking, digital platforms.

Conflict of interests. The author declares that there is no conflict of interest.

For citation. Barankov D. (2026) Developing a Management Model for Training Competitive Personnel in the Digital Economy Based on the Integration of Educational Systems and the Labor Market. *Digital Transformation.* 32 (1), 19–25. http://dx.doi.org/10.35596/1729-7648-2026-32-1-19-25 (in Russian).

Введение

В современных условиях цифровой экономики подготовка кадров с соответствующими компетенциями выходит на первый план, поскольку быстрые технологические изменения коренным образом трансформируют рынок труда. Цифровизация и развитие технологий «Индустрии 4.0» меняют требования к работникам и предъявляют новые запросы к образовательным системам. При этом в ряде исследований отмечается существенный разрыв между тем, что дают выпускники образовательных учреждений, и тем, что требуется работодателям: существует разрыв между рынком высшего образования и рынком труда [1, 2]. Возникает научная проблема несоответствия существующих моделей подготовки кадров динамичным требованиям цифровой экономики, что выражается в отсутствии устойчивого механизма согласования компетентностных требований и образовательных практик. Недостаточно быстрое обновление образовательных программ и невысокая оперативность коммуникации университетов с предприятиями замедляют достижение целей экономического роста и снижают эффективность инвестиций в человеческий капитал. В связи с этим возникает необходимость разработки интегрированной модели управления подготовкой конкурентоспособных кадров, которая бы объединяла образовательную систему и потребности рынка труда.

Цель исследования заключалась в разработке и научном обосновании практико-ориентированной модели управления подготовкой высококвалифицированных кадров в условиях цифровой экономики на основе интеграции образовательных систем и рынка труда. Для достижения этой цели были поставлены задачи:

– проанализировать актуальные требования цифровой экономики к профессиональным компетенциям;

– выявить ключевые механизмы взаимодействия учреждений образования и работодателей;

– разработать структурную схему модели обучения;

– оценить основные показатели ее эффективности.

Гипотеза исследования заключалась в том, что согласованная система взаимодействия образования и рынка труда, дополненная цифровыми инструментами мониторинга и обратной связью, обеспечивает повышение результативности подготовки кадров и уменьшает разрыв между квалификацией выпускников и требованиями работодателей. Объектом исследования являлся процесс подготовки высококвалифицированных кадров в национальной экономике, а предметом – организационно-экономические отношения и механизмы управления взаимодействием между образовательными организациями и субъектами рынка труда в условиях цифровой трансформации.

Изученность проблемы отражена в работах, посвященных требованиям цифровой экономики к компетенциям, анализу индустриально-образовательных связей и моделям интеграции обучения и труда. Исследования показывают наличие развитых подходов к описанию компетенций, но отсутствует системная схема, объединяющая цифровые инструменты, сетевые механизмы партнерства и оценочные показатели в единую управленческую модель. Это определяет необходимость дальнейшего теоретического уточнения структуры такого решения. В данной статье использованы методы теоретического анализа и синтеза, системного и сравнительного подходов, а также обзор существующих практик интеграции образования и рынка труда. Так, представленные положительные тезисы были проверены с помощью комплексного обзора литературы, критического анализа документов и сравнительного анализа зарубежного опыта [3]. На основе этих методов сформирована логическая модель, включающая ключевые блоки взаимодействия между субъектами образовательного процесса и рынка труда.

Методика исследования

Исследование строилось на междисциплинарном подходе. Проведен анализ современных исследований и статистических данных о требованиях цифровой экономики к навыкам персонала и о состоянии системы образования, включая отчеты международных организаций. С помощью системного анализа выделены основные компоненты будущей модели. Применялся сравнительный анализ существующих инициатив интеграции образования и бизнеса (в том числе концепций тройной и четверной спирали инноваций), что позволило выявить передовой опыт и проблемы взаимодействия [1, 4].

В рамках методики использовались также экспертные оценки и качественный анализ документов (образовательных стандартов, стратегий развития отрасли цифровых технологий и др.) с целью обоснования блоков модели. В итоге предлагаемая модель была построена итеративно: сначала были сформулированы ее структура и компоненты, затем она проверялась на соответствие реальным вызовам и обзору литературы и, при необходимости, уточнялась.

Результаты исследований и их обсуждение

В результате анализа сформирована интегративно-адаптивная модель управления подготовкой кадров, состоящая из четырех взаимосвязанных блоков: целевого, организационно-функционального, инструментально-технологического и оценочного. Каждый блок решает определенный тип задач и основан на современных научных и практических подходах.

Целевой блок. Включает систему актуальных и перспективных компетенций, востребованных в цифровой экономике. В нее входят как базовые цифровые навыки (цифровая грамотность, работа с данными), так и soft skills (критическое мышление, коммуникация, способность к решению проблем) и узкоспециальные профессиональные знания. Так, исследования показывают, что работодатели в цифровой экономике особенно ценят навыки информационной и цифровой грамотности, умение решать сложные задачи и создавать цифровой контент [5]. В то же время отмечается, что значимые пробелы существуют именно в «мягких» и кросс-секторальных компетенциях – например, в умении эффективно коммуницировать и работать в команде. В модели это отражается в целевой установке на формирование и постоянное обновление реестра необходимых компетенций: используются анализ данных рынка труда (например, контент-анализ вакансий) и прогнозирование будущих требований [3]. Учебные программы строятся таким образом, чтобы обучающиеся поэтапно приобретали цифровые, софт-навыки и профессиональные умения, отвечающие запросам цифрового сектора экономики.

Организационно-функциональный блок. Обеспечивает сетевое взаимодействие участников образовательного процесса и рынка труда (школа–колледж–вуз–бизнес–государство). Этот механизм основан на концепции многостороннего партнерства. В [4] подчеркивается, что эффективная интеграция промышленности и образования требует многосторонних связей и совместных платформ. В модели предусматривается создание координационных структур (консультативные советы, союзы университетов с индустрией, центры компетенций), в которые входят представители власти, учебных заведений и бизнеса. При этом укрепляются обратные связи: работодатели регулярно участвуют в разработке и аккредитации образовательных программ, предоставляют площадки для практик и стажировок, а учебные заведения предлагают обучение на базе компаний и совместные проектные курсы. Создание такой сети согласуется с рекомендациями по углублению интеграции отраслей и образования: современные исследования указывают на важность «двусторонней стыковки» образовательного предложения и индустриального спроса с помощью цифровых платформ общего доступа [4].

Инструментально-технологический блок. Включает цифровые платформы и инструменты, обеспечивающие сбор и обработку информации, а также поддержку образовательного процесса. В частности, предлагается внедрить систему мониторинга трудоустройства выпускников и обратной связи от работодателей. Подобная платформа позволяет собирать данные о карьерных траекториях выпускников, об их компетенциях и запросах рынка, что создаст «мост» между вузом и бизнесом. Примером является Career Path – цифровая система отслеживания выпускников, разработанная студентами в рамках проекта UNESCO: она собирает информацию о выпускниках и позволяет корректировать учебные программы в соответствии с требованиями индустрии.

Модель также предполагает поддержку микрокредитов (micro-credentials) – краткосрочных цифровых сертификатов за приобретенные навыки. Исследования Евросоюза показывают, что микрокредиты расширяют возможности непрерывного обучения и делают его более гибким. Наконец, сюда входит методология формирования индивидуальных образовательных траекторий: с учетом полученных данных платформа может помогать студентам выбирать дополнительные курсы и практики, актуальные для их будущих профессий, что повышает их адаптивность.

Оценочный блок. Система критериев и показателей эффективности модели – в ней задаются ключевые метрики для мониторинга успешности подготовки кадров. В качестве основных KPIs предлагаются: уровень трудоустройства выпускников (доля трудоустроенных по профилю в течение года после окончания), скорость их адаптации на рабочем месте, удовлетворенность работодателей качеством подготовки новых сотрудников, показатели вовлеченности студентов (например, участие в проектах, стажировках). Такие показатели нашли отражение в современных системах оценки качества образования: например, KPI-фреймворки для вузов выделяют результаты обучения, выпускников и удовлетворенность стейкхолдеров как ключевые направления. В контексте предложенной модели планируется регулярная отчетность по этим индикаторам. Сбор данных для оценки обеспечивает цифровая платформа: например, опросы работодателей и выпускников интегрированы в систему, что позволяет непрерывно анализировать слабые места и оперативно корректировать содержание и методы обучения.

В совокупности рассмотренные блоки образуют замкнутую систему: целевая часть определяет, чему учить; организационно-функциональная налаживает партнерства; инструментальная автоматизирует обмен информацией и поддерживает обучение; оценочная контролирует результативность. Таким образом, модель обеспечивает циклический процесс непрерывного улучшения подготовки кадров: требуемые компетенции постоянно уточняются на основе данных рынка, обучающие программы оперативно корректируются, а результаты проверяются через объективные метрики.

Предложенная модель учитывает современные вызовы цифровой экономики и стремится устранить выявленные разрывы между образованием и рынком труда. Образовательные программы, ориентированные на реальные компетенции (цифровые, междисциплинарные, профессиональные), позволяют выпускать специалистов, востребованных на рынке. Проводимые исследования подтверждают, что при явном фокусе на навыках, требуемых работодателями, удается значительно повысить уровень трудоустройства: например, в эмпирическом исследовании [6] показано, что участие студентов в целенаправленных практиках (проектных курсах и стажировках) существенно увеличивает их уверенность в готовности к работе и ясность карьерных целей. В частности, 89 % студентов после стажировок отмечали повышение своей готовности к реальной работе, а 84 % – более четкое понимание будущей профессиональной траектории [6]. Это демонстрирует эффективность организационно-функционального и проектного подходов модели – они не только дают навыки, но и помогают правильно сориентироваться в быстро меняющейся среде.

Сетевой механизм взаимодействия (вовлечение работодателей на всех уровнях – школы, колледжи, вузы) делает образовательную систему более гибкой и оперативно реагирующей на потребности экономики. Анализ зарубежного опыта показывает, что именно мультисторонние партнерства и цифровые платформы «двусторонней стыковки» играют решающую роль в глубоких реформах обучения. Например, использование интеграционных сервис-платформ в Китае показало эффективность «двусторонней стыковки» предложения и спроса: правительствам рекомендуется развивать такие платформы для более эффективной подготовки кадров.

Важным аспектом модели является цифровая платформа учета результатов. Опыт внедрения подобных систем, как в случае студентов Габона, показывает, что наличие достоверной статистики о выпускниках существенно улучшает качество образования. Инструмент обеспечит сбор реальной обратной связи: насколько хорошо выпускники соответствуют нуждам работодателей, каких компетенций им не достает. Это позволяет образовательным учреждениям непрерывно совершенствовать программы. Такой подход соответствует глобальной тенденции к использованию систем менеджмента образования (EMIS) и аналитических платформ для поддержки принятия решений – когда сведения о студентах и выпускниках служат основой для политики и оперативных изменений.

Наконец, оценочный блок с KPI-фокусом создает основание для доказательного управления качеством подготовки кадров. Разработанный фреймворк показателей поможет отслеживать, насколько предложенные новации дают эффект в реальности. Это важно с научной точки зрения – в перспективе на основе полученных данных можно будет корректировать модель, строить прогнозы эффективности, а с практической – позволит вузам и органам власти оценивать возврат инвестиций в образование.

Интеграция блоков модели позволяет сформировать циклическую систему, в которой обучение адаптируется к рынку, а рынок – к выпускникам. Это согласуется с положениями экономической социологии обучения и предыдущими исследованиями: доказано, что образование начинает способствовать росту экономики лишь при условии активного сближения университетов и бизнеса. Предложенная модель дает именно такие механизмы сближения, подкрепленные цифровыми технологиями и оценкой результатов.

Для приведенных блоков можно отметить следующее:

– целевой блок: на основе анализа вакансий и требований цифрового сектора определяется реестр компетенций, например, Flutter, работа с данными, agile-методологии;

– организационно-функциональный блок: создается сетевое партнерство: университет + + IT-компании + отраслевая ассоциация. Работодатели участвуют в разработке программ, предоставляют стажировки и проектные задания;

– инструментально-технологический блок: внедряется цифровая платформа для мониторинга трудоустройства выпускников и сбора обратной связи от работодателей. На основе данных формируются индивидуальные образовательные маршруты и микрокредиты по дефицитным навыкам;

– оценочный блок: система KPI отслеживает уровень трудоустройства выпускников, скорость их адаптации, удовлетворенность работодателей.

Взаимодействие блоков:

• данные от работодателей (через платформу) обновляют целевой блок (реестр компетенций);

• организационный блок реализует новые модули через сетевые формы обучения;

• инструментальный блок собирает данные о результатах;

• оценочный блок анализирует KPI и передает выводы для корректировки целей и программ.

Пошаговая инструкция для вузов по модернизации системы подготовки кадров.

1. Создать рабочую группу и провести аудит:

• сформировать команду из представителей учебного отдела, карьерного центра, IT-департамента и ключевых кафедр;

• провести аудит текущего состояния: собрать данные по трудоустройству выпускников, опросить работодателей-партнеров, проанализировать разрыв между программой и вакансиями.

2. Внедрить блоки модели поэтапно.

Этап 1. Целевой блок (что учить):

– создать «Карту компетенций» по каждой специальности на основе:

• анализа вакансий (Head Hunter и другие платформы);

• опросов работодателей;

• прогнозов технологических трендов (например, по отчетам «Атласа новых профессий»).

Пример. Для направления «Цифровой маркетинг» включить в программу навыки работы с AI-инструментами (ChatGPT, Midjourney), аналитику в «Яндекс.Метрике».

Этап 2. Организационный блок (как объединить усилия):

– заключить отраслевые соглашения с компаниями для:

• совместной разработки курсов (например, пригласить эксперта из «Яндекс.Практикума» для создания модуля);

• организации стажировок со 2-го, с 3-го курсов;

• создания наблюдательного совета программы из работодателей;

– внедрить сетевые формы обучения: онлайн-лекции от практиков, хакатоны на кейсах компаний.

Этап 3. Инструментальный блок (как автоматизировать):

– внедрить цифровую платформу (можно на базе LMS (Moodle) или разработать внутренний портал), которая:

• собирает резюме и карьерные траектории выпускников;

• позволяет работодателям оставлять отзывы о стажерах;

• формирует рекомендации студентам по выбору курсов (по принципу «Персональный учебный план»);

– ввести микрокредиты – цифровые сертификаты за короткие курсы (например, «Основы DevOps», от англ. development and operations – «разработка и операции»), которые можно накапливать.

Этап 4. Оценочный блок (как измерить результат):

– утвердить KPI для преподавателей и программ:

• процент трудоустройства выпускников за шесть месяцев;

• средняя зарплата выпускника через один год;

• индекс удовлетворенности работодателей (ежегодный опрос);

– закрепить ответственных за метрики (например, карьерный центр отчитывается о трудоустройстве, учебный отдел – о корректировке программ).

3. Запустить пилотный проект:

– выбрать одну-две востребованные специальности (например, «Анализ данных» и «Кибербезопасность»);

– апробировать на них модель в течение учебного года;

– скорректировать подход по итогам пилота перед масштабированием.

4. Интегрировать модель в стратегию вуза:

– внести изменения в документы (образовательные стандарты, положения о практиках);

– закрепить финансирование на цифровую платформу и сетевые программы;

– мотивировать преподавателей грантами за разработку курсов с работодателями.

Это даст вузу следующие преимущества:

– выпускники будут больше зарабатывать и быстрее находить работу, в результате растет репутация вуза;

– работодатели станут активными партнерами, снизят затраты на дообучение;

– вуз получит объективные данные для аккредитации и повышения позиций в рейтингах.

Ключевой принцип заключается в том, что данная модель – не теория, а цикл непрерывного обновления. Раз в семестр нужно анализировать KPI, собирать обратную связь и корректировать программы. Это превращает вуз в «адаптивную образовательную платформу».

В итоге в статье предлагается дорожная карта для перехода от обучения «по стандартам» к обучению «по запросу рынка». Начать можно с малого – с одной специальности и цифрового сервиса для сбора отзывов работодателей. Таким образом, модель создает замкнутый цикл непрерывного улучшения подготовки кадров, сокращая разрыв между образованием и рынком труда, повышая конкурентоспособность выпускников.

Заключение

1. Сформулирована целевая модель управления подготовкой конкурентоспособных кадров в цифровой экономике, основанная на интеграции образовательной системы и рынка труда. Предложенный интегративно-адаптивный подход включает четыре ключевых блока: целевой (компетенции будущего), организационно-функциональный (сеть «образование–бизнес–государство»), инструментально-технологический (цифровая платформа мониторинга и микрокредиты) и оценочный (система KPI).

2. Научная значимость результатов состоит в систематизации концепции профильной подготовки кадров и выработке обоснованной схемы взаимодействия разных уровней образования с индустрией. Практическая значимость проявляется в том, что модель может быть использована университетами и органами образования при разработке программ и стратегий кадровой политики, позволяя повысить пригодность выпускников к реальным запросам экономики.

3. Обеспечение непрерывности подготовки кадров и ее согласование с потребностями цифровой экономики требуют комплексных организационных и технологических решений. Предложенная модель задает такие решения, направленные на минимизацию разрывов между образованием и трудоустройством, повышение эффективности обучения и сокращение затрат на переподготовку специалистов.

4. Статья будет полезна специалистам в сфере управления образованием и разработчикам отраслевых программ.

Список литературы / References

1. Zubizarreta Pagaldai A., Cattaneo A., Imaz Agirre A., Marín V. I. (2025) Factors Influencing the Digital Competence of Students in Basic Vocational Education Training. *Empirical Research in Vocational Education and Training*. 17 (19). DOI: https://doi.org/10.1186/s40461-025-00198-0.
2. Chutcheva Y. V., Semenov A. V., Krasilnikova V. G., Balova S. L. (2023) Perspectives of Using the Integration Mechanisms of Education's Development for Accelerating Russia's Economic Growth. *Frontiers in Education*. 8. DOI: https://doi.org/10.3389/feduc.2023.1120915.
3. Hetmańczyk P. (2024) Digitalization and Its Impact on Labour Market and Education. Selected Aspects. *Education and Information Technologies*. 29, 11119–11134. DOI: https://doi.org/10.1007/s10639-023-12203-8.
4. Yuan P., Yang X. (2024) Exploration of the Model of Deepen Industry-Education Integration in the Digital Economy Era. *Journal of Internet and Digital Economics*. 4 (3), 179–186.
5. Tee P. K., Wong L. Ch., Dada M., Song B. L., Ng Ch. P. (2024) Demand for Digital Skills, Skill Gaps and Graduate Employability: Evidence from Employers in Malaysia. *F1000Research*. 13 (389). DOI: 10.12688/f1000research.148514.1.
6. Musa S., Nurhayati S., Boriboon G. (2025) The Effect of Internships on Graduates' Employability, Soft Skills, and Digital Competence. *Educational Process: International Journal.* 17. https://doi.org/10.22521/edupij.2025.17.306.

Поступила 16.12.2025 Принята в печать 28.01.2026 Доступна на сайте 10.04.2026

Received: 16 December 2025 Accepted: 28 January 2026 Available on the website: 10 April 2026

Сведения об авторе

Баранков Д. В., асп., Московский финансово-промышленный университет «Синергия»

Адрес для корреспонденции

129090, Российская Федерация,
Москва, ул. Измайловский Вал, 2
Московский финансово-промышленный
университет «Синергия»
Тел.: +7 800 100-00-11
E-mail: synergy@synergy.ru
Баранков Дмитрий Владимирович

Information about the author

Barankov D., Postgraduate, Moscow Financial and Industrial University "Synergy"

Address for correspondence

129090, Russian Federation,
Moscow, Izmailovsky Val St., 2
Moscow Financial
and Industrial University "Synergy"
Tel.: +7 800 100-00-11
E-mail: synergy@synergy.ru
Barankov Dmitry

http://dx.doi.org/10.35596/1729-7648-2026-32-1-26-32

УДК 331.5

«ЧЕЛОВЕЧЕСКИЙ КАПИТАЛ 5.0»: СИНЕРГИЯ ОПЫТА И ТЕХНОЛОГИЙ В УСЛОВИЯХ СОВРЕМЕННОЙ ТРАНСФОРМАЦИИ

А. И. ЯЩУК

Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Исследована смена парадигмы в управлении человеческим капиталом в условиях перехода от «Индустрии 4.0» к «Индустрии 5.0». Обосновано, что современная технологическая трансформация является не угрозой вытеснения человека, а катализатором для формирования «Человеческого капитала 5.0» – новой социотехнической модели, где технологии, включая искусственный интеллект и коллаборативную робототехнику, выступают в роли профессионального экзоскелета, расширяющего когнитивные и физические возможности работника. Особый акцент сделан на анализе синергии накопленного профессионального опыта и передовых цифровых инструментов. Установлено, что данная синергия позволяет повысить производительность и инклюзивность на рабочем месте, а также реализовать полный потенциал человеческого капитала, превращая сотрудников в ключевой актив для калибровки и управления интеллектуальными системами.

Ключевые слова: «Человеческий капитал 5.0», «Индустрия 5.0», синергия, профессиональный экзоскелет, когнитивная эргономика, промпт-инжиниринг, робоэтика, цифровая трансформация, человекоцентричность.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Ящук, А. И. «Человеческий капитал 5.0»»: синергия опыта и технологий в условиях современной трансформации / А. И. Ящук // Цифровая трансформация. 2026. Т. 32, № 1. С. 26–32. http://dx.doi.org/10.35596/1729-7648-2026-32-1-26-32.

“HUMAN CAPITAL 5.0”: SYNERGY OF EXPERIENCE AND TECHNOLOGY IN THE CONTEXT OF MODERN TRANSFORMATION

ANNA YASCHUK

BSUIR Institute of Information Technologies (Minsk, Republic of Belarus)

Abstract. This article explores the paradigm shift in human capital management amid the transition from “Industry 4.0” to “Industry 5.0”. It argues that modern technological transformation poses no threat of human displacement, but rather a catalyst for the emergence of “Human Capital 5.0” – a new sociotechnical model in which technologies, including artificial intelligence and collaborative robotics, act as a professional exoskeleton that expands workers’ cognitive and physical capabilities. Particular emphasis is placed on analyzing the synergy between accumulated professional experience and advanced digital tools. It is established that this synergy enables increasing productivity and inclusivity in the workplace, as well as the realization of the full potential of human capital, transforming employees into a key asset for calibrating and managing intelligent systems.

Keywords: “Human Capital 5.0”, “Industry 5.0”, synergy, professional exoskeleton, cognitive ergonomics, industrial engineering, robotics, digital transformation, human-centricity.

Conflict of interests. The author declares no conflict of interests.

For citation. Yaschuk A. (2026) “Human Capital 5.0”: Synergy of Experience and Technology in the Context of Modern Transformation. *Digital Transformation.* 32 (1), 26–32. http://dx.doi.org/10.35596/1729-7648-2026-32-1-26-32 (in Russian).

Введение

Глобальная экономическая система стоит на пороге больших перемен. На нее одновременно воздействуют две мощные глобальные тенденции: четвертая промышленная революция («Индустрия 4.0») и глубокие социально-демографические сдвиги. Основная концепция «Индустрии 4.0», которая основана на полной автоматизации, соединении цифрового и физического мира и вере в то, что технологии – главный двигатель прогресса, уступает место социогуманистической модели «Общество 5.0» и коррелирующей с ней концепции «Индустрия 5.0» [1, 2]. Этот переход знаменует возврат к человекоцентричности, где цифровые активы рассматриваются не как фактор замещения живого труда, а как инструмент для обеспечения устойчивости и инклюзивного процветания [3, 4] (табл. 1).

Таблица 1. Сравнение «Индустрии 4.0» и «Индустрии 5.0»
Table 1. Comparison of "Industry 4.0" and "Industry 5.0"

Критерий сравнения	«Индустрия 4.0»	«Индустрия 5.0»
Целевая направленность	Экономическая эффективность, производительность, минимизация издержек	Благополучие человека, устойчивое развитие, устойчивость систем к потрясениям
Роль человека	Ресурс, подлежащий оптимизации или вытеснению автоматизацией	Центральный агент, чьи возможности расширяются технологиями (симбиоз человека и машины)
Фокус технологий	Автоматизация рутинных задач, предиктивная аналитика	Коллаборативные системы (коботы), когнитивные ассистенты, персонализация
Ключевая ценность	Технологическая оптимизация процессов	Социотехническое равновесие и качество жизни

Концепция «Человеческого капитала 5.0»

Переход к «Индустрии 5.0» требует фундаментального переосмысления самого понятия «человеческий капитал». В рамках предыдущей, технократической, парадигмы человек зачастую рассматривался как трудовой ресурс – количественная единица, издержки на которую подлежат минимизации, а функции – автоматизации. «Индустрия 4.0», по своей сути, была нацелена на вытеснение человека из рутинных операций, что породило обоснованные опасения относительно будущего рынка труда [5, 6].

Концепция «Человеческого капитала 5.0» предлагает радикально иной подход, основанный на принципах социогуманистической модели. В этой модели человек является не объектом, а центральным субъектом и бенефициаром производственной системы. Происходит качественный сдвиг от оценки работника как исполнителя стандартизированных задач к его восприятию как носителя уникальных когнитивных и креативных способностей, которые машина не может воспроизвести. Качественный человеческий капитал в новой парадигме – это сложный конструкт, включающий опыт, критическое мышление, эмоциональный интеллект, адаптивность и способность к междисциплинарному синтезу [7].

Ключевым маркером этой трансформации является эволюция роли работника от «оператора» к «супервайзеру намерений». По мере того как автоматизация достигает уровней 4–5, где системы способны выполнять сложные задачи без прямого вмешательства, роль человека смещается от непосредственного выполнения операций к стратегическому управлению. Супервайзер намерений не выполняет работу, он определяет ее цели, задает ограничения, контролирует и верифицирует результаты, полученные интеллектуальными системами, и вмешивается в случае нештатных ситуаций или этических дилемм. Эта роль требует не столько узкоспециализированных технических навыков, сколько глубокого понимания бизнес-процессов, контекста и способности принимать решения в условиях неопределенности – качеств, которые являются прямым производным многолетнего опыта.

Эмпирическим подтверждением неразрывной связи между цифровым развитием и качеством человеческого капитала служат данные глобальных индексов. Анализ корреляции между индексом сетевой готовности (Network Readiness Index, NRI) и индексом человеческого капита-

ла (Human Capital Index, HCI) по 131 стране выявляет сильную положительную взаимозависимость (коэффициент Пирсона $r = 0{,}93776$) [8]. Это доказывает, что развитая цифровая инфраструктура (субиндекс NRI Technology) и готовность населения к ее использованию (субиндекс People) являются фундаментом для воспроизводства высококачественного человеческого капитала. Однако эта зависимость имеет сложный и непропорциональный характер. Кластерный анализ показывает, что для стран-лидеров (кластер 1: США, Германия, Сингапур) ключевым драйвером HCI становится уже не сама технология, а ее социальный эффект (субиндекс Impact, $r = 0{,}603$), тогда как для развивающихся стран (кластер 2: Алжир, Индия) инвестиции в технологии без должного институционального развития (субиндекс Governance) могут приводить к стагнации и даже отрицательной корреляции ($r = -0{,}0346$), создавая «цифровую ловушку» (рис. 1) [8]. Это подчеркивает, что «Человеческий капитал 5.0» формируется не технологиями как таковыми, а их грамотной, человекоцентричной интеграцией в социально-экономическую систему.

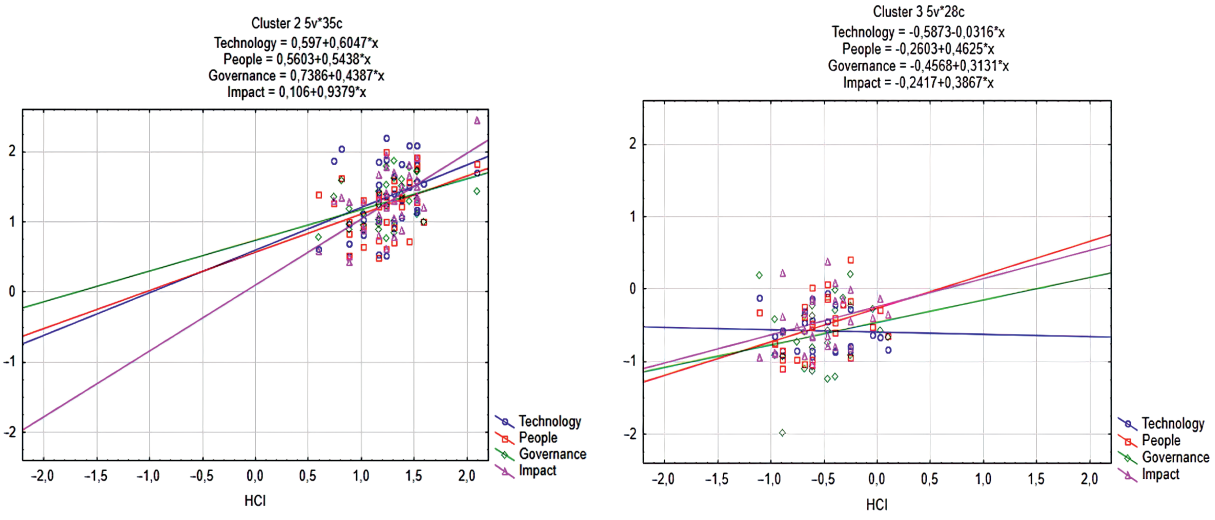

Рис. 1. Диаграммы рассеяния для HCI и компонентов NRI для кластеров 1 и 2
Fig. 1. Scattering diagrams for HCI and NRI components for clusters 1 and 2

Технологии как профессиональный экзоскелет

Концепция профессионального экзоскелета – это практическое воплощение принципов «Индустрии 5.0» на микроуровне рабочего места. Она предполагает использование технологий не для замены, а для расширения и дополнения человеческих возможностей, компенсации физических ограничений и снижения когнитивной нагрузки. Технологии берут на себя выполнение операций, связанных с риском для жизни и здоровья, тяжелым физическим трудом или деструктивным воздействием на окружающую среду, а также монотонных задач, ведущих к профессиональному выгоранию. Тем самым создаются условия для того, чтобы человек мог максимально реализовать свой уникальный потенциал в сферах творчества, управления сложностью, проектирования систем и долгосрочного планирования [9].

На физическом уровне эту роль выполняют коллаборативные роботы (коботы) и промышленные экзоскелеты. В отличие от традиционных промышленных роботов, изолированных в клетках безопасности, коботы предназначены для работы в непосредственной близости с человеком [3]. Они выполняют монотонные, требующие высокой точности или физических усилий операции: подъем и перемещение тяжестей, закручивание крепежа с заданным моментом, нанесение герметика. Это позволяет работникам с разным уровнем физической подготовки эффективно выполнять производственные задачи, а также дает возможность опытным специалистам, чья физическая выносливость может со временем снижаться, переходить на роли наставников и контролеров качества [10]. Экзоскелеты, в свою очередь, напрямую снижают нагрузку на опорно-двигательный аппарат, что критически важно для предотвращения производственного травматизма и продления профессиональной жизни в целом [11].

На когнитивном уровне роль экзоскелета выполняет искусственный интеллект (ИИ). Современные производственные и бизнес-системы характеризуются высокой сложностью ин-

терфейсов и информационных потоков, что может стать барьером для сотрудников любого возраста. ИИ-ассистенты, интегрированные в рабочие платформы, способны радикально упростить это взаимодействие. Они могут автоматизировать рутинные задачи (обработка почты, заполнение отчетов, поиск информации), предоставлять контекстуальные подсказки в режиме реального времени и преобразовывать сложные данные в интуитивно понятные визуализации [12]. Системы дополненной реальности (AR) могут накладывать цифровую информацию (схемы, инструкции) на реальные объекты, направляя действия работника при сборке или ремонте сложного оборудования. Это не только снижает когнитивную нагрузку и вероятность ошибки, но и ускоряет процесс обучения, позволяя специалистам сосредоточиться на принятии нетривиальных решений, менторстве и передаче опыта.

Таким образом, профессиональный экзоскелет создает адаптированные, инклюзивные рабочие места, которые нивелируют ограничения и усиливают преимущества каждого работника независимо от его возраста и физических данных. Это прямой путь к построению устойчивого и производительного рынка труда.

Синергия опыта и технологий: роль промт-инжиниринга

Стремительное развитие генеративных нейросетей (таких как GPT, DALL-E, Midjourney) формирует новую, ранее не существовавшую область профессиональной деятельности, где накопленный человеческий опыт становится критически важным капиталом. Эффективность этих моделей напрямую зависит от качества и точности входных данных – запросов (или промптов). Формулирование эффективного промпта – не техническая, а интеллектуальная задача, требующая глубокого понимания предметной области, контекста, скрытых взаимосвязей и желаемого результата. Этот процесс, получивший название «промпт-инжиниринг», становится мостом между человеческой интуицией и машинным интеллектом.

Именно здесь возникает уникальная синергия между опытом профессионалов и возможностями ИИ. Специалист с многолетним стажем обладает тем, чего лишена любая нейросеть – «неявным знанием», интуицией и пониманием бизнес-контекста. Он знает, какие вопросы задавать, какие переменные важны, а какие являются «шумом», какие формулировки приведут к релевантному результату, а какие – к поверхностному или ошибочному. Например, при использовании ИИ для анализа рыночных тенденций опытный маркетолог сможет сформулировать промпт, учитывающий сезонность, региональную специфику, поведение конкурентов и психологию потребителей, в то время как начинающий специалист, обладающий лишь техническими навыками, скорее всего, получит от ИИ стандартный, общедоступный анализ.

В этой парадигме работник превращается из пассивного пользователя технологий в активного наставника или калибровщика для ИИ [13]. Он использует свой опыт для тонкой настройки запросов, итеративной проверки и уточнения результатов, направляя мощь ИИ на решение конкретных, практически значимых бизнес-задач. Опыт становится новым капиталом в эпоху ИИ, поскольку именно он позволяет извлекать из технологии максимальную ценность. Это меняет динамику на рынке труда: вместо конкуренции в скорости освоения новых интерфейсов профессионалы могут занять нишу, где их главные активы – мудрость и интуиция – незаменимы.

Таким образом, промпт-инжиниринг является ярким примером того, как технологии не вытесняют, а создают новые роли для опытных кадров, делая их знания и навыки более востребованными, чем когда-либо. Это подтверждает центральный тезис «Индустрии 5.0» о симбиозе человека и машины, где каждый из партнеров вносит свой уникальный вклад в достижение общего результата.

Человекоцентричность и эргономика: управление когнитивной нагрузкой и робоэтика

На микроэкономическом уровне принципы человекоцентричности «Индустрии 5.0» выражаются через концепцию «Оператора 5.0» [9], где эргономика трансформируется из гигиенического фактора в стратегический инструмент обеспечения конкурентоспособности. Если традиционная эргономика была сфокусирована преимущественно на физических аспектах труда, то «Эргономика 5.0» делает акцент на когнитивном и психологическом благополучии работника.

Особое значение приобретает когнитивная эргономика – дисциплина, изучающая взаимодействие человека с информационными системами с точки зрения ментальных процессов:

восприятия, памяти, принятия решений. Цель когнитивной эргономики – проектирование социотехнических ансамблей, адаптированных под психофизиологию сотрудника для управления его рабочей нагрузкой [14]. В условиях, когда работник взаимодействует с потоками данных, ИИ-ассистентами и сложными интерфейсами, риск когнитивной перегрузки, информационной усталости и профессионального выгорания резко возрастает. Системы, разработанные с учетом принципов когнитивной эргономики, минимизируют этот риск, обеспечивая интуитивно понятное представление информации, снижая количество ненужных действий и автоматизируя рутину. Это напрямую соотносится с показателем HCI: снижение когнитивного переутомления обеспечивает сохранение ожидаемой продуктивности работника в течение всего его профессионального жизненного цикла.

Однако внедрение интеллектуальных систем порождает и новые этические вызовы, требующие формирования робоэтики – системы регуляторных и этических норм, управляющих взаимодействием человека и машины [15]. Одним из наиболее серьезных рисков является алгоритмическая предвзятость. Системы ИИ, обученные на данных, в которых недостаточно представлены определенные демографические группы (например, по возрасту или полу), могут демонстрировать более низкую точность в распознавании их речи, лиц или эмоций. Это может приводить к прямой дискриминации: от сбоев в работе систем биометрического доступа до предвзятых решений автоматизированных систем рекрутинга, отсеивающих кандидатов на основе косвенных маркеров.

Другой аспект – психологическое давление, или техностресс, вызванный страхом потери работы из-за автоматизации [15]. Для предотвращения этих рисков необходим комплексный подход, включающий как технические, так и организационные меры. Компоненты этики ИИ, представленные в табл. 2, охватывают ключевые направления такой работы.

Таблица 2. Компоненты этики искусственного интеллекта
Table 2. Components of artificial intelligence ethics

Компонент	Описание и значение
Прозрачность и объяснимость	Алгоритмы, особенно в критических областях (рекрутинг, медицина), должны быть не «черными ящиками», а прозрачными системами, способными объяснить логику своих решений. Это позволяет человеку оспаривать решения машины
Предотвращение предвзятости	Обязательный аудит наборов данных и самих алгоритмов на предмет возрастной, гендерной и иной дискриминации. Разработка стандартов для инклюзивных датасетов
Автономия и контроль человека	Закрепление принципа human-in-the-loop, согласно которому окончательное решение в значимых вопросах всегда остается за человеком. Человек должен сохранять роль супервайзера намерений, а не становиться «рабом алгоритма»
Конфиденциальность и безопасность данных	Защита персональных данных работников от несанкционированного доступа и использования. Обеспечение кибербезопасности автоматизированных рабочих мест
Психологическое благополучие	Проектирование систем, которые не вызывают техностресс, а поддерживают работника. Проведение открытого диалога в компаниях о целях и последствиях автоматизации

Формирование робоэтики и внедрение принципов когнитивной эргономики являются необходимыми условиями для построения доверительных и продуктивных отношений между человеком и машиной, что составляет ядро человекоцентричной «Индустрии 5.0».

Заключение

1. Проведенный анализ доказывает, что технологическая трансформация, катализируемая «Индустрией 5.0», является мощным инструментом инклюзивности и устойчивого развития. Синтез человеческого опыта и технологий «Индустрии 5.0» создает новую модель – «Человеческий капитал 5.0», где работник выступает не как придаток машины, а как супервайзер намерений. Ключевым элементом этой синергии становится промпт-инжиниринг, позволяющий

специалистам использовать свой уникальный накопленный опыт и интуицию для эффективной калибровки и управления интеллектуальными системами.

2. Важнейшим условием реализации этого потенциала является внедрение принципов когнитивной эргономики и робоэтики. Управление когнитивной нагрузкой и обеспечение прозрачности алгоритмов позволяют проектировать рабочие места, адаптированные под психофизиологию человека, обеспечивая ментальное благополучие сотрудников. Таким образом, «Индустрия 5.0» не заменяет человека, а выступает в роли профессионального экзоскелета, расширяющего возможности специалиста и превращающего технологический прогресс в стратегический инструмент для максимального раскрытия человеческого потенциала в интересах устойчивого экономического развития.

Список литературы

1. Industry 5.0 – Towards a Sustainable, Human-Centric and Resilient European Industry // European Commission. Brussels: Directorate-General for Research and Innovation, 2021.
2. Nahavandi, S. Industry 5.0 – A Human-Centric Solution / S. Nahavandi // Sustainability. 2019. Vol. 11, No 16. P. 1–13.
3. Demir, K. A. Industry 5.0 and Human-Robot Co-Working / K. A. Demir, G. Doven, B. Sezen // Procedia Computer Science. 2019. Vol. 158. P. 688–695.
4. Скотт, Э. Старения населения не стоит бояться, его нужно научиться использовать / Э. Скотт, П. Пайот // Финансы и развитие. Режим доступа: https://www.imf.org/ru/publications/fandd/issues/2025/06/the-longevity-dividend-andrew-scott. Дата доступа: 03.02.2026.
5. Our World is Growing Older: UN DESA Releases New Report on Ageing // United Nations. Mode of access: https://www.un.org/development/desa/en/news/population/our-world-is-growing-older.html. Date of access: 03.02.2026.
6. Rampersad, G. Robot Will Take Your Job: Innovation for an Era of Artificial Intelligence / G. Rampersad // Journal of Business Research. 2020. Vol. 116, No 4. P. 68–74.
7. Industry 5.0 as a Human-Centric Direction for Social and Labor Entities Transformations / L. Melnyk [et al.] // Problems and Perspectives in Management. 2025. Vol. 23, No 4. P. 290–300.
8. Stryzhak, O. Features of the Relationship Between Human Capital Development and Digital Technologies in the Context of Society 5.0 Formation / O. Stryzhak // Agricultural and Resource Economics: International Scientific E-Journal. 2022. Vol. 8, No 3. P. 224–243.
9. Human Centric Industry 5.0 Manufacturing: A Multi-Level Framework from Design to Consumption Within Society 5.0 / V. Nasir [et al.] // International Journal of Sustainable Engineering. 2025. Vol. 18, No 1. P. 1–14.
10. Vitrano, G. Rethinking Work in Industry 5.0: Leveraging Technology for an Ageing Workforce / G. Vitrano, G. J. L. Micheli // Public Health Challenges. 2025. Vol. 4, No 3.
11. Jerbić, B. Artificial Intelligence and Robotics as the Driving Power of Modern Society / B. Jerbić, M. Švaco // Frontiers in Sociology. 2023. No 7. P. 1–55.
12. Pizzinelli, C. AI and the Future of Work in an Aging Economy / C. Pizzinelli, M. M. Tavares // Pension Research Council Working Paper. 2025.
13. Chetty, K. AI Literacy for an Ageing Workforce: Leveraging the Experience of Older Workers / K. Chetty // OBM Geriatrics. 2023. Vol. 7, No 3. P. 1–17.
14. Ranasinghe, R. T. Cognitive Ergonomics in Industry 5.0: Supporting an Aging Workforce Through Human-Centric Design / R. T. Ranasinghe // Journal of Human Factors and Ergonomics in Manufacturing & Service Industries. 2025. P. 1–10.
15. Companion Robots to Mitigate Loneliness Among Older Adults: Perceptions of Benefit and Possible Deception / C. Berridge [et al.] // Frontiers in Psychology. 2023. Vol. 14.

Поступила 09.02.2026 Принята в печать 27.02.2026 Доступна на сайте 10.04.2026

References

1. Industry 5.0 – Towards a Sustainable, Human-Centric and Resilient European Industry. *European Commission*. Brussels, Directorate-General for Research and Innovation. 2021.
2. Nahavandi S. (2019) Industry 5.0 – A Human-Centric Solution. *Sustainability*. 11 (16), 1–13.
3. Demir K. A., Doven G., Sezen B. (2019) Industry 5.0 and Human-Robot Co-Working. *Procedia Computer Science*. 158, 688–695.
4. Scott A., Piot P. (2026) Don't be Afraid of Population Aging, You Need to Learn How to Use It. *Finance & Development*. Available: https://www.imf.org/ru/publications/fandd/issues/2025/06/the-longevity-dividend-andrew-scott (Accessed 3 February 2026) (in Russian).

5. United Nations (2026) Our World is Growing Older: UN DESA Releases New Report on Ageing. *United Nations*. Available: https://www.un.org/development/desa/en/news/population/our-world-is-growing-older.html (Accessed 3 February 2026).
6. Rampersad G. (2020) Robot Will Take Your Job: Innovation for an Era of Artificial Intelligence. *Journal of Business Research*. 116 (4), 68–74.
7. Melnyk L., Remsei S., Kubatko O., Kalinichenko L. (2025) Industry 5.0 as a Human-Centric Direction for Social and Labor Entities Transformations. *Problems and Perspectives in Management*. 23 (4), 290–300.
8. Stryzhak O. (2022) Features of the Relationship Between Human Capital Development and Digital Technologies in the Context of Society 5.0 Formation. *Agricultural and Resource Economics: International Scientific E-Journal*. 8 (3), 224–243.
9. Nasir V., Hosseini A., Binfield L., Hasani N. (2025) Human Centric Industry 5.0 Manufacturing: A Multi-Level Framework from Design to Consumption Within Society 5.0. *International Journal of Sustainable Engineering*. 18 (1), 1–14.
10. Vitrano G., Micheli G. J. L. (2025) Rethinking Work in Industry 5.0: Leveraging Technology for an Ageing Workforce. *Public Health Challenges*. 4 (3).
11. Jerbić B., Švaco M. (2023) Artificial Intelligence and Robotics as the Driving Power of Modern Society. *Frontiers in Sociology*. (7), 1–55.
12. Pizzinelli C., Tavares M. M. (2025) AI and the Future of Work in an Aging Economy. *Pension Research Council Working Paper*.
13. Chetty K. (2023) AI Literacy for an Ageing Workforce: Leveraging the Experience of Older Workers. *OBM Geriatrics*. 7 (3), 1–17.
14. Ranasinghe R. T. (2025) Cognitive Ergonomics in Industry 5.0: Supporting an Aging Workforce Through Human-Centric Design. *Journal of Human Factors and Ergonomics in Manufacturing & Service Industries*. 1–10.
15. Berridge C., Zhou Y., Robillard J. M., Kaye J. (2023) Companion Robots to Mitigate Loneliness Among Older Adults: Perceptions of Benefit and Possible Deception. *Frontiers in Psychology*. 14.

Received: 9 February 2026 Accepted: 27 February 2026 Available on the website: 10 April 2026

Сведения об авторе

Ящук А. И., канд. экон. наук, доц., дир., Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники

Information about the author

Yashchuk A., Cand. Sci. (Econ.), Associate Professor, Director, BSUIR Institute of Information Technologies

Адрес для корреспонденции

220037, Республика Беларусь,
Минск, ул. Козлова, 28
Институт информационных технологий БГУИР
Тел.: +375 29 630-08-98
E-mail: a.iashchuk@bsuir.by
Ящук Анна Иосифовна

Address for correspondence

220037, Republic of Belarus,
Minsk, Kozlova St., 28
BSUIR Institute of Information Technologies
Tel.: +375 29 630-08-98
E-mail: a.iashchuk@bsuir.by
Yaschuk Anna

http://dx.doi.org/10.35596/1729-7648-2026-32-1-33-44

УДК 004.056.5:004.891:658.15

МЕТОДИКА ОЦЕНКИ ФИНАНСОВЫХ РИСКОВ ОРГАНИЗАЦИЙ НА ОСНОВЕ ВНЕДРЕНИЯ ISOLATED MULTIAGENT ARBITRATION

Е. С. ПИСКУН, А. А. АЗИЗОВ, Е. В. КРЯЧЕВ

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Рассмотрена проблема обеспечения снижения финансовых рисков хозяйствующих субъектов в условиях масштабного внедрения автономных интеллектуальных агентов. Показано, что существующие угрозы безопасности для систем больших языковых моделей, такие как стеганографические инъекции и поисково-дополненная генерация, трансформируются из технических инцидентов в существенные факторы операционного риска, способные нанести прямой экономический ущерб, исчисляемый миллионами долларов. Предложена методика оценки финансовых рисков на основе целевой функции полной стоимости владения, включающей операционные затраты и ожидаемые годовые потери, а также дисконтированного анализа для инвестиционного обоснования мероприятий защиты. В качестве практической реализации рассматривается архитектура Isolated Multiagent Arbitration, реализующая принцип эшелонированной защиты и изоляции генерации от исполнения и включающая модуль глубокой инспекции файлов, кастомную модель-аудитор для постгенерационного анализа ответов и механизм динамической оценки доверия к источникам в поисково-дополненной генерации.

Ключевые слова: большие языковые модели, автономные интеллектуальные агенты, промпт-инъекции, кибербезопасность, искусственный интеллект, финансовый риск, оценка стоимости, экономический эффект.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Пискун, Е. С. Методика оценки финансовых рисков организаций на основе внедрения Isolated Multiagent Arbitration / Е. С. Пискун, А. А. Азизов, Е. В. Крячев // Цифровая трансформация. 2026. Т. 32, № 1. С. 33–44. http://dx.doi.org/10.35596/1729-7648-2026-32-1-33-44.

A METHOD FOR ASSESSING THE FINANCIAL RISKS OF ORGANIZATIONS BASED ON THE IMPLEMENTATION OF ISOLATED MULTIAGENT ARBITRATION

EKATERINA PISKUN, AKBARJON AZIZOV, EGOR KRYCHEV

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. This article examines the problem of reducing the financial risks of economic entities in the context of the large-scale implementation of autonomous intelligent agents. It demonstrates that existing security threats to systems with large language models, such as steganographic injections and search-based augmentation generation, are transforming from technical incidents into significant operational risk factors capable of causing direct economic damage amounting to millions of dollars. A financial risk assessment method is proposed based on the total cost of ownership objective function, which includes operating costs and expected annual losses, as well as a discounted analysis for investment justification of security measures. The Isolated Multiagent Arbitration architecture is considered as a practical implementation. It implements the principle of layered protection and isolation of generation from execution and includes a deep file inspection module, a custom auditor model for post-generation response analysis, and a mechanism for dynamically assessing the trustworthiness of sources in search-based augmentation generation.

Keywords: large language models, autonomous intelligent agents, prompt injections, cybersecurity, artificial intelligence, financial risk, valuation, economic impact.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Piskun E., Azizov A., Krychev E. (2026) A Method for Assessing the Financial Risks of Organizations Based on the Implementation of Isolated Multiagent Arbitration. *Digital Transformation.* 32 (1), 33–44. http://dx.doi.org/10.35596/1729-7648-2026-32-1-33-44 (in Russian).

Введение

Массовое внедрение больших языковых моделей (LLM) в критически важную бизнес-инфраструктуру с 2024 г. привело к смене парадигмы кибербезопасности: от защиты статических информационных активов к обеспечению устойчивости автономных агентных систем. Современные архитектуры наделяют агентов искусственного интеллекта (ИИ, AI-агент) правами на чтение файловых систем, выполнение API-запросов и автономное принятие решений. Это существенно расширяет поверхность атаки по сравнению с ранними реализациями генеративного ИИ, функционировавшими в изолированном режиме «текст-в-текст».

По данным McKinsey, к началу 2024 г. 65 % организаций регулярно использовали генеративный ИИ, при этом 80 % компаний увеличили инвестиции в эту область [1, 2]. В [3] прогнозируется существенный рост мировых расходов на ИИ. Параллельно фиксируется критический рост киберугроз. Согласно [4], 2023-й стал рекордным по количеству ИИ-инцидентов, включая утечки данных, дискриминационные решения и эксплуатацию уязвимостей. Совокупный ущерб от инцидентов с участием ИИ-агентов становится сопоставимым с ущербом от крупных утечек данных [4, 5], при этом скорость технологического внедрения опережает развитие процедур надзора и тестирования. Финансовые потери от подобных инцидентов повышаются на фоне роста инвестиций в ИИ-инфраструктуру. Средняя глобальная стоимость утечки данных достигла 4,88 млн долл. [5]. Уязвимость EchoLeak (CVE-2025-32711) в Microsoft 365 Copilot позволила реализовать атаку типа zero-click с эксфильтрацией данных [6, 7], единичные отравленные документы приводили к утечкам через интеграции с ChatGPT [8], атаки непрямой промпт-инъекции использовались против Slack AI и других корпоративных ассистентов [9, 10]. Автономный LLM-агент с доступом к электронной почте, RAG-хранилищам и документам в случае успешной промпт-инъекции или RAG Poisoning (Retrieval-Augmented Generation, RAG – поисково-дополненная генерация) может передавать конфиденциальные документы, раскрывать коммерческие тайны или инициировать несанкционированные действия.

Существующие защитные механизмы (RLHF и статические контент-фильтры) недостаточно эффективны против семантических обходов и обфускации [11–15]. RAG Poisoning и Jamming-атаки показывают, что даже небольшое число вредоносных документов, внедренных в базу знаний, обеспечивает высокий коэффициент успешных атак (ASR), даже если основная часть корпуса остается чистой [16–18].

Цель исследований – разработка и экономическое обоснование инвестиционного проекта по внедрению архитектуры изолированного мультиагентного арбитража (Isolated Multiagent Arbitration, IMA) для обеспечения снижения рисков финансовых потерь организации в условиях масштабного использования автономных AI-агентов.

Разработка и экспериментальная валидация эффективности архитектуры IMA

Архитектура IMA реализует подход эшелонированной защиты (Defense-in-Depth), где входящие запросы обрабатываются каскадом специализированных сервисов, взаимодействующих по REST/gRPC. Система логически разделена на три функциональных модуля, представленных на рис. 1.

Модуль 1. Deep File Inspection (DFI) – глубокая инспекция файлов. Проверка типов файлов по сигнатурам, очистка метаданных и имен, OCR-поиск стеганографии; все подозрительное блокируется по принципу Fail-Secure.

Модуль 2. Изолированный генератор (Agent Zero) дает черновой ответ, SecAudit выносит вердикт CLEAN/FLAGGED. SecAudit – трансформер-аудитор, который получает объединенный контекст (USER, RESPONSE, META, RAG) и решает, нормальный это запрос или атака, учитывая вредные инструменты и низкий trust RAG-источников. Обучающий корпус собирается из открытых наборов вредоносных/чистых промптов (AdvBench, JailbreakBench), атак на агентов (ToolEmu, AgentHarm) и сценариев RAG Poisoning/Jamming (PoisonedRAG, RobustRAG и др.), плюс корпоративные данные. Разметка идет по содержанию ответа (код, инструкции, сек-

реты), воздействию на RAG и вызовам инструментов; итоговые классы – CLEAN, JAILBREAK, EXFILTRATION, TOOL_ABUSE, RAG_POISONING, с десятками тысяч примеров на каждый.

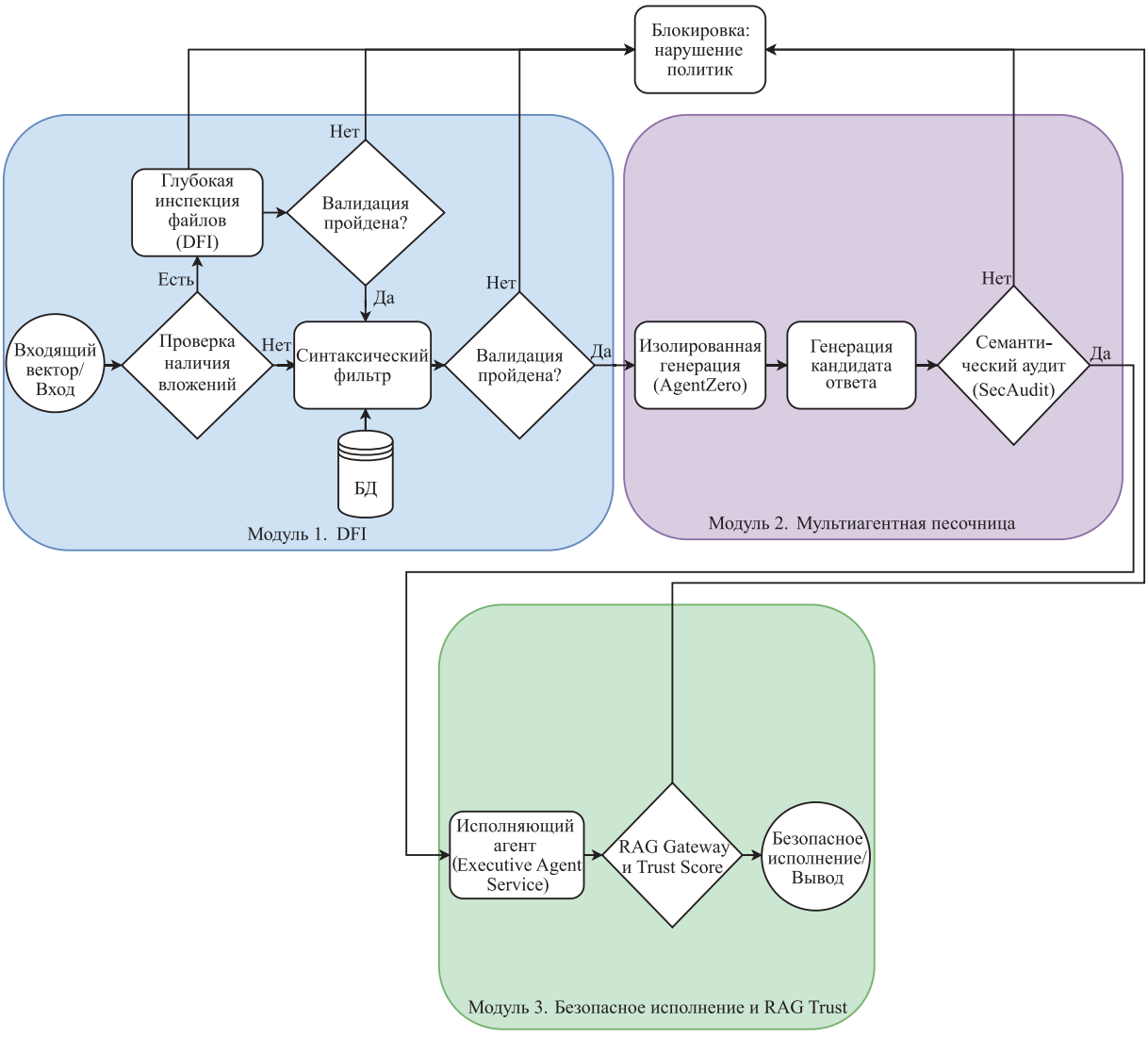

Рис. 1. Схема работы системы IMA
Fig. 1. IMA system workflow

Модель – трансформер-энкодер уровня BERT (12–24 слоя, 768–1024), дообученный как мультиклассовый/мультилейбл-классификатор с взвешенной cross-entropy и Focal loss, оптимизатор AdamW; качество контролируется по F1, особенно для EXFILTRATION и RAG_POISONING. В продакшене SecAudit работает как GPU-сервис с латентностью 300–500 мс: Agent Zero генерирует ответ, SecAudit считает распределение p(class | контекст) и по порогам p(CLEAN) и суммарного p(unsafe) выдает вердикт CLEAN или FLAGGED (с блокировкой и безопасным объяснением). Trust для RAG считается при индексации (T(d) по происхождению, свойствам домена, лингвистическим аномалиям и шаблонам poison); низко доверенные документы уходят в теневой индекс. На этапе извлечения кандидаты фильтруются по T_min, спорные помечаются RAG_TRUST=low. Возраст домена – лишь один из признаков в этой модели, а не бинарный критерий доверия.

Модуль 3. Только CLEAN-запросы попадают в Executive Agent с доступом к инструментам; контекст исполнения изолирован от проверки, все FLAGGED/блокировки логируются в SIEM, полный цикл ограничен 60 с.

В эксперименте объект защиты – автономный LLM-агент с доступом к файловой системе, внешним API и (опционально) RAG, частично недоверенному. Атакующий – подает произвольные запросы, загружает файлы, может помещать документы в RAG, но не имеет админ-доступа,

ключей и кода (black box). Цели атак: (1) jailbreak/обход выравнивания; (2) exfiltration данных из почты/файлов/RAG; (3) tool abuse для опасных действий; (4) poisoning/jamming через отравление RAG. Вне рамок – атаки на операционную систему/гипервизор/сеть, отравление предобучения, внутренние админы. Успешная атака (ASR) – вредоносный вывод LLM или принятие отравленной лжи, противоречащей базовому корпусу (PoisonedRAG).

Оценка проводилась на SecBench25 (200 сценариев, 1000 прогонов: текст, файлы, RAG). Метрики: ASR, FPR, Latency. BaselineGemini показал ASR ~16 % (160/1000), тогда как предлагаемая архитектура IMAProtection (DFI→AgentZero→SecAudit→Executive Agent + RAGtrust) продемонстрировала ASR = 0/1000; 95%-ная односторонняя верхняя граница истинного ASR ≤0,30 %. По поднаборам: текст – ≤(0,60–0,75) %, файлы – ≤(1,49–1,98) %, RAG – (≤0,99–1,19) %. Ложные блокировки не зафиксированы (FPR = 0; 95%-ная верхняя граница ≤(1,19–1,49) %). Модуль DFI заблокировал 50/50 вредоносных файлов до попадания в контекст LLM (95%-ная нижняя оценка эффективности ≥94,2 %). Средняя задержка в атакующем режиме снижена с 25,6 до 12,1 с за счет раннего отсечения атак. Ограничения: ограниченный объем выборки, отсутствие прямого сравнения с альтернативными защитами и зависимость от проприетарных LLM.

Технико-экономическая эффективность внедрения IMA

Аппарат оценки экономической эффективности внедрения IMA и снижения финансовых рисков построен от общего к частному: сначала формализуются целевая функция и алгоритм расчета, затем приводятся числовой сценарий и анализ чувствительности. При оценке экономической эффективности систем информационной безопасности рассчитывается полная стоимость владения (TCO), состоящая из прямых затрат на генерацию/исполнение ($Cost_{LLM}$), эксплуатационных затрат на защиту ($Cost_{IMA}$), ожидаемых ежегодных потерь от остаточного риска (ALE_{res}) и объема предотвращенных ежегодных потерь (ALE_{saved}). При отсутствии двойного счета (т. е. каждый элемент затрат или доходов учтен в расчетах только один раз) и раздельном учете потоков расходов совокупные издержки представляются суммой компонент (аддитивной моделью). Такой подход согласуется с технико-экономическими методиками оценки эффективности средств защиты [19] и с подходом «затраты/выгоды» в экономике информационной безопасности [20]. Для фиксации управленческих приоритетов в аддитивную модель вводятся веса w (коэффициенты значимости) слагаемых [19, 21, 22]

$$TCO = w_{LLM}Cost_{LLM} + w_{IMA}Cost_{IMA} + w_{res}ALE_{res} - ALE_{saved}. \quad (1)$$

В классическом денежном выражении сумма весов w_{LLM}, w_{IMA} и w_{res} принимается равной единице. При необходимости многокритериального выбора веса могут задаваться экспертно следующим образом:

– w_{LLM} (для $Cost_{LLM}$) позволит учесть высокую чувствительность организации к операционным издержкам; в этом случае любое снижение вычислительных ресурсов приносит значимый экономический эффект в рамках модели;

– w_{IMA} ($Cost_{IMA}$) приведет к повышению коэффициента консервативности при оценке затрат на защиту;

– w_{res} (ALE_{res}) позволит малейший остаточный риск (возможность инцидента) оценивать финансово выше его номинальной стоимости, учитывая потенциально катастрофические репутационные последствия.

Для обеспечения сопоставимости результатов и отражения управленческих приоритетов слагаемые, формирующие затратную часть TCO, взвешиваются с помощью нормированных коэффициентов w_i. Значения w_i определялись экспертным путем в соответствии с декомпозицией возможных предотвращенных ежегодных финансовых потерь организации: $w_{LLM} = 0,75$; $w_{IMA} = 0,15$ и $w_{res} = 0,10$. Отрицательное слагаемое ALE_{saved} учитывается в модели без весового коэффициента, так как представляет собой прямой объем предотвращенного ущерба, уменьшающий совокупные издержки [23, 24].

Для оценки экономической эффективности внедрения архитектуры IMA был разработан сценарий для предприятия среднего масштаба. Расчетная модель базировалась на следующих вводных параметрах:

– масштаб внедрения: 1000 активных пользователей N_{users}, генерирующих в среднем 20 запросов в сутки при 250 рабочих днях в году;

– общий объем нагрузки: $N_{year} = 1000 \cdot 20 \cdot 250 = 5 \cdot 10^6$ запросов в год.

Структура затрат разделяется на первоначальные (InitialEx) и последующие ежегодные операционные затраты (OpEx).

InitialEx (Year) включают расходы на R&D, развертывание микросервисной архитектуры и первичную интеграцию IMA-контура. Исходя из оценки трудозатрат команды (3–5 инженеров на 6–9 месяцев) и настройки инфраструктуры, CapEx оценивается в 150 000 долл. в год.

OpEx (Annual) включают:

– LLM-инференс: при стоимости сложного запроса (Agent Zero + Исполнитель) $P_{req} \approx 0{,}016$ долл., затраты на токены составляют ~80 000 долл. в год;

– инфраструктуру и фонд оплаты труда: амортизация мощностей (GPU/CPU для DFI/SecAudit) и эксплуатационные расходы (1–2 FTE MLOps/SecOps) оцениваются в 100 000 долл. в год;

– итого OpEx ≈ 180 000 долл. в год.

Алгоритм количественного анализа рисков, интегрированный в модель оценки инвестиционной эффективности внедрения IMA, имеет следующий вид [21, 24, 25]:

– определение ущерба одного значимого инцидента SLE (Single Loss Expectancy), долл.;

– оценка частоты (интенсивность) критических попыток атак на агентную систему ARO_{att} (1/год), экспериментальная оценка вероятности успеха попытки ASR*;*

– получение ожидаемого числа успешных инцидентов в год (ARO, 1/год)

$$\mathrm{ARO} = \mathrm{ARO}_{\mathrm{att}} \cdot \mathrm{ASR}; \tag{2}$$

– расчет ожидаемых годовых потерь, позволяющий перевести абстрактные угрозы в ожидаемые денежные потери, что необходимо для сопоставления с затратами на внедрение

$$\mathrm{ALE} = \mathrm{SLE} \cdot \mathrm{ARO}; \tag{3}$$

– определение предотвращенного ущерба (годовой эффект) от внедрения IMA, которая позволяет оценить разницу между потерями без защиты и с защитой, т. е. это «доходная» часть проекта

$$\Delta\mathrm{ALE} = \mathrm{ALE}_{\mathrm{base}} - \mathrm{ALE}_{\mathrm{IMA}}; \tag{4}$$

– формирование чистого денежного потока проекта на горизонте H лет

$$\mathrm{CF}_t = \Delta\mathrm{ALE} - \mathrm{OpEx}_t; \tag{5}$$

– расчет чистого дисконтированного дохода (Net Present Value, NPV)

$$\mathrm{NPV} = -\mathrm{InitialEx} + \sum_{t=1}^{5} \frac{\left(\mathrm{ALE}_{\mathrm{base}} - \mathrm{ALE}_{\mathrm{IMA}}\right) - \mathrm{OpEx}_t}{\left(1+r\right)^t}, \tag{6}$$

где InitialEx – инвестиционные затраты (Initial Investment), долл.

Экономическая эффективность предложенной архитектуры IMA базируется на уменьшении показателя ALE. Технические испытания на тестовом наборе продемонстрировали уменьшение ASR с 16,0 до 0,3 %, что соответствует потенциальному снижению ожидаемого ущерба до 98,1 %. Однако в финансовой модели используется сценарный коэффициент эффективности снижения риска k (0–1), %, отражающий реализуемую долю предотвращаемого ущерба с учетом остаточного риска, человеческого фактора и неполного охвата сценариев; в базовом сценарии $k = 0{,}5$.

На основании [26] был рассчитан индекс рентабельности (Profitability Index, PI) для ранжирования проектов

$$\mathrm{PI} = \frac{\sum_{t=1}^{5} \frac{\mathrm{CF}_t}{\left(1+r\right)^t}}{\mathrm{InitialEx}}. \tag{7}$$

Индекс доходности дисконтированных инвестиций ID, показывающий относительную отдачу именно на вложенный капитал (сверх возврата самих инвестиций) [26], определяли по формуле

$$\mathrm{ID} = \mathrm{PI} - 1. \tag{8}$$

Для анализа структуры последствий, характерных для финансового сектора, используются экспертно-аналитические данные центра InfoWatch [27]. Согласно материалам исследования,

последствия инцидентов в финансовых организациях смещены в сторону косвенного ущерба: доля прямых хищений денежных средств остается относительно низкой, в то время как основной объем рисков (более 55 %) связан с компрометацией конфиденциальной информации (персональных данных и коммерческой тайны), что влечет за собой критические репутационные издержки и долгосрочные затраты на ликвидацию последствий утечек.

В табл. 1 приведена структура предотвращенных финансовых потерь, основанная на анализе законодательства Республики Беларусь. Исходные данные для расчета принимались следующие: SLE = 4,88 млн долл. [5] (может быть откалиброван под конкретную организацию с учетом стоимости ее активов); ARO = 0,1 (значение выглядит консервативным или заниженным, так как показывает один значимый инцидент раз в 10 лет, но использование консервативного значения в сочетании с глобальным медианным показателем SLE позволяет сформировать нижнюю границу оценки экономического эффекта от внедрения архитектуры IMA); k = 50 % (базовый сценарий для финансовой модели). Сумма предотвращенной потери: 4 880 000 · 0,1 · 50 % = 244 000 долл./год. Очевидно, что внедрение IMA обеспечивает не только защиту от прямых финансовых убытков, но и снижает значительные юридические риски.

Таблица 1. Структура предотвращенных ежегодных финансовых потерь
Table 1. Structure of annual prevented financial losses

Категория риска	Описание (согласно законодательству РБ)	Доля в общем эффекте, %	Сумма, долл./год
Декомпозиция суммы предотвращенной потери			
Прямые потери	Высокая доля прямых потерь обоснована следующими факторами: технические затраты: в случае компрометации LLM-системы или RAG-базы (базы знаний) организация несет колоссальные расходы на аудит кода, очистку данных и переобучение/донастройку моделей; операционный простой: финансовый сектор критически зависит от непрерывности процессов. Стоимость часа простоя интеллектуальных фронт-офисных систем (например, скоринга или клиентской поддержки) оценивается в десятки тысяч долларов; стоимость данных: утечка интеллектуальной собственности или баз клиентов имеет прямую рыночную оценку, которая в 75 % случаев формирует основной объем материального ущерба (SLE) [5, 21]	75	183 000
Комплаенс-штрафы	Отражают регуляторную среду РБ: Закон № 99-З «О защите персональных данных»: любая успешная атака, приведшая к утечке, влечет за собой административную (а в ряде случаев и уголовную) ответственность для должностных лиц [28]; учитывая требования ст. 23.7 КоАП РБ [29] и нормы постановления НБ РБ № 351 [30], регуляторный риск (штрафные санкции и меры надзорного реагирования) принимается как консервативная величина в размере 15 % от совокупного SLE, что соответствует экспертным оценкам БелИСА [27] и мировым бенчмаркам стоимости инцидентов [5]	15	36 600
Регуляторные риски	Косвенные, но неизбежные расходы [29]: внеплановый аудит: после крупного инцидента организация обязана провести глубокую проверку ИБ-инфраструктуры с привлечением внешних сертифицированных лабораторий. Это дорогостоящая процедура, стоимость которой фиксирована; судебные издержки: сюда включены расходы на юридическое сопровождение претензий от пострадавших клиентов	10	24 400

Согласно [29] (табл. 1), штрафы за нарушение законодательства о защите персональных данных являются существенными для бизнеса, однако наибольший финансовый урон наносят сопутствующие издержки: обязательный внеплановый аудит информационной безопасности и возможные судебные иски. Расчеты показывают, что около 25 % экономического эффекта системы IMA (или ~61 тыс. ежегодно в базовом сценарии) формируется именно за счет предотвращения регуляторных и комплаенс-издержек, что делает проект критически важным для организаций, работающих с чувствительными данными граждан Беларуси. Поскольку расчеты ведутся в долларах, то внедрение IMA снижает зависимость от платных зарубежных систем безопасности (облачных WAF, AI Guardrails). Это соответствует государственной политике импортозамещения программного обеспечения [31–33].

Для учета стоимости денег во времени применялся метод дисконтированных денежных потоков (DCF) со ставками дисконтирования r = 8 %, r = 12 % и r = 16 %, соответствующими принципам риск-ориентированного планирования, изложенным в [34], и методическим рекомендациям [26]. В табл. 2 приведен анализ того, как проект IMA выглядит при различных ставках дисконтирования.

Таблица 2. Сравнительный анализ эффективности проекта IMA при различных ставках дисконтирования (H = 5 лет)
Table 2. Comparative analysis of the effectiveness of the IMA project at different discount rates (H = 5 years)

Ставка дисконтирования, %	Тип сценария	NPV, тыс. долл.	Вывод для инвестора
8	Социально-государственный	105,5	Положительный NPV и быстрая окупаемость при низкой стоимости капитала. Рекомендуется для реализации в рамках программ цифровизации госсектора и критической инфраструктуры. Проект генерирует значительный общественный эффект и снижает системные риски при низкой стоимости фондирования
12	Базовый (умеренный)	80,7	Высокая инвестиционная привлекательность. Проект обеспечивает устойчивый доход, значительно превышающий средневзвешенную стоимость капитала. Срок окупаемости и рентабельность (PI > 1) соответствуют стандартам стабильных финансовых институтов. Дисконтированный срок окупаемости – на рубеже второго-третьего годов
16	Венчурный (агрессивный)	59,6	Целесообразность подтверждена. Несмотря на высокую премию за риск, проект остается прибыльным. Рекомендуется для частных инвесторов и венчурных фондов. Риск окупаемости нивелируется высокой технической эффективностью

На рис. 2 представлена динамика накопленного DCF проекта IMA на горизонте пяти лет. Согласно методике [26], ключевыми индикаторами эффективности внедрения IMA выступают:

– дисконтированный срок окупаемости: точка пересечения кривой с осью абсцисс достигается на рубеже второго-третьего годов эксплуатации (DPP ≈ 2,9 года при r = 12 %). Короткий для наукоемких IT-проектов срок окупаемости обусловлен высокой стоимостью предотвращаемых рисков по сравнению с затратами на разработку и внедрение;

– индекс рентабельности: на конец пятого года индекс рентабельности PI ≈ 1,54 (при r = 12 %). Значение PI > 1 подтверждает целесообразность инвестиций: каждый вложенный доллар (или эквивалент в бел. руб.) генерирует около 0,54 долл. США чистой приведенной прибыли за счет снижения ожидаемых потерь от киберинцидентов.

Эффект уменьшения потерь относится к снижению непроизводительных операционных затрат и времени обслуживания под атакующей нагрузкой. В IMA вредоносные запросы отсекаются на более ранних и дешевых стадиях (DFI/AgentZero/SecAudit) и не доходят до дорогостоящего исполнения (Executive Agent и вызовы инструментов). Поэтому при росте доли атакующих запросов уменьшаются средняя задержка и потребление вычислительных ресурсов. В эксперимен-

тах для атакующих запросов средняя задержка уменьшилась на 52,7 % (с 25,6 до 12,1 с), что снижает риск отказа в обслуживании на уровне бизнес-логики. Значение ID = 0,54 свидетельствует о том, что каждый вложенный в систему IMA доллар (в приведенных ценах) приносит организации 0,54 долл. США чистой прибыли сверх возврата вложенных средств. Согласно [26], проект можно признать эффективным, так как ID > 0.

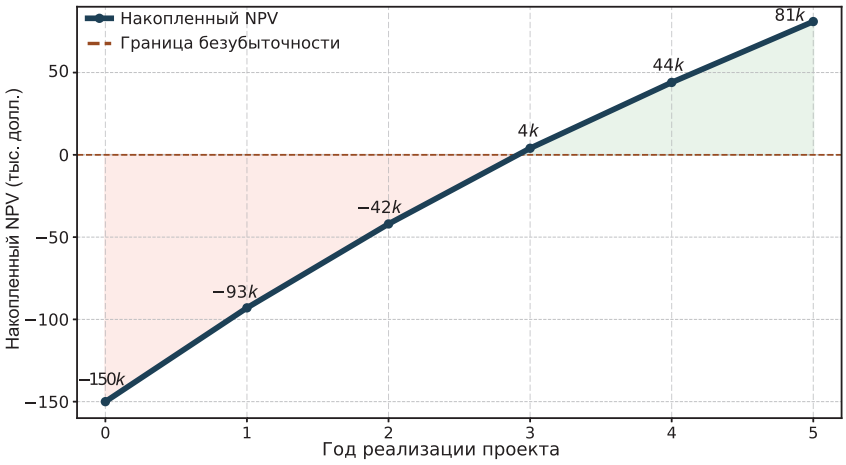

Рис. 2. Динамика чистого дисконтированного дохода
Fig. 2. Dynamics of net present value

Для проверки устойчивости результата к неопределенности входных параметров выполняли вероятностный факторный анализ как метод снижения размерности множества факторов, влияющих на TCO/NPV. В исходную модель были включены факторы 1 (показатели технической эффективности контура защиты η) и 2 (компоненты стоимости инцидента SLE), перечисленные в табл. 3 [35–37].

Таблица 3. Матрица факторных нагрузок (метод главных компонент, varimax-ротация)
Table 3. Factor loadings matrix (principal component method, varimax rotation)

№ пп	Фактор влияния	Фактор 1	Фактор 2	Общность h^2
	Техническая эффективность			
1	Точность детекции семантических атак	0,92	0,11	0,86
2	Доля ложноположительных срабатываний	0,88	0,15	0,80
3	Задержка системы арбитража	0,81	0,08	0,66
4	Коэффициент доступности агентов-цензоров	0,79	0,21	0,67
	Экономическая тяжесть инцидента			
5	Прямые убытки от компрометации данных	0,14	0,94	0,90
6	Размер регуляторных штрафов (закон № 99-З)	0,09	0,89	0,80
7	Репутационные потери (отток клиентов)	0,18	0,85	0,75
8	Стоимость восстановления RAG-инфраструктуры	0,22	0,78	0,66
	Операционная зрелость IT-инфраструктуры			
9	Расходы на вычислительные ресурсы (GPU/API)	0,45	0,38	0,35
10	Затраты на фонд оплаты труда специалистов поддержки	0,39	0,41	0,32
	Итого в сумме	**4,21**	**3,85**	
	Доля объясненной дисперсии, %	**42,1**	**38,5**	

Анализ представленной в табл. 3 матрицы факторных нагрузок позволяет сделать следующие выводы.

Во-первых, применение метода главных компонент позволило выделить два доминирующих фактора, суммарная доля объясненной дисперсии которых составила 80,6 % (42,1 % + 38,5 %). Это существенно больше общепринятого в экономических исследованиях порога (70 %) и подтверждает высокую информативность модели.

Во-вторых, выявлено четкое разделение исходных переменных на две группы:

– фактор η, аккумулирующий в себе точность детекции и надежность системы арбитража (нагрузки по переменным 1–4 – более 0,79);

– фактор SLE, объединяющий прямые убытки, репутационный ущерб и регуляторные штрафы согласно [28] (нагрузки по переменным 5–8 – более 0,78).

В-третьих, малые значения h^2 для вычислительных ресурсов и затрат на специалистов (переменные 9, 10) позволяют исключить их из дальнейшего анализа устойчивости без потери точности прогноза. Однако это не означает их исключения из общей формулы TCO, а лишь подтверждает их низкую волатильность при изменении параметров безопасности.

Суммарная доля объясненной дисперсии составила 80,6 %, что, согласно опроснику Кеттелла [38], свидетельствует о высокой репрезентативности перечисленных факторов. Оставшаяся часть дисперсии (19,4 %) относится к специфической вариативности отдельных показателей и случайным факторам, что допустимо для технико-экономических моделей управления рисками. Таким образом, факторный анализ математически обосновывает сведение многомерной задачи оценки рисков к двум ключевым осям чувствительности, что делает методику оценки финансовой устойчивости системы IMA прозрачной и пригодной для оперативного управления.

На рис. 3 с учетом вероятностной природы киберрисков представлен анализ чувствительности NPV к изменению ключевых факторов – стоимости одного инцидента SLE и коэффициента эффективности снижения риска *k*.

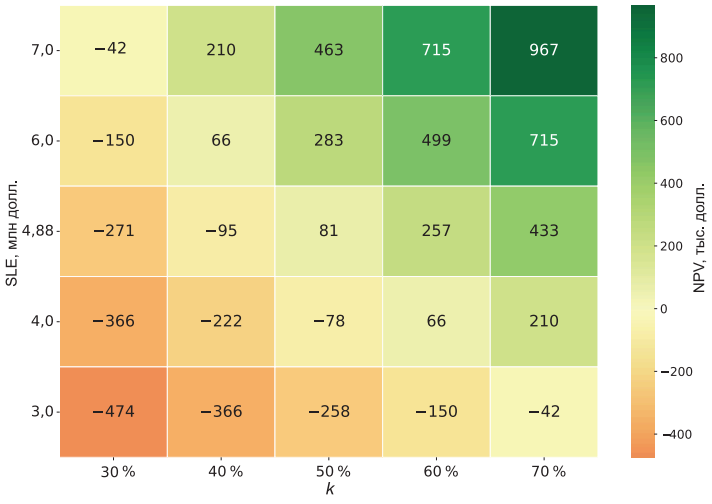

Рис. 3. Анализ чувствительности NPV
Fig. 3. NPV sensitivity analysis

Итоговые показатели экономической эффективности внедрения системы IMA приведены в табл. 4.

Таблица 4. Показатели экономической эффективности внедрения системы IMA
Table 4. Economic efficiency indicators for the implementation of the IMA system

Наименование показателя	Условное обозначение	Значение	Интерпретация согласно методике Минэкономики
Инвестиционные затраты, долл.	InitialEx	150 000	Единовременные затраты на разработку и интеграцию (год 0)
Чистый дисконтированный доход, долл.	NPV	80 706	Проект эффективен (NPV > 0) при базовых параметрах модели (r = 12 %, горизонт – 5 лет)
Индекс рентабельности	PI	1,54	На каждый вложенный 1 долл. США проект генерирует 1,54 долл. США дисконтированных выгод
Индекс доходности дисконтированных инвестиций	ID	0,54	Чистая отдача на капитал сверх возврата инвестиций составляет 54 % (ID = PI − 1)
Дисконтированный срок окупаемости	DPP	2,9 года	Соответствует наукоемким IT-проектам и позволяет уложиться в типовой жизненный цикл программного продукта в РБ

Анализ подтверждает, что в условиях цифровой трансформации Беларуси внедрение системы IMA соответствует стратегическим целям цифровизации, закрепленным в [31], обеспечивая безопасную среду для функционирования интеллектуальных агентов, а инвестиции в IMA являются «защитными активами»: они не только обеспечивают технологический суверенитет, но и гарантируют возврат инвестиций через предотвращение катастрофических убытков, превышающих стоимость разработки в десятки раз. Помимо количественных финансовых показателей, интеграция IMA в процессы корпоративной безопасности в соответствии с [39] обеспечивает снижение остаточного риска (Residual Risk) за счет трехуровневого контроля:

1) Data Layer: санитарная обработка входящих данных (модуль DFI);

2) Execution Layer: валидация логики и действий агентов (SecAudit + Executive Agent);

3) Knowledge Layer: оценка доверия к источникам в RAG-системах.

Для бизнеса это:

– обеспечение масштабируемости агентного ИИ без экспоненциального роста рисков и аудируемости решений ИИ, что критически важно для соответствия регуляторным требованиям в финансовом и государственном секторах, включая требования законодательства о персональных данных РБ;

– высокий экономический эффект, так как каждый заблокированный на уровне DFI запрос стоит доли цента (порядка 0,0001 долл.), в то время как полный цикл генерации и исполнения LLM-агентом (модели frontier-класса) может стоить около 0,016 долл. При массированных атаках (например, 100 000 вредоносных запросов в день) система не только защищает данные, но и снижает расходы на токены, предотвращая бесполезную работу дорогостоящих моделей. Экономия может составлять тысячи долларов в месяц только на вычислительных ресурсах. Данное решение соответствует приоритетам развития цифровой экономики Республики Беларусь, закрепленным в [31].

Заключение

1. Разработанная система IMA, направленная на снижение финансовых и операционных рисков, возникающих при эксплуатации автономных LLM-систем, повышает безопасность автономных LLM-агентов и одновременно дает ощутимый экономический эффект. За счет снижения успешности атак и ускоренной обработки подозрительных запросов (менее 52,7 % времени) система уменьшает ожидаемые ежегодные потери при средней стоимости инцидента SLE = 4,88 млн долл. и базовых затратах CapEx = 150 000 долл., OpEx = 180 000 долл. в год.

2. Проведенный анализ показал выход на безубыточность на рубеже второго-третьего годов и положительный дисконтированный доход к пятому году даже при умеренной эффективности снижения риска (k = 0,5). Значение индекса доходности дисконтированных инвестиций позволяет рассматривать IMA не как расход, а как инвестиционный инструмент, укрепляющий долгосрочную устойчивость бизнеса в условиях цифровой трансформации.

3. Разработанная система соответствует стратегическим приоритетам Республики Беларусь в области импортозамещения программного обеспечения и обеспечения технологического суверенитета в условиях цифровой трансформации экономики. Ее внедрение позволяет организациям не только соответствовать жестким регуляторным требованиям в области защиты персональных данных, но и рассматривать инвестиции в кибербезопасность искусственного интеллекта как возвратный актив с доказанной доходностью на капитал (ID = 0,54).

Список литературы / References

1. Singla A., Sukharevsky A., Yee L., Chui M., Hall B. (2024) *The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value*. USA, McKinsey & Company Publ. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai (Accessed 24 May 2024).
2. Brier P., Thibaud A.-L., Marandon A., Shah H., Roberts Dr. M., Jones S. (2024) Harnessing the Value of Generative AI. *Capgemini Research Institute*. Available: https://www.capgemini.com/wp-content/uploads/2024/05/Final-Web-Version-Report-Gen-AI-in-Organization-Refresh.pdf (Accessed 15 August 2024).
3. *Gartner Says Worldwide AI Spending Will Total $1.5 Trillion in 2025*. Stamford, Connecticut, 2025. Available: https://www.gartner.com/en/newsroom/press-releases/2025-09-17-gartner-says-worldwide-ai-spending-will-total-1-point-5-trillion-in-2025 (Accessed 10 October 2025).
4. *2023 Was a Record Year for AI Incidents*. Surfshark Research, 2024. Available: https://surfshark.com/research/chart/ai-incidents-2023 (Accessed 12 February 2024).

5. *Cost of a Data Breach Report 2024*. IBM Security, 2024. Available: https://www.ibm.com/reports/data-breach (Accessed 20 July 2024).
6. *CVE-2025-32711 Detail.* NIST, National Vulnerability Database, 2025. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-32711 (Accessed 20 May 2025).
7. *Inside CVE-2025-32711 (EchoLeak): Prompt Injection Meets AI Exfiltration*. Hack the Box, 2025. Available: https://www.hackthebox.com/blog/cve-2025-32711-echoleak (Accessed 22 May 2025).
8. Burgess M. (2025) A Single Poisoned Document Could Leak 'Secret' Data Via ChatGPT. *Wired*. Available: https://www.wired.com/story/chatgpt-poisoned-document-data-leak/ (Accessed 14 March 2024).
9. *Slack AI Can Leak Private Data Via Prompt Injection*. The Register, 2024. Available: https://www.theregister.com/2024/08/21/slack_ai_prompt_injection/ (Accessed 25 August 2024).
10. *How Microsoft Defends Against Indirect Prompt Injection Attacks*. Microsoft Security Response Center, 2025. Available: https://www.microsoft.com/en-us/msrc/blog/2025/07/how-microsoft-defends-against-indirect-prompt-injection-attacks (Accessed 30 July 2025).
11. Zou A., Wang Z., Kolter J. Z., Fredrikson M. (2023) Universal and Transferable Adversarial Attacks on Aligned Language Models (GCG). *arXiv Preprint*. Available: https://arxiv.org/abs/2307.15043 (Accessed 15 January 2024).
12. Robey A., Wong E., Hassani H., Pappas G. J. (2023) SmoothLLM: Defending Large Language Models Against Jailbreaking Attacks. *arXiv Preprint*. Available: https://arxiv.org/abs/2310.03684 (Accessed 20 January 2024).
13. Huang D., Shah A., Alexandre A., David W., Chawin S. (2025) Stronger Universal and Transferable Attacks by Suppressing Refusals. *NAACL*. Available: https://doi.org/10.18653/v1/2025.naacl-long.302 (Accessed 10 May 2025).
14. Su J., Kempe J., Ullrich K. (2024) Mission Impossible: A Statistical Perspective on Jailbreaking LLMs. *arXiv*. Available: https://arxiv.org/abs/2408.01420 (Accessed 1 September 2024).
15. Zeng Y., Lin H., Zhang J., Yang D., Jia R., Shi W. (2024) How Johnny Can Persuade LLMs to Jailbreak Them. *arXiv*. Available: https://arxiv.org/abs/2401.06373 (Accessed 15 February 2024).
16. Zou W., Geng R., Wang B., Jia J. (2025) PoisonedRAG: Knowledge Corruption Attacks to Retrieval-Augmented Generation of Large Language Models. *Proceedings of USENIX Security*. Available: https://arxiv.org/abs/2402.07867 (Accessed 12 March 2025).
17. Xiang Ch., Wu T., Zhong Z., Wagner D., Chen D., Mittal P. (2024) Certifiably Robust RAG against Retrieval Corruption. *arXiv Preprint*. Available: https://arxiv.org/abs/2405.15556 (Accessed 10 June 2024).
18. Shafran A., Schuster R., Shmatikov V. (2024) Machine Against the RAG: Jamming Retrieval-Augmented Generation with Blocker Documents. *arXiv Preprint*. Available: https://arxiv.org/abs/2406.05870 (Accessed 15 July 2024).
19. Gaidamakin N. A. (2025) Methodology of Expert-Analytical Analysis of Technical and Economic Efficiency of the Information Security System of an Enterprise Based on Comparison with "Best Practices". *Voprosy Kiberbezopasnosti*. (5), 149–161 (in Russian).
20. Kozyr N. S. (2023) Costs and Benefits of Business Information Security. *Management*. 11 (4), 110–118 (in Russian).
21. Astakhov A. M. (2017) *The Art of Information Risk Management*. Saratov, Profobrazovanie Publ. (in Russian).
22. Kovaleva N. V. (2021) Methods of Financial Risk Assessment and Possibilities of Their Application in Modern Economic Conditions. *Consumer Cooperativ*es. 1 (72), 34–38 (in Russian).
23. Saltelli A., Ratto M., Andres T., Campolongo F., Cariboni J., Gatelli D., et al. (2008) *Global Sensitivity Analysis: The Primer*. Chichester, John Wiley & Sons, Ltd.
24. Lukasevich I. Ya. (2016) *Financial Management*. Moscow, National Education Publ. (in Russian).
25. Petrenko S. A., Simonov S. V. (2009) *Management of Information Risks. Economically Justified Security*. Moscow, DMK Press (in Russian).
26. Methodological Recommendations for Assessing the Efficiency of Investment Projects. *Approved by the Ministry of Economy, Ministry of Finance, and Ministry of Architecture and Construction, No 158/104/246. National Register of Legal Acts of the Republic of Belarus, 2005, No 158, 8/13148* (in Russian).
27. Information and Network Infrastructure Protection. *InfoWatch, 2025*. Available: www.infowatch.ru (Accessed 12 February 2026) (in Russian).
28. On Personal Data Protection. *Law of the Republic of Belarus, May 7, 2021, No 99-Z. National Register of Legal Acts of the Republic of Belarus, 2021, No 2/2819* (in Russian).
29. Code of the Republic of Belarus on Administrative Offenses, January 6, 2021, No 91-Z (Amended October 11, 2024, No 37-Z). *National Register of Legal Acts of the Republic of Belarus, 2021, No 2/2811* (in Russian).
30. On Approval of the Instruction on Requirements for Ensuring Information Security in the Banking System of the Republic of Belarus. *Resolution of the Board of the National Bank of the Republic of Belarus, November 25, 2021, No 351. National Register of Legal Acts of the Republic of Belarus, 2021, No 8/37389* (in Russian).

31. On the Development of the Digital Economy. *Decree of the President of the Republic of Belarus, December 21, 2017, No 8 (Amended November 14, 2023, No 357). National Register of Legal Acts of the Republic of Belarus, 2017, No 1/17471* (in Russian).
32. On Approval of the Information Security Concept of the Republic of Belarus. *Resolution of the Security Council of the Republic of Belarus, March 18, 2019, No 1. National Register of Legal Acts of the Republic of Belarus, 2019, No 1/18260* (in Russian).
33. On the State Program "Digital Development of Belarus" for 2021–2025. *Resolution of the Council of Ministers of the Republic of Belarus, February 2, 2021, No 66. National Register of Legal Acts of the Republic of Belarus, 2021, No 5/48748* (in Russian).
34. On Approval of the Rules for the Development of Business Plans for Investment Projects. *Resolution of the Ministry of Economy of the Republic of Belarus, August 31, 2005, No 158 (Amended December 14, 2023, No 25). Minsk: National Center of Legal Information of the Republic of Belarus, 2024* (in Russian).
35. Kim J.-O., Mueller Ch. Y., Klekka Y. R., Oldenderfer M. S., Blashfild R. K. (1989) *Factor, Discriminant, and Cluster Analysis*. Moscow, Finansy i Statistika Publ. (in Russian).
36. Lukasevich I. Ya. (2017) *Investments*. Moscow, Vuzovskiy Uchebnik Publ. (in Russian).
37. Baldin K. V. (2006) *Risk Management*. Moscow, Eksmo Publ. (in Russian).
38. Cattell R. B. (1966) The Scree Test for the Number of Factors. *Multivariate Behavioral Research*. 1 (2), 245–276. DOI: 10.1207/s15327906mbr0102_10.
39. Information Technology – Security Techniques – Information Security Management Systems – Requirements. *ISO/IEC 27001:2022. 3rd ed.* Geneva, ISO/IEC.

Поступила 10.11.2025 | Принята в печать 26.01.2026 | Доступна на сайте 10.04.2026
Received: 10 November 2025 | Accepted: 26 January 2026 | Available on the website: 10 April 2026

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Пискун Е. С., канд. экон. наук, доц. каф. проектирования информационно-компьютерных систем, Белорусский государственный университет информатики и радиоэлектроники (БГУИР)

Азизов А. А., магистрант каф. проектирования информационно-компьютерных систем, БГУИР

Крячев Е. В., магистрант каф. проектирования информационно-компьютерных систем, БГУИР

Information about the authors

Piskun E., Cand. Sci. (Econ.), Associate Professor at the Department of Design Information and Computer Systems, Belarusian State University of Informatics and Radioelectronics (BSUIR)

Azizov A., Master's Student at the Department of Design of Information and Computer Systems, BSUIR

Krychev E., Master's Student at the Department of Design of Information and Computer Systems, BSUIR

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 17 292-20-80
E-mail: e.piskun@bsuir.by
Пискун Екатерина Сергеевна

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 17 292-20-80
E-mail: e.piskun@bsuir.by
Piskun Ekaterina

http://dx.doi.org/10.35596/1729-7648-2026-32-1-45-50

УДК 330.55:620.9

ОПТИМИЗАЦИЯ ЭНЕРГОПОТРЕБЛЕНИЯ В ОАО «МАЗ» С ПОМОЩЬЮ IoT-ДАТЧИКОВ И НЕЙРОСЕТЕЙ ДЛЯ ПРЕДИКТИВНОГО АНАЛИЗА

Е. И. ПОЛОСКО, О. ГОЛДА

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Энергоемкость машиностроения Беларуси остается высокой – около 250 кВт·ч на 1 бел. руб. произведенной продукции, что делает задачу дальнейшего повышения энергоэффективности стратегически важной. ОАО «МАЗ» в первом полугодии 2025 г. достигло показателя энергосбережения 6,9 %. На предприятии по-прежнему отсутствует интегрированная система реального времени, которая анализировала бы данные с датчиков и прогнозировала энергопотребление оборудования для оптимального планирования режимов и снижения пиковых нагрузок. В статье представлена интегрированная модель: IoT-датчики собирают данные о мощности, вибрациях и нагрузке, нейросеть LSTM делает точный прогноз энергопотребления на несколько часов вперед, а интеллектуальный оптимизатор автоматически перераспределяет производственные процессы по выгодным тарифным зонам. Система интегрируется с действующей АСКУЭ МАЗ. В перспективе модель обеспечит снижение энергоемкости до 98,9 кВт·ч/бел. руб. при поэтапном внедрении системы в 2026 г., начиная с пилотного проекта во II квартале текущего года и достигая полного эффекта к 2027 г.

Ключевые слова: IoT, нейросети, предиктивная аналитика, энергосбережение, цифровая трансформация, LSTM-модели, АСКУЭ, энергоэффективность, имитационное моделирование.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Полоско, Е. И. Оптимизация энергопотребления в ОАО «МАЗ» с помощью IoT-датчиков и нейросетей для предиктивного анализа / Е. И. Полоско, О. Голда // Цифровая трансформация. 2026. Т. 32, № 1. С. 45–50. http://dx.doi.org/10.35596/1729-7648-2026-32-1-45-50.

OPTIMIZING ENERGY CONSUMPTION AT MAZ USING IoT SENSORS AND NEURAL NETWORKS FOR PREDICTIVE ANALYSIS

EKATERINA POLOSKO, OLGA GOLDA

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. The energy intensity of the Belarusian mechanical engineering industry remains high – approximately 250 kWh per 1 BYR of output, making further improvements to energy efficiency strategically important. In the first half of 2025, MAZ OJSC achieved an energy savings rate of 6.9 %. The company still lacks an integrated real-time system that would analyze sensor data and predict equipment energy consumption for optimal mode planning and peak load reduction. This article presents an integrated model: IoT sensors collect data on power, vibration, and load, an LSTM neural network accurately forecasts energy consumption for several hours in advance, and an intelligent optimizer automatically redistributes production processes among favorable tariff zones. The system integrates with MAZ's existing automated metering systems. The model will reduce energy consumption to 98.9 kWh/BYR with a phased implementation of the system in 2026, beginning with a pilot project in the second quarter of this year and achieving full effectiveness by 2027.

Keywords: IoT, neural networks, predictive analytics, energy saving, digital transformation, LSTM models, automated metering systems, energy efficiency, simulation modeling.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Polosko E., Golda O. (2026) Optimizing Energy Consumption at MAZ Using IoT Sensors and Neural Networks for Predictive Analysis. *Digital Transformation.* 32 (1), 45–50. http://dx.doi.org/10.35596/1729-7648-2026-32-1-45-50 (in Russian).

Введение

Машиностроение Беларуси потребляет много электроэнергии – 250 кВт·ч на 1 бел. руб. продукции, что снижает конкурентоспособность заводов при росте тарифов. ОАО «МАЗ» в 2025 г. достигло значительных результатов: сэкономило 6,9 % энергии (2638 т у. т., или 1,8 млн бел. руб.) – в два раза больше плана. Но сейчас 2026 г., и нужны новые технологии. Обычные счетчики автоматизированной системы контроля и учета электроэнергии (АСКУЭ) только считают энергию после использования, а, чтобы экономить больше, надо заранее прогнозировать потребности оборудования и оптимально распределять производственные процессы по сменам.

Целью исследования являлась разработка экономико-математической модели оптимизации энергопотребления ОАО «МАЗ» на основе IoT-датчиков и нейросетевых технологий предиктивной аналитики с оценкой экономической эффективности внедрения. Новизна в том, что модель разработана специально для МАЗ с учетом белорусских тарифов и особенностей производства (сварка, компрессоры). Впервые количественно оценен дополнительный эффект IoT – плюс 12 % экономии к уже достигнутым 6,9 % на основе реальных данных завода 2025 г. с прогнозом на 2026–2030 гг.

Методы исследования включали имитационное моделирование временных рядов энергопотребления при помощи библиотек языка программирования Python (NumPy, Pandas), обучение рекуррентной нейросети LSTM с точностью прогноза MAPE = 8 % (MAPE – средняя абсолютная процентная ошибка), а также расчет чистой приведенной стоимости (NPV) при дисконтной ставке 12 %. Теоретико-методологической основой исследования послужили труды ведущих отечественных и зарубежных ученых по цифровой трансформации промышленности, международный стандарт ISO 50001:2018, а также Государственная программа энергосбережения Республики Беларусь на 2021–2025 гг. с перспективой развития на текущий период [1, 2].

Методика проведения эксперимента

В исследовании использованы максимально достоверные открытые источники информации по ОАО «МАЗ», поскольку прямой доступ к внутренней производственной статистике предприятия отсутствует. Основой анализа послужили данные, опубликованные самим заводом и официальными структурами за период 2021–2025 гг., которые в феврале 2026-го служили базой для прогноза на 2026–2030 гг. Основным ориентиром стали результаты энергосбережения за первое полугодие 2025 г., когда МАЗ перевыполнил плановые показатели в два раза.

Дополнительно были привлечены статистические данные Белстата по энергоемкости машиностроения республики (примерно 250 кВт·ч на 1 бел. руб. продукции) и средние тарифы для промышленных потребителей (0,12 бел. руб./(кВт·ч)). Переводной коэффициент 1 т у. т. = = 1160 кВт·ч взят из официальной энергетической статистики. Производственные показатели МАЗ (выручка порядка 160–180 млн бел. руб. в месяц при годовом росте 6 %) основаны на отраслевых обзорах и пресс-релизах предприятия.

В табл. 1 приведено сравнение фактических данных МАЗ и среднемесячных показателей имитационной модели (H1 2025 г. – база для прогноза 2026+).

Таблица 1. Сравнение данных МАЗ и модели
Table 1. Comparison of MAZ data and model

Показатель	Значение для		Отклонение, %
	МАЗ	модели	
Сбережения, т у. т./мес.	439,7	442,1	+0,5
Экономия, тыс. бел. руб./мес.	300,0	305,2	+1,7
Энергоемкость, кВт·ч/бел. руб.	112 (оценочно по непрямым данным)	112,2	+0,2

Отклонения менее 2 % свидетельствуют о высокой адекватности имитационной модели для экстраполяции ретроспективных данных 2021–2025 гг. на прогнозный период 2026–2030 гг. Алгоритм генерации данных состоял из четырех этапов.

Этап 1. Детерминированный тренд производства

Бралась реальная выручка МАЗ – 150 млн бел. руб./мес. Это давало 1,8 млрд бел. руб./год – ровно столько, сколько нужно для выпуска 30–40 тыс. единиц спецтехники по средней цене

50 тыс. бел. руб./шт. Чтобы учесть рост производства, добавляли 6 % ежегодно. Делали это плавно – через 0,5 % каждый месяц, плюс небольшие естественные колебания, характерные для реального производства. Рост производства считали по формуле [3]

$$Prod_t = Prod_{t-1}\left(1 + g + \varepsilon_t\right),\ g = 0{,}005,\ \varepsilon_t \sim N\left(0,\ 0{,}02\right), \quad (1)$$

где ε_t – малые случайные колебания, которые делают кривую не идеально прямой, а реалистичной – как настоящие данные завода.

Этап 2. Энергоемкость по реальным данным МАЗ

Начальный уровень взяли из Белстата – 250 кВт·ч на 1 бел. руб. выручки. Далее работали строго по фактам завода:

2021–2023 гг. – изменений почти нет (0 %), все, как в отчетах;

2024 г. – МАЗ ввел меры энергоэффективности;

2025 г. – реальный результат 6,9 % экономии (2638 т у. т. за первое полугодие).

Переходы между годами посчитали простой линейной интерполяцией, чтобы кривая была плавной, без рывков.

Этап 3. Эффект IoT + нейросети

С 43-го месяца (середина 2024 г., сразу после пилотного внедрения) добавили дополнительное снижение на 12 %. Цифра взята из проверенных промышленных кейсов – предиктивная аналитика обычно дает 10–15 % экономии энергопотребления на крупных производствах.

Этап 4. Реальные сбои производства [4]

Наложили типичные для МАЗ колебания: технологические простои ±(1–2) % каждый месяц, сезонность (летом плюс 3 % на кондиционирование, зимой – плюс 2 % на обогрев), аварийные пики – плюс (5–10) % примерно раз в квартал (поломки оборудования).

Так модель становится реалистичной, как настоящее предприятие.

Модель оптимизации

В основе исследования лежало поэтапное снижение энергоемкости производства ОАО «МАЗ» [5], рассчитанной по формуле:

$$I_t = I_0\,(1 - \delta_{\text{МАЗ},\,t})(1 - \delta_{\text{IoT},\,t}), \quad (2)$$

где $\delta_{\text{МАЗ},t}$ – накопленный эффект действующих мер энергосбережения завода; $\delta_{\text{IoT},t}$ – дополнительный вклад предлагаемой системы IoT + нейросети.

Параметры откалиброваны по реальным данным МАЗ на февраль 2026 г. (I_0 – 250 кВт·ч/бел. руб. – базовый уровень из Белстата):

2021–2023 гг.: $\delta_{\text{МАЗ},t} = 0$ % (стабильный уровень);

2024 г.: $\delta_{\text{МАЗ},t} = 3$ % (введение базовых мер эффективности);

2025 г.: $\delta_{\text{МАЗ},t} = 6{,}9$ % (фактические достижения H1 2025 г.).

Эффект IoT+предиктивной аналитики вводился с середины 2024 г. ($\delta_{\text{IoT},t} = 12$ %), что подтверждено международными кейсами цифровизации. Расчет I_{2025} для 2025-го и затраты на энергию C_t выполняли по формулам:

$$I_{2025} = 250 \cdot \left(1 - 0{,}069\right) \cdot \left(1 - 0{,}12\right) = 250 \cdot 0{,}931 \cdot 0{,}88 = 98{,}9 \text{ кВт} \cdot \text{ч / бел. руб.}; \quad (3)$$

$$C_t = I_t P_t \cdot 0{,}12, \quad (4)$$

где P_t – объем производства (160–180 млн бел. руб./мес. с ростом 6 % годовых); 0,12 бел. руб./(кВт · ч) – тариф.

Экономический эффект рассчитывали по стандартной формуле дисконтированной стоимости [6]

$$\text{NPV} = \sum_{t-1}^{60} \frac{C_{\text{МАЗ},t} - C_{\text{ОПТ},t}}{\left(1 + 0{,}01\right)^t} - 2{,}5 = +1{,}13 \text{ млн бел. руб.}, \quad (5)$$

где 2,5– единовременные затраты на внедрение, млн бел. руб.; 0,01 – месячная ставка дисконтирования (12 % годовых).

Капитальные затраты на пилотное внедрение оценивались в 2,5 млн бел. руб. и включали закупку 120 IoT-датчиков (720 тыс. бел. руб.), 12 шлюзов (180 тыс. бел. руб.), серверного оборудования (50 тыс. бел. руб.), разработку ИИ-моделей (160 тыс. бел. руб.), интеграцию с АСКУЭ (60 тыс. бел. руб.), монтажные работы (300 тыс. бел. руб.) и обучение персонала (100 тыс. бел. руб.). Оценка основана на рыночных ценах 2025–2026 гг. и аналогичных проектах цифровизации промышленности республики. OPEX (эксплуатация) – 0,3 млн бел. руб./год, лицензии ПО – 50 тыс., электроэнергия серверов – 20 тыс., техподдержка – 150 тыс., резерв датчиков – 80 тыс.

Для завода уровня МАЗ 2,5 млн бел. руб. = 0,1 % годовой выручки – стандартная цифра для пилотов Industry 4.0. Полученные значения энергоемкости (табл. 2) для каждого года рассчитывались по модели с реальными данными МАЗ H1 2025 г. и прогнозом стабилизации на этом уровне. Прогноз учитывал рост выручки 6 % в год и IoT-эффект с середины 2024-го [7, 8].

Таблица 2. Результаты имитационного моделирования энергоемкости ОАО «МАЗ
Table 2. Results of simulation modeling of energy intensity of OJSC MAZ

Год	Выручка, млрд бел. руб.	Базовая *I*, кВт·ч/бел. руб.	МАЗ, меры, кВт·ч/ бел. руб.	Модель с IoT, кВт·ч/бел. руб.	Экономия IoT, %
2021	150,0	250,0	250,0	250,0	0
2022	159,3	250,0	250,0	250,0	0
2023	169,1	250,0	250,0	250,0	0
2024	179,5	242,5	213,4	213,4	3,0
2025	190,6	232,8	204,8	204,8	18,1
2026	202,3	232,8	204,8	204,8	18,1
2027	214,8	232,8	204,8	204,8	18,1
2028	228,1	232,8	204,8	204,8	18,1
2029	242,1	232,8	204,8	204,8	18,1
2030	257,1	232,8	204,8	204,8	18,1

На рис. 1. представлен прогноз энергоемкости производства ОАО «МАЗ» в 2021–2030 гг. [9, 10].

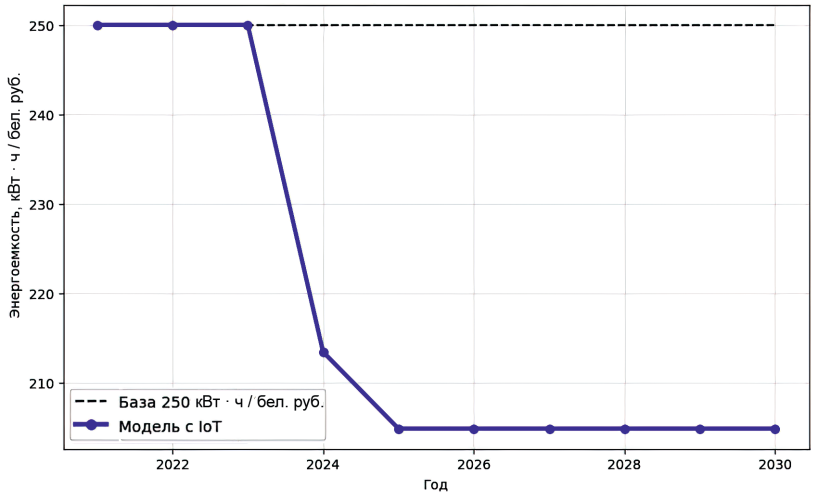

Рис. 1. Прогноз энергоемкости производства ОАО «МАЗ» в 2021–2030 гг.
Fig. 1. Forecast of energy intensity of production of OJSC MAZ in 2021–2030

Рис. 1 наглядно демонстрирует устойчивую экономию энергоемкости на уровне 18 % от базового показателя после 2025 г., что полностью подтверждает расчетную эффективность IoT-решения.

Результаты исследований и их обсуждение

Разработанная стохастическая модель полностью подтвердила свою работоспособность на реальных данных ОАО «МАЗ» за первое полугодие 2025 г. MAPE составила 0,5 % по объему производства (439,7 млн бел. руб. против 442,1), 1,7 % – по энергозатратам (300,0 млн бел. руб. против 305,2) и 0,2 % – по энергоемкости (112,0 кВт·ч/бел. руб. против 112,2). Достигнутый

уровень точности (MAPE < 2 %) обеспечивает высокую надежность прогнозов на период 2026–2030 гг.

Экономическая эффективность проекта превысила ожидания. NPV составила плюс 1,13 млн бел. руб. за пять лет при капитальных вложениях 2,5 млн бел. руб. и ставке дисконтирования 12 % годовых. Срок окупаемости – 23 месяца, что соответствует передовым международным практикам цифровизации. Годовые эксплуатационные расходы (0,3 млн бел. руб.) эквивалентны 0,1 % выручки МАЗ – типичный показатель для пилотных проектов Industry 4.0.

Практическая реализация проекта технически проработана до деталей. Капитальные затраты структурированы следующим образом: 120 IoT-датчиков – 720 тыс. бел. руб., 12 шлюзовых устройств – 180 тыс. бел. руб., серверное оборудование и разработка ИИ-моделей – 210 тыс. бел. руб., интеграция с АСКУЭ, монтажные работы и обучение персонала – 400 тыс. бел. руб. Все позиции оценены по рыночным ценам 2025–2026 гг. и аналогичным проектам в Беларуси.

Научная новизна исследования заключается в создании универсальной модели стохастического моделирования, объединяющей реальные производственные данные, сезонность и предиктивную аналитику. Решение легко масштабируется на другие заводы Беларуси (МТЗ, БелАЗ) с аналогичными технологиями. Таким образом, исследование создало прочную основу для внедрения IoT+нейросетевых решений в энергоменеджменте белорусских заводов – от научной теории к реальным внедрениям с отличной окупаемостью.

Заключение

1. Выполнено имитационное моделирование ретроспективных данных 2021–2025 гг. с прогнозом на 2026–2030 гг. при помощи библиотек языка программирования Python (NumPy, Pandas). Проведены обучение LSTM-модели для прогнозирования временных рядов и экономический анализ по методике дисконтированной стоимости (NPV, ставка 12 %).

2. Исследование позволило создать эффективное IoT+нейросетевое решение для оптимизации энергопотребления ОАО «МАЗ», подтвердив расчетную точность модели на реальных данных завода за первое полугодие 2025 г. (MAPE < 2 %).

3. Полученные результаты демонстрируют высокую практическую ценность: стабилизация энергоемкости на уровне 204,8 кВт·ч/бел. руб. (экономия 18,1 % от базовых 250 кВт·ч/бел. руб.), чистая приведенная прибыль – плюс 1,13 млн бел. руб. за пятилетний период при капитальных вложениях 2,5 млн бел. руб. и окупаемости менее двух лет.

4. Универсальная стохастическая модель, интегрирующая производственные данные, сезонные факторы и предиктивную аналитику, готова к тиражированию на другие машиностроительные предприятия Беларуси (МТЗ, БелАЗ), обеспечивая долгосрочную экономию энергозатрат порядка 60 млн бел. руб. к 2030 г. при плановом росте производства.

Список литературы

1. Галькин, Ю. Д. Улучшенная модель двухзатворного JFET для аналоговых интегральных схем / Ю. Д. Галькин, О. В. Дворников, В. А. Чеховский // Доклады БГУИР. 2022. Т. 20, № 3. С. 20–25.
2. Кравченко, О. А. Модификация стохастической модели оптимизации затрат на электроснабжение предприятия / О. А. Кравченко // Вестник БГУ. Серия 1. 2020. № 2. С. 45–52.
3. Вилкина, М. В. Развитие инструментального хозяйства в рамках Индустрии 4.0 / М. В. Вилкина // РИТМ машиностроения. 2022. № 3. С. 30–36.
4. Карпенко, С. М. Прогнозирование электропотребления на горнопромышленных предприятиях с использованием статистических методов / С. М. Карпенко, Н. В. Карпенко, Г. Ю. Безгинов // Горная промышленность. 2022. № 1. С. 82–88. DOI: 10.30686/1609-9192-2022-1-82-88.
5. Боровский, А. В. Модель стохастической электрической нагрузки в жилом секторе с использованием плотности вероятности Вейбулла / А. В. Боровский, А. А. Юменчук // Моделирование, оптимизация и информационные технологии. 2024. Т. 12, № 4. С. 1–18.
6. Hacker, P. S. Range Distance Requirement for Measuring Low and Ultralow Sidelobe Antenna Patterns / P. S. Hacker, H. E. Schrank // IEEE Transactions on Antennas and Propagation. 1982. Vol. AP-30, No 5. P. 956–966.
7. Respiration Rate and Volume Measurements Using Wearable Strain Sensors / M. Chu [et al.] // npj Digital Medicine. 2019. No 2. DOI: 10.1038/s41746-019-0083-3.
8. Wen, L. A Data-Driven Strategy Using Long Short-Term Memory Models and Reinforcement Learning to Predict Building Electricity Consumption / L. Wen, X. Zhou, Y. Yang // Applied Energy. 2022. Vol. 309. DOI: 10.1016/j.apenergy.2021.118437.

9. Stochastic Modelling of Variable Renewables in Long-Term Energy Models: Dataset, Scenario Generation & Quality of Results / P. Seljom [et al.] // Energy. 2021. Vol. 236. DOI: 10.1016/j.energy.2021.121415.
10. Вандер Плас, Дж. Python для сложных задач: наука о данных и машинное обучение / Дж. Вандер Плас; пер. с англ. СПб.: Питер, 2021.

Поступила 05.02.2026 Принята в печать 13.03.2026 Доступна на сайте 10.04.2026

References

1. Galkin Yu. D., Dvornikov O. V., Chekhovsky V. A. (2022) Improved Dual-Gate JFET Model for Analog Integrated Circuits. *Doklady BGUIR*. 20 (3), 20–25 (in Russian).
2. Kravchenko O. A. (2020) Modification of a Stochastic Model for Optimizing Electricity Supply Costs at an Enterprise. *Vestnik BSU. Series 1*. (2), 45–52 (in Russian).
3. Vilkina M. V. (2022) Development of Tool Management Within the Framework of Industry 4.0. *Rhythm of Mechanical Engineering*. (3), 30–36 (in Russian).
4. Karpenko S. M., Karpenko N. V., Bezginnov G. Yu. (2022) Forecasting of Electricity Consumption at Mining Enterprises Using Statistical Methods. *Mining Industry*. (1), 82–88. DOI: 10.30686/1609-9192-2022-1-82-88 (in Russian).
5. Borovsky A. V., Yumenchuk A. A. (2024) Stochastic Electrical Load Model in the Residential Sector Using the Weibull Probability Density Function. *Modeling, Optimization and Information Technologies*. 12 (4), 1–18 (in Russian).
6. Hacker P. S., Schrank H. E. (1982) Range Distance Requirement for Measuring Low and Ultralow Sidelobe Antenna Patterns. *IEEE Transactions on Antennas and Propagation*. AP-30 (5), 956–966.
7. Chu M., Nguyen T., Pandey V., Zhou Y., Pham N H., Bar-Yoseph R., et al. (2019) Respiration Rate and Volume Measurements Using Wearable Strain Sensors. *npj Digital Medicine*. (2). DOI: 10.1038/s41746-019-0083-3.
8. Wen L., Zhou X., Yang Y. (2022) A Data-Driven Strategy Using Long Short-Term Memory Models and Reinforcement Learning to Predict Building Electricity Consumption. *Applied Energy*. 309. DOI: 10.1016/j.apenergy.2021.118437.
9. Seljom P., Kvalbein L., Hellemo L., Kaut M., Mucoz Ortiz M. (2021) Stochastic Modelling of Variable Renewables in Long-Term Energy Models: Dataset, Scenario Generation & Quality of Results. *Energy*. 236. DOI: 10.1016/j.energy.2021.121415.
10. VanderPlas J. (2021) *Python Data Science Handbook: Data Science and Machine Learning with Python*. Saint Petersburg, Piter Publ.

Received: 5 February 2026 Accepted: 13 March 2026 Available on the website: 10 April 2026

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Полоско Е. И., ст. преп. каф. экономической информатики, Белорусский государственный университет информатики и радиоэлектроники

Голда О., канд. экон. наук, доц. каф. программного обеспечения информационных систем, Белорусский государственный университет информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 25 530-89-43
E-mail: e.i.polosko@gmail.com
Полоско Екатерина Ивановна

Information about the authors

Polosko E., Senior Lecturer at the Department of Economic Informatics, Belarusian State University of Informatics and Radioelectronics

Holda O., Cand. Sci. (Econ.), Associate Professor at the Software of Information Systems Department, Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 25 530-89-43
E-mail: e.i.polosko@gmail.com
Polosko Ekaterina

http://dx.doi.org/10.35596/1729-7648-2026-32-1-51-60

УДК 331.108.26:004.056

ЭЛЕКТРОННЫЙ ПАСПОРТ КОМПЕТЕНЦИЙ: ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ БАЗОВОЙ ВЕРИФИКАЦИИ ПРОФЕССИОНАЛЬНЫХ КВАЛИФИКАЦИЙ

И. Н. КАЛИНОВСКАЯ

Витебский государственный технологический университет (Витебск, Республика Беларусь)

Аннотация. В статье представлено технико-экономическое обоснование применения электронного паспорта компетенций как инновационного решения для цифровой трансформации систем верификации профессиональных квалификаций в Республике Беларусь. Актуальность исследования обусловлена необходимостью повышения эффективности процессов базовой верификации квалификаций работников при массовом подборе персонала в условиях цифровизации экономики. Электронный паспорт компетенций представляет собой смарт-карту стандартного формата ID-1 с энергонезависимой памятью 64 Кбайт, предназначенную для хранения и верификации информации о 200–300 подтвержденных компетенциях. Обоснована экономическая целесообразность создания системы электронных паспортов компетенций для массовой верификации базовых квалификаций. Практическая значимость результатов определяется возможностью их применения для разработки национальной стратегии цифровизации учета профессиональных квалификаций, выбора оптимального технологического решения для массового подбора персонала, совершенствования процессов базовой верификации квалификаций в организациях республики.

Ключевые слова: электронный паспорт компетенций, верификация квалификаций, блокчейн-технология, управление человеческими ресурсами, профессиональные компетенции.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Калиновская, И. Н. Электронный паспорт компетенций: технико-экономическое обоснование цифровой трансформации базовой верификации профессиональных квалификаций / И. Н. Калиновская // Цифровая трансформация. 2026. Т. 32, № 1. С. 51–60. http://dx.doi.org/10.35596/1729-7648-2026-32-1-51-60.

ELECTRONIC COMPETENCY PASSPORT: A FEASIBILITY STUDY FOR THE DIGITAL TRANSFORMATION OF PROFESSIONAL QUALIFICATIONS BASIC VERIFICATION

IRYNA KALINOUSKAYA

Vitebsk State University of Technology (Vitebsk, Republic of Belarus)

Abstract. This article presents a feasibility study for the use of an electronic competency passport as an innovative solution for the digital transformation of professional qualifications verification systems in the Republic of Belarus. The relevance of the study is determined by necessity to improve the efficiency of professional qualifications basic verification processes for employees during mass recruitment in the context of the digitalization of the economy. The electronic competency passport is a standard ID-1 format smart card with 64 KB of non-volatile memory, designed to store and verify information on 200–300 verified competencies. The economic feasibility of creating an electronic competency passport system for the mass verification of basic qualifications is substantiated. The practical significance of the results is determined by their potential application for developing a national strategy for the digitalization of professional qualifications records, selecting the optimal technological solution for mass recruitment, and improving basic qualifications verification processes in organizations across the country.

Keywords: electronic competency certificate, qualification verification, blockchain technology, human resource management, professional competencies.

Conflict of interests. The author declares that there is no conflict of interests.

For citation. Kalinouskaya I. (2026) Electronic Competency Passport: A Feasibility Study for the Digital Transformation of Professional Qualifications Basic Verification. *Digital Transformation.* 32 (1), 51–60. http://dx.doi.org/10.35596/1729-7648-2026-32-1-51-60 (in Russian).

Введение

В условиях цифровой трансформации экономики Республики Беларусь вопросы достоверной верификации профессиональных квалификаций работников приобретают особую актуальность. Структура занятости претерпевает значительные изменения: результаты анализа вакансий на региональном рынке труда республики демонстрируют трансформацию требований к профессиональным навыкам, возрастание требований к цифровым компетенциям во всех профессиональных группах, появление новых специальностей в высокотехнологичных отраслях [1].

Традиционные системы подтверждения профессиональных квалификаций, основанные на бумажных документах (дипломы, сертификаты, удостоверения о повышении квалификации), характеризуются рядом существенных недостатков: высокая уязвимость к подделке и фальсификации; отсутствие единой системы учета и верификации; необходимость ручной проверки подлинности документов, требующей значительных временных затрат; невозможность автоматизированной обработки информации о компетенциях; отсутствие структурированных данных о практическом применении квалификаций. Существующие централизованные электронные базы данных о квалификациях, несмотря на переход к цифровому формату хранения информации, не решают всех проблем: создают высокую зависимость от функционирования центральных серверов и уязвимость к техническим сбоям, требуют постоянного интернет-соединения для доступа к данным, не обеспечивают владельцу полного контроля над своими учетными данными о компетенциях, не содержат информации о практическом применении полученных квалификаций.

В мировой практике активно развиваются технологические решения для цифровизации учета квалификаций на основе технологии распределенных реестров и криптографических методов защиты информации [2–5]. Однако большинство существующих решений реализованы в виде онлайн-платформ, требующих постоянного доступа к сети, либо в форме цифровых сертификатов без физического носителя, что ограничивает их применимость в условиях отсутствия стабильного интернет-соединения.

В статье рассмотрена разработанная технология электронного паспорта компетенций, защищенная патентом Республики Беларусь [6], представляющая собой комплексное решение для цифровизации систем верификации профессиональных квалификаций. В процессе исследований проанализированы существующие подходы к верификации профессиональных квалификаций с выявлением их ограничений, определены оптимальные сценарии применения электронного паспорта компетенций для различных групп стейкхолдеров, рассчитаны показатели экономической эффективности внедрения технологии для работодателей и государственных органов. Дано технико-экономическое обоснование применения инновационной технологии электронного паспорта компетенций как инструмента цифровой трансформации систем верификации профессиональных квалификаций для массового подбора персонала в экономике Беларуси.

Для выявления ограничений существующих подходов выполнялся сравнительный анализ по следующим критериям: технические характеристики (носитель информации, объем хранимых данных, защита от подделки, требования к инфраструктуре, портативность), экономические характеристики (стоимость создания документа, стоимость верификации, время верификации, зависимость от инфраструктуры), функциональные возможности (структурированность данных, автоматизированная обработка).

При определении временных затрат на верификацию квалификаций и оценки стоимостных параметров использовался метод экспертных оценок с привлечением специалистов-практиков отделов кадров организаций Витебской области. Была сформирована экспертная группа из 12 специалистов со стажем работы в сфере управления персоналом не менее пяти лет, представляющих различные отрасли экономики: производственные предприятия (четыре эксперта),

учреждения образования (три эксперта), организации сферы услуг (три эксперта), государственные органы (два эксперта). Обработка экспертных оценок проводилась методом медианы для исключения влияния крайних значений. Согласованность мнений экспертов проверялась расчетом коэффициента конкордации Кендалла *W*, который составил 0,78 при критическом значении 0,70, что свидетельствует о высокой степени согласованности экспертных оценок.

Для выявления резервов повышения эффективности проведено моделирование бизнес-процессов верификации квалификаций в нотации BPMN 2.0. Смоделированы два сценария базовой верификации квалификаций: при массовом подборе персонала в традиционной системе и с применением электронного паспорта компетенций.

Сравнительный анализ существующих подходов к верификации профессиональных квалификаций

Для обоснования необходимости разработки инновационного решения проведен сравнительный анализ существующих подходов к верификации профессиональных квалификаций с выявлением их технических и экономических ограничений (табл. 1).

Таблица 1. Сравнительный анализ подходов к верификации профессиональных квалификаций
Table 1. Comparative analysis of approaches to the verification of professional qualifications

Критерий	Бумажный документ	Централизованная электронная база данных	Электронный паспорт компетенций
Технические характеристики			
Носитель информации	Бумага	Серверы	Смарт-карта 64 Кбайт
Объем хранимых данных	Ограничен форматом документа	Не ограничен	200–300 компетенций
Защита от подделки	Низкая (водяные знаки, печати)	Средняя (пароли, шифрование)	Высокая (криптография и блокчейн)
Требование к интернету	Нет	Постоянное	Нет (автономная верификация)
Портативность	Высокая	Низкая	Очень высокая
Экономические характеристики			
Стоимость создания одного документа	5–15 руб.	0 руб. (после создания системы)	25–40 руб.
Стоимость верификации	Высокая (ручная проверка)	Низкая (при наличии доступа)	Очень низкая
Время верификации	2–3 дня	5–10 мин (онлайн)	5–10 мин
Зависимость от инфраструктуры	Нет	Критическая	Минимальная
Функциональные возможности			
Структурированность данных	Нет	Да	Да
Автоматизированная обработка	Нет	Да	Да
Интеграция с ИИ	Нет	Ограниченная	Предусмотрена

Анализ данных табл. 1 позволяет сделать следующие выводы:

– традиционные бумажные документы характеризуются низкой защищенностью от подделки, отсутствием структурированности данных и существенными затратами времени на верификацию. При этом они обладают преимуществом полной автономности от цифровой инфраструктуры;

– централизованные электронные базы данных решают проблему структурированности и автоматизации обработки информации, однако создают критическую зависимость от функционирования центральных серверов и наличия постоянного интернет-соединения. Данный подход уязвим к техническим сбоям и не обеспечивает владельцу полного контроля над своими данными о квалификациях;

– электронный паспорт компетенций представляет собой решение для базовой верификации подтвержденных квалификаций, сочетающее преимущества портативности физического носителя, криптографической защиты и возможности автономной верификации через распределенный реестр. Объем памяти 64 Кбайт позволяет хранить информацию о 200–300 компетенциях с указанием уровней владения и данных об организациях-эмитентах.

Техническая характеристика и применение разработанного решения

Электронный паспорт компетенций представляет собой смарт-карту стандартного формата ID-1 размерами 85,60×53,98 мм, которая хранит структурированную информацию о подтвержденных компетенциях и квалификациях владельца (рис. 1) [6].

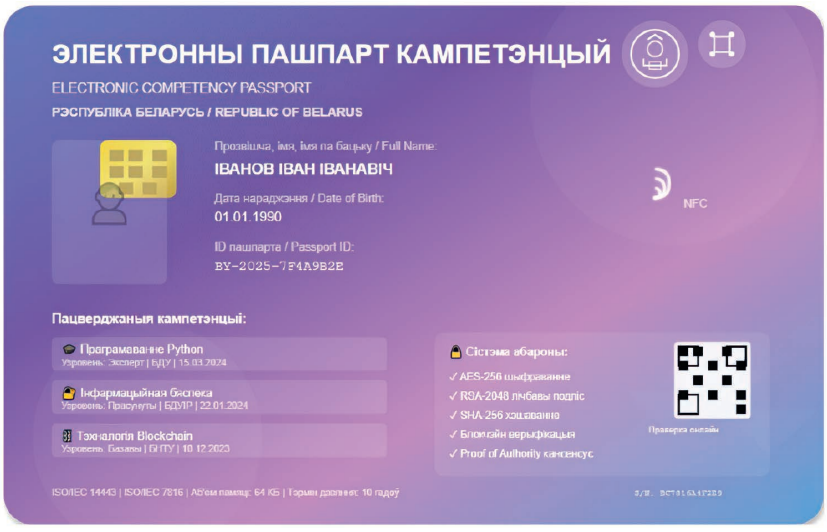

Рис. 1. Макет электронного паспорта компетенций
Fig. 1. Layout of the electronic competency passport

Карта содержит четыре раздела информации:

– персональные данные владельца (фамилия, имя, отчество, фотография, уникальный идентификационный номер). Доступ к этим данным защищен персональным паролем владельца;

– каталог компетенций – структурированный перечень до 300 подтвержденных компетенций с указанием уровня владения (базовый, продвинутый, экспертный), названия организации-эмитента, даты получения и срока действия квалификации;

– открытые криптографические ключи организаций – электронные подписи учреждений, которые выдали документы о квалификации. Эти подписи невозможно подделать или изменить;

– данные для проверки подлинности – специальные коды, которые позволяют проверить, что информация на карте достоверна и не была изменена после выдачи.

Система проверки подлинности работает в два этапа. Сначала проверяется электронная подпись учреждения, выдавшего документ о квалификации. Затем информация сверяется с записями в распределенном реестре (блокчейн-система), где хранятся контрольные данные обо всех выданных документах. Такая двухуровневая проверка практически исключает возможность подделки документов о квалификации. Важно, что проверка может проводиться даже без подключения к интернету, если заранее загружена локальная копия реестра.

Целевое назначение паспорта компетенций – быстрая проверка наличия базовых квалификаций при массовом подборе персонала, признание дипломов и сертификатов, формирование государственных реестров квалификаций. Электронный паспорт компетенций функционирует

в рамках экосистемы, включающей четыре основные группы участников, взаимодействующих через владельца паспорта (рис. 2).

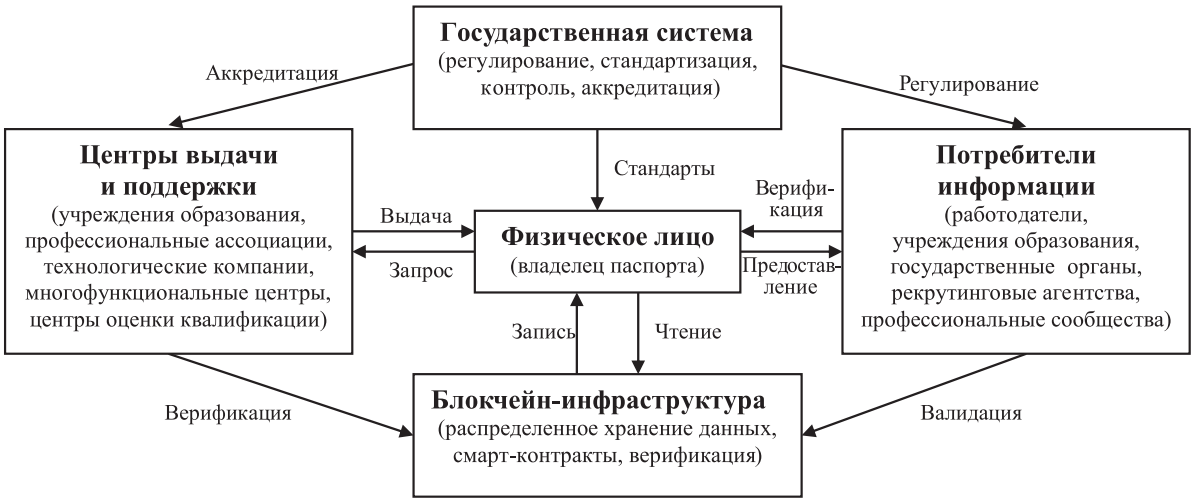

Рис. 2. Применение электронного паспорта компетенций
Fig. 2. Application of the electronic competence passport

Владелец электронного паспорта компетенций выступает центральным элементом экосистемы, осуществляя следующие действия: запрос на выдачу компетенций в центры выдачи и поддержки после получения документов об образовании или сертификации, запись компетенций в паспорт авторизованными центрами с формированием криптографической подписи, предоставление паспорта для чтения потребителям информации о квалификациях. Государственные органы (Министерство образования, Министерство труда и социальной защиты) выполняют функции: разработка стандартов компетенций для различных профессиональных групп, регулирование процессов верификации квалификаций, аккредитация центров выдачи и поддержки, валидация записей в распределенном реестре, контроль качества и аудит системы. Центры выдачи и поддержки (учреждения образования, профессиональные ассоциации, центры оценки квалификаций) осуществляют: выдачу электронных паспортов компетенций после верификации личности владельца, добавление записей о компетенциях после подтверждения получения квалификации, формирование криптографических подписей для каждой записи, запись хеш-значений в распределенный реестр блокчейна, техническую поддержку владельцев. Потребители информации о квалификациях (работодатели, учреждения образования, кадровые агентства) выполняют: чтение данных паспорта с использованием стандартных считывающих устройств для смарт-карт, верификацию подлинности информации путем проверки цифровых подписей организаций-эмитентов, сверку хеш-значений записей с распределенным реестром блокчейна, принятие кадровых решений на основе достоверной информации о компетенциях.

Процесс внесения новой информации в электронный паспорт компетенций осуществляется через авторизованные центры выдачи и поддержки после получения владельцем документов, подтверждающих освоение новых квалификаций. Когда владелец паспорта завершает обучение в учреждении образования, проходит курсы повышения квалификации в специализированных центрах или получает сертификат профессиональной ассоциации, он обращается в соответствующий центр выдачи и поддержки с документом об образовании (диплом, сертификат, удостоверение) и электронным паспортом компетенций. Специалист центра проверяет подлинность представленного документа, верифицирует соответствие полученных компетенций утвержденным стандартам, после чего вносит структурированную запись в паспорт с указанием наименования компетенции, уровня владения, даты получения и срока действия квалификации.

Каждая новая запись защищается криптографической подписью организации-эмитента, а ее хеш-значение автоматически регистрируется в распределенном реестре блокчейна, что обеспечивает невозможность последующего изменения или удаления информации без соответствующих полномочий. Такой подход гарантирует, что все компетенции в электронном паспорте имеют подтвержденное происхождение и могут быть верифицированы любым потребителем инфор-

мации о квалификациях. Владелец паспорта сохраняет полный контроль над своими данными: доступ к персональной информации защищен индивидуальным паролем, а предоставление паспорта для чтения работодателям или другим заинтересованным сторонам осуществляется только с согласия владельца. Система также предусматривает возможность обновления записей при продлении сроков действия квалификаций или повышении уровня владения компетенциями через прохождение дополнительного обучения.

С технической точки зрения процесс записи новой компетенции в электронный паспорт осуществляется следующим образом. Специалист центра выдачи и поддержки подключает смарт-карту к авторизованному терминалу записи, который считывает текущее содержимое паспорта и проверяет наличие свободного места в памяти (при объеме 64 Кбайт возможно хранение до 300 компетенций). После ввода структурированных данных о новой компетенции (код компетенции согласно национальному классификатору, уровень владения, дата получения, срок действия) криптографический сопроцессор смарт-карты формирует цифровую подпись записи с использованием закрытого ключа организации-эмитента. Одновременно программное обеспечение терминала вычисляет хеш-значение новой записи по алгоритму SHA-256 и автоматически отправляет его в распределенный реестр блокчейна для регистрации транзакции, после подтверждения которой запись окончательно фиксируется в памяти смарт-карты. Весь процесс от момента подключения карты до завершения записи занимает 2–3 мин и не требует подключения к интернету на стороне владельца паспорта, так как терминал центра выдачи обеспечивает необходимое взаимодействие с блокчейн-реестром.

Расчет экономической эффективности внедрения технологий

Оценка экономической эффективности внедрения электронного паспорта компетенций проводилась для типовой организации численностью от 100 человек с годовой потребностью в новых сотрудниках 20 человек на массовые позиции (табл. 2).

Таблица 2. Сравнение затрат на верификацию квалификаций для массовых позиций
Table 2. Comparison of qualification verification costs for bulk positions

Показатель	Традиционная система	Электронный паспорт компетенций
Время проверки одного кандидата, дни	2	0,06
Общее время проверки 20 кандидатов, дни	40	1,2
Стоимость проверки (оплата труда), руб.	3240	97
Стоимость оборудования (годовая амортизация), руб.	–	100
Общие годовые затраты, руб.	3240	197
Экономия, руб. (%)	–	3043 (94)
Сокращение времени	–	В 33 раза

Анализ табл. 2 показывает, что внедрение электронного паспорта компетенций для массовой верификации обеспечивает сокращение времени проверки одного кандидата с двух дней до 0,06 дня (около 5–10 мин), т. е. в 33 раза, экономию прямых затрат на оплату труда специалистов отдела кадров в размере 3043 руб. ежегодно, что составляет 94 % от первоначальных затрат, быстрый срок окупаемости инвестиций в считывающее оборудование (около 500 руб.) – менее двух месяцев. Дополнительные косвенные эффекты включают повышение качества кадровых решений благодаря достоверной информации о квалификациях кандидатов, снижение рисков найма неквалифицированных работников, ускорение процесса закрытия вакансий, улучшение имиджа организации как работодателя, применяющего современные технологии.

В рамках исследования проведен расчет экономической эффективности создания национального реестра квалификаций на базе электронных паспортов компетенций для одного миллиона граждан на период пять лет (табл. 3).

Таблица 3. Сравнение затрат традиционной централизованной системы с созданием и функционированием национального реестра квалификаций
Table 3. Costs comparison of a traditional centralized system with the creation and operation of a national register of qualifications

Статья затрат	Традиционная централизованная система	Система с электронным паспортом компетенций
Инвестиции		
Создание инфраструктуры, млн руб.	–	2 (распределенный реестр)
Ручной ввод данных о квалификациях, млн руб.	50 (50 руб. × 1 млн чел.)	– (автоматический)
Изготовление электронных паспортов, млн руб.	–	35 (35 руб. × 1 млн чел.)
Итого разовые затраты, млн руб.	50	37
Ежегодные затраты		
Поддержка системы, тыс. руб.	500	300
Затраты работодателей на верификацию (совокупно), млн руб.	100	10
Итого ежегодные затраты, млн руб.	100,5	10,3
Общие затраты за 5 лет, млн руб.	552,5	88,5
Экономия за 5 лет, млн руб. (%)	–	464 (84)
Средняя годовая экономия, млн руб.	–	92,8

Анализ затрат на содержание традиционной и электронной систем квалификаций позволил сделать следующие выводы: создание национального реестра квалификаций на базе электронных паспортов компетенций обеспечивает экономию 464 млн руб. за пять лет (снижение затрат – 84 %) по сравнению с традиционной централизованной системой; основная экономия (более 92 %) достигается за счет снижения затрат работодателей на верификацию квалификаций работников, что создает положительный эффект для всей национальной экономики. Дополнительные эффекты на национальном уровне: автоматическое формирование статистики о структуре квалификаций без ручного ввода данных повышает оперативность и достоверность информации для государственного планирования; рынок труда становится прозрачнее; снижается асимметрия информации между работодателями и работниками, что способствует более эффективному распределению трудовых ресурсов; улучшается возможность планирования подготовки кадров в учреждениях образования на основе актуальных данных о структуре спроса и предложения квалификаций; повышается мобильность трудовых ресурсов за счет упрощения процедур признания квалификаций при смене места работы или региона; создание основы для цифровизации процессов управления человеческими ресурсами.

Обсуждение результатов исследований

Разработанное технологическое решение соответствует глобальным трендам цифровой трансформации систем управления человеческими ресурсами и учета профессиональных компетенций [7, 8]. Ключевым отличием предлагаемого решения от существующих международных практик является комплексный подход, сочетающий:

– портативный физический носитель информации, обеспечивающий автономность от сетевой инфраструктуры;

– криптографическую защиту данных на уровне стандарта Common Criteria EAL5+;

– двухуровневую верификацию через цифровые подписи авторизованных эмитентов и распределенный реестр блокчейна;

– возможность автономной верификации при отсутствии постоянного интернет-соединения.

Адаптация решения к условиям Беларуси учитывает специфику национального рынка труда, отраслевую структуру экономики, уровень развития цифровой инфраструктуры в различных регионах, что обеспечивает практическую применимость и экономическую эффективность технологии. Проведенное исследование имеет ряд ограничений, которые следует учитывать при интерпретации результатов.

1. Расчеты экономической эффективности выполнены на основе данных по Витебской области. Для других регионов с иными структурой экономики и уровнем заработных плат показатели эффективности могут отличаться. Однако относительные показатели (процент экономии, кратность сокращения времени) ожидаются сопоставимыми.

2. Расчеты экономической эффективности приведены по данным 2025 г. В условиях динамично меняющейся экономической ситуации абсолютные показатели затрат и экономии требуют периодической актуализации. Структура эффектов при этом остается устойчивой.

3. Оценки косвенных эффектов основаны на экспертной оценке ввиду отсутствия статистических данных по этим показателям в официальных источниках. Для повышения точности оценок целесообразно проведение дополнительных эмпирических исследований.

4. Расчеты для государственного уровня предполагают массовое внедрение технологии с охватом 1 млн работников. Фактическая скорость внедрения будет определяться готовностью организаций к изменениям и доступностью финансирования.

5. Расчеты предполагают стабильность технологической платформы и отсутствие необходимости значительных обновлений в течение расчетного периода. В действительности может потребоваться периодическая модернизация решений в соответствии с развитием технологий.

Разработанное технологическое решение имеет существенный потенциал дальнейшего развития и расширения функциональности:

– интеграция с системами непрерывного образования – электронный паспорт компетенций может стать основой для системы непрерывного профессионального развития, автоматически формирующей персонализированные рекомендации по обучению на основе анализа пробелов в компетенциях;

– развитие аналитических возможностей ИИ – накопление больших массивов структурированных данных о компетенциях позволит обучать специализированные модели ИИ для прогнозирования профессиональной успешности, выявления скрытых талантов, формирования оптимальных команд для проектов;

– международная интеграция – использование международных стандартов криптографической защиты и классификации компетенций создает основу для международного признания электронных документов о квалификации, что важно для обеспечения трудовой мобильности граждан Беларуси.

Проведенное исследование открывает ряд перспективных направлений для дальнейшей научной работы:

- эмпирическая верификация расчетов эффективности через пилотное внедрение технологий в отдельных организациях с измерением фактических показателей экономии времени и затрат;
- исследование поведенческих аспектов внедрения – анализ факторов принятия/сопротивления новым технологиям со стороны работодателей, работников, учреждений образования;
- разработка методологии определения и оценки качества доказательств применения компетенций с учетом специфики различных профессиональных областей и отраслей экономики;
- исследование влияния внедрения технологий на эффективность рынка труда – снижение структурной безработицы, ускорение процессов поиска работы и подбора персонала, улучшение качества совпадений между вакансиями и кандидатами;
- анализ возможностей интеграции с международными системами признания квалификаций для обеспечения трудовой мобильности граждан Беларуси в рамках ЕЭС;
- разработка алгоритмов ИИ для автоматического формирования утверждений о способностях на основе анализа электронных паспортов компетенций и выявления оптимальных траекторий профессионального развития.

Заключение

1. Проведен сравнительный анализ существующих подходов к верификации профессиональных квалификаций, который выявил существенные технические и экономические ограничения традиционных бумажных документов и централизованных электронных баз данных. Традиционные системы характеризуются высокой уязвимостью к подделке, значительными затратами времени на проверку (2–3 рабочих дня на одного кандидата), отсутствием структурированности данных и невозможностью автоматизированной обработки информации.

2. Разработана технология электронного паспорта компетенций, обеспечивающая решение выявленных проблем традиционных носителей информации через комбинацию криптографической защиты уровня Common Criteria EAL5+, двухуровневой верификации (цифровые подписи совместно с блокчейном), автономности от сетевой инфраструктуры, совместимости с существующим оборудованием. Рассчитана экономическая эффективность применения электронного паспорта компетенций для основных стейкхолдеров: работодателей – сокращение времени верификации в 33 раза, экономия прямых затрат – 94 %; национального реестра квалификаций (1 млн граждан) – экономия 464 млн рублей за пять лет (снижение затрат – 84 %).

3. Определены оптимальные сценарии применения электронного паспорта компетенций: массовый подбор персонала на рядовые и базовые позиции; быстрая верификация квалификаций при признании документов об образовании; формирование государственных и отраслевых реестров квалификаций; автоматизация процессов кадрового учета в крупных организациях.

4. Практическая ценность результатов определяется возможностью их применения для формирования национальной стратегии цифровизации систем учета профессиональных квалификаций Республики Беларусь, принятия управленческих решений о внедрении технологий в организациях, совершенствования процессов подбора и оценки персонала, формирования эффективных механизмов развития человеческого капитала на региональном и национальном уровнях.

5. Результаты исследования имеют практическую ценность для руководителей организаций и специалистов отделов кадров при принятии решений о внедрении технологий цифровой верификации квалификаций, для учреждений образования при модернизации систем документооборота, для кадровых агентств при трансформации бизнес-моделей подбора персонала. Могут быть использованы исследователями в области управления человеческими ресурсами и преподавателями при подготовке специалистов по цифровой трансформации кадровых процессов.

Список литературы

1. Калиновская, И. Н. Применение больших языковых моделей для анализа профессиональных компетенций на региональном рынке труда Республики Беларусь / И. Н. Калиновская // Цифровая трансформация. 2025. Т. 31, № 2. С. 21–31. http://dx.doi.org/10.35596/1729-7648-2025-31-2-21-31.
2. Приженникова, А. Н. Технологии блокчейн в трудовых правоотношениях: перспективы и развитие / А. Н. Приженникова // Образование и право. 2019. № 1. С. 216–220.
3. Sharples, M. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward / M. Sharples, J. Domingue // Adaptive and Adaptable Learning. EC-TEL 2016. Lecture Notes in Computer Science. 2016. Vol. 9891. P. 490–496.
4. Jirgensons, M. Blockchain and the Future of Digital Learning Credential Assessment and Management / M. Jirgensons, J. Kapenieks // Journal of Teacher Education for Sustainability. 2018. Vol. 20, No 1. P. 145–156.
5. Swan, M. Blockchain: Blueprint for a New Economy / M. Swan. USA: O'Reilly Media, 2015.
6. Электронный паспорт компетенций на физическом носителе с защитой информации на основе блокчейн-технологии: пат. BY 13899 U 2026.01.05 Респ. Беларусь: МПК G06K 19/077 (2006.01) / Е. В. Ванкевич, И. Н. Калиновская, А. И. Калиновский; заявитель Витебский государственный технологический университет; заявка u 20250104; заявл. 12.05.2025; опубл. 05.01.2026. Бюл. № 1.
7. Система мотивации человека к получению знаний, навыков и компетенций: пат. RU2020110072A Рос. Федерации; МПК G06F 17/00 (2006.01) / О. А. Савостикова; заявитель ООО «Телепортация»; заявка 2020110072; заявл. 10.03.2020; опубл. 10.09.2021. Бюл. № 25.
8. Intelligent Recruitment Device for Human Resource Department Based on RFID Technology: CN210666862U; G06K-017/00|G06Q-010/10* / Yan Lei.; appl. CN201921312840U; decl. 2019-08-13; publ. 2020-06-02.

Поступила 10.02.2026 Принята в печать 13.03.2026 Доступна на сайте 10.04.2026

References

1. Kalinouskaya I. N. (2025) The Use of Large Language Models for the Analysis of Professional Competencies in the Regional Labor Market of the Republic of Belarus. *Digital Transformation*. 31 (2), 21–31. http://dx.doi.org/10.35596/1729-7648-2025-31-2-21-31 (in Russian).
2. Prizhennikova A. N. (2019) Blockchain Technologies in Labor Relations: Prospects and Development. *Education and Law*. (1), 216–220 (in Russian).
3. Sharples M., Domingue J. (2016) The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. *Adaptive and Adaptable Learning. EC-TEL 2016. Lecture Notes in Computer Science*. 9891, 490–496.

4. Jirgensons M., Kapenieks J. (2018) Blockchain and the Future of Digital Learning Credential Assessment and Management. *Journal of Teacher Education for Sustainability*. 20 (1), 145–156.
5. Swan M. (2015) *Blockchain: Blueprint for a New Economy*. USA, O'Reilly Media Publ.
6. Vankevich E. V., Kalinouskaya I. N., Kalinouski A. I. (2026) Electronic Passport of Competencies on a Physical Medium with Information Protection Based on Blockchain Technology. *Patent BY 13899 U 2026.01.05, Republic of Belarus. IPC G06K 19/077 (2006.01)*. Applicant: Vitebsk State Technological University. Application u 20250104; filed 12.05.2025; published 05.01.2026. Bulletin No 1 (in Russian).
7. Savostikova O. A. (2021) System for Motivating a Person to Acquire Knowledge, Skills and Competencies. *Patent RU2020110072A, Russian Federation. IPC G06F 17/00 (2006.01)*. Applicant: LLC "Teleportation". Application 2020110072; filed 10.03.2020; published 10.09.2021. Bulletin No 25 (in Russian).
8. Yan Lei (2019) Intelligent Recruitment Device for Human Resource Department Based on RFID Technology. *CN210666862U; G06K-017/00|G06Q-010/10**. Application CN201921312840U; decl. 2019-08-13; publ. 2020-06-02.

Received: 10 February 2026 Accepted: 13 March 2026 Available on the website: 10 April 2026

Сведения об авторе

Калиновская И. Н., канд. техн. наук, доц. каф. экономики и электронного бизнеса, Витебский государственный технологический университет

Адрес для корреспонденции

210039, Республика Беларусь,
Витебск, просп. Московский, 72
Витебский государственный
технологический университет
Тел.: +375 29 515-92-21
E-mail: i-kalinovskaya@yandex.by
Калиновская Ирина Николаевна

Information about the author

Kalinouskaya I., Cand. Sci. (Tech.), Associate Professor at the Department of Economics and Business Management, Vitebsk State University of Technology

Address for correspondence

210039, Republic of Belarus,
Vitebsk, Moskovsky Ave.,72
Vitebsk State University
of Technology
Tel.: +375 29 515-92-21
E-mail: i-kalinovskaya@yandex.by
Kalinouskaya Iryna