УДК 338

УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ВЫСОКОТЕХНОЛОГИЧНЫХ ОРГАНИЗАЦИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Кристина Михайловна ЕНИНА[1], аспирант

[1]Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Российская Федерация

Адрес для корреспонденции: Енина К.М., 191023, Санкт-Петербург, Невский пр., 60

Аннотация

В статье рассматриваются угрозы экономической безопасности высокотехнологичных организаций в Российской Федерации. Целью исследования является анализ существующих рисков и угроз, влияющих на стабильное экономическое развитие безопасности высокотехнологичных организаций. Автором для достижения поставленной цели использованы методы системного анализа, сравнительного исследования и экспертных оценок, что позволило выявить ключевые угрозы, такие как: кибератаки, утечка данных, зависимость от иностранных технологий и недостаточный уровень защиты информации.

В результате исследования было выявлено, что наибольшей угрозой для экономической безопасности высокотехнологичных организаций являются кибератаки, направленные на критически важную инфраструктуру, а также недостаточная координация между государственными органами и частным сектором в области обеспечения безопасности. Более того, были выявлены основные сценарии экономического развития высокотехнологичных организаций с учетом изменения геополитической и макроэкономической ситуации.

Основные выводы статьи подчеркивают необходимость создания комплексной стратегии развития высокотехнологичных организаций, включая развитие отечественных технологий, усиление нормативно-правового регулирования и повышение уровня осведомленности пользователей о возможных угрозах.

Ключевые слова

угрозы, экономическая безопасность, высокотехнологичные организации, технологии, кибератаки, данные

Для цитирования: Енина К.М. Угрозы экономической безопасности высокотехнологичных организаций в Российской Федерации // Ученые записки Международного банковского института. 2025. № 2(52). С. 63-77.

UDC 338

THREATS TO ECONOMIC SECURITY OF HIGH-TECH ORGANIZATIONS IN THE RUSSIAN FEDERATION

Kristina Mikhailovna ENINA[1], postgraduate student

[1]Autonomous non-profit organization of higher education «International Banking Institute named after Anatoly Sobchak», Saint-Petersburg, Russia

Address for correspondence: Enina K.M., 191023, Saint-Petersburg, Nevsky pr., 60

Abstract

The article examines the threats to the economic security of high-tech organizations in the Russian Federation. The aim of the study is to analyze the existing risks and threats affecting the stable economic development and security of high-tech entities. The author employs methods such as systems analysis, comparative studies, and expert assessments to achieve this goal, which has allowed for the identification of key threats such as cyberattacks, data leaks, dependence on foreign technologies, and insufficient information protection.

As a result of the research, it was found that the greatest threat to the economic security of high-tech organizations comes from cyberattacks targeting critical infrastructures, as well as the lack of coordination between government agencies and the private sector in security provision. Furthermore, the study identified key scenarios for the economic development of high-tech organizations, taking into account changes in the geopolitical and macroeconomic situations.

The main conclusions of the article emphasize the necessity of creating a comprehensive strategy for the development of high-tech organizations, including the development of domestic technologies, strengthening regulatory frameworks, and raising user awareness about potential threats.

Keywords

threats, economic security, ICT sector, technologies, cyberattacks, data

For citation: Enina K.M. Threats to economic security of high-tech organizations in the Russian Federation // Proceedings of the International Banking Institute. 2025. 2 (52). pp. 63-77 (in Russ.).

Введение

Двадцать первый век – эпоха технологий и безграничных цифровых возможностей, время машинного обучения, развития искусственного интеллекта, а также период, когда информация является ключевым ресурсом развития экономических отношений между различными субъектами. В связи

с этим, наряду с такими отраслями как: медицина, сельское хозяйство, промышленность, транспорт и туризм, развивается и отрасль информационно-коммуникационных технологий (ИКТ), следовательно, и стимулируется развитие высокотехнологичных организаций.

Высокотехнологичные организации – это юридические лица, которые специализируются на развитии технологий и сервисов, которые направлены на обработку, хранение, распространение информации. Деятельность подобных организаций связана с аппаратным обеспечением, сетевыми технологиями, услугами ИКТ (цифровые медиа, облачные вычисления и телекоммуникационные услуги), искусственным интеллектом и машинным обучением, и также социальными аспектами (к примеру, кибератаками). Таким образом, область работы высокотехнологичных организаций достаточно обширна и охватывает множество ключевых элементов повседневной жизни современного гражданина, а значит, развитие этих организаций влияет и на качество и уровень жизни общества.

В данной статье будут выявлены и рассмотрены угрозы экономической безопасности высокотехнологичных организаций с целью разработать рекомендации по минимизации выявленных угроз.

Материалы и методы

В данной статье использованы материалы, опубликованные на официальном сайте Министерстве цифрового развития, а именно: реестр российского программного обеспечения, реестр аккредитованных ИТ-организаций в РФ, объем выделенных инвестиций в ИТ-отрасль, статистические данные по киберугрозам и атакам на высокотехнологичные организации, а также основные нормативно-правовые акты, которые регулируют действия высокотехнологичных организаций, и так далее. В данной статье используются аналитические методы исследования, основанные на анализе данных из официальных реестров и статистической информации, также применяются сравнительный и описательный анализ для оценки текущего состояния ИТ-отрасли и угроз, с которыми она сталкивается.

Основная часть

Развитие технологий, интеграция цифровых решений в бизнес-процессы всех компаний, не только высокотехнологичных, и возрастание значимости данных как основного ресурса обуславливают появление новых вызовов и угроз. На вопрос, какие угрозы являются наиболее критичными для

высокотехнологичных организаций и какие подходы необходимо применить юридическим лицам для их минимизации, у ведущих экономистов есть различные точки зрения. Рассмотрим некоторые из них.

Гераськин Д.В. подчеркивает, что не только внешние угрозы представляют опасность, но и внутренние угрозы, основным источником которых являются сотрудники организации и связанные с этим нарушения целостности информации [1]. Данилин И.В. особое внимание уделяет кибератакам, говоря о том, что киберугрозы становятся все более сложными и многоступенчатыми, что требует от организаций постоянного мониторинга и адаптации [4]. Козлова Е.В. выступает с противоположной точкой зрения, указывая на то, что чрезмерные инвестиции в IT-безопасность не всегда уместны, так как малые и средние компании не всегда могут позволить себе большие расходы и могут замедлить их экономический рост [5].

Также можно рассмотреть исследования на тему зависимости высокотехнологичных организаций от иностранных технологий. Кустова М. Н. рассматривает эту ситуацию как критическую угрозу, которая может привести к утрате контроля над ключевыми технологиями и, как следствие, к ухудшению уровня экономической безопасности Российской Федерации в целом, автор подчеркивает важность развития отечественной индустрии программного обеспечения [8]. С другой стороны, Глухов В.В. утверждает, что импорт иностранных технологий в бизнес-процессы высокотехнологичных компаний ускоряет процесс инноваций, а также способствует международному сотрудничеству [3]. Шполянская А. А. считает, что управление стратегией развития высокотехнологичных компаний должно быть модернизировано, предлагая масштабировать коммерциализации цифровых решений и продавать в виде самостоятельного продукта или модуля сторонним экономическим агентам, тем самым, развивая стратегические альянсы высокотехнологичных компаний [10].

Таким образом, существуют противоречия в современных научных дискуссиях по вопросам обеспечения экономической безопасности высокотехнологичных организаций в Российской Федерации и дальнейшем экономическом развитии таких организаций – это подчеркивает актуальность исследования этой темы.

Высокотехнологичные компании – это драйвера российской экономики, компании, которые производят высокотехнологичную продукцию. Куприков Н.М. выделяет 4 отрасли по использованию технологий [7]:

1. Высокотехнологичные (High Technology);
2. Высококачественные среднетехнологичные;
3. Отрасли с низкой интенсивностью НИОКР;
4. Отрасли с очень низкой интенсивностью НИОКР («низкие технологии»).

Высокотехнологичные компании в Российской Федерации в 2024 году относятся к следующим отраслям: авиационная и ракетно-космическая промышленность, судостроение, радиоэлектронная промышленность, атомный энергопромышленный комплекс, энергетическое машиностроение, информационно-коммуникационные технологии (согласно распоряжению Правительства РФ от 17.11.2008 N 1662-р (ред. от 28.09.2018).

Рассмотрим несколько критериев отнесения предприятия к высокотехнологичным:

—экономический потенциал, который подтвержден экономическим ростом основных показателей (в среднем на 15–20% в год);

—обязательное осуществление финансирования научно-исследовательский и опытно-конструкторских работ (не менее 15% на НИОКР из общего числа инвестиций компании);

—ежегодный ввод и продажа новых продуктов на рынок (продукты фармакологической отрасли, новое программное обеспечение и т.д.) [13];

—участие и поддержка использования отечественных наукоемких продуктов.

И на данный момент есть два сдерживающих фактора экономического развития высокотехнологичных компаний, что в свою очередь негативно влияет и на их экономическую безопасность:

—отсутствие единого реестра высокотехнологичных компаний, следовательно, отсутствие единой структуры высокотехнологичных компаний и отчетности по прогрессу этих предприятий;

—отсутствие аккредитации у высокотехнологичных компаний по аналогии с аккредитованными ИТ-организациями, что ограничивает рассматриваемые организации в получении льгот от государства.

Таким образом, подтверждается актуальность экономического развития высокотехнологичных компаний, но нет механизма контроля процесса развития этих предприятий. Рассмотрим некоторые НПА, которые в комплексе не могут быть механизмом, однако являются началом для создания центра управления высокотехнологичными компаниями.

Таблица 1– Основные нормативно-правовые акты, регулирующие деятельность высокотехнологичных компаниях

НПА	Значение для высокотехнологичных компаний
Федеральный закон «О науке и государственной научно-технической политике» от 23.08.1996 N 127-ФЗ	Регулирование проведения научных исследований и развития технологий.
Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ	ФЗ устанавливает требования к защите информации в высокотехнологичных компаниях.
Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ	Устанавливает правила обработки, хранения и защиты персональных данных (как сотрудников, так и клиентов компании).
Постановление Правительства РФ от 09.04.2010 N 218 (ред. от 28.09.2023) «О мерах государственной поддержки развития кооперации российских образовательных организаций высшего образования, государственных научных учреждений и организаций реального сектора экономики в целях реализации комплексных проектов по созданию высокотехнологичных производств»	Определяет порядок получения субсидий для поддержки высоких технологий.

Источник: [2], [3], [4]

Экономическая безопасность как состояние защищенности субъекта от внешних и внутренних угроз влияет и на развитие высокотехнологичных компаний, так как при существенных тратах на обеспечение безопасности и формировании стратегии по защите материальных и нематериальных активов может снизиться уровень инвестиций в развитие продуктов и создание наукоемкой продукции. Подробнее остановимся на угрозах экономической безопасности высокотехнологичных компаний.

Угроза экономической безопасности – комплекс событий, реализация которого приведет к нарушению функционирования хозяйствующего субъекта и финансовому ущербу. Выявим основные угрозы экономической безопасности высокотехнологичных компаний:

—утечка данных [7];

—нехватка или утечка высококвалифицированных специалистов;

—увеличение количества кибератак.

Рассмотрим более подробно первую угрозу – утечка данных (рисунок 1).

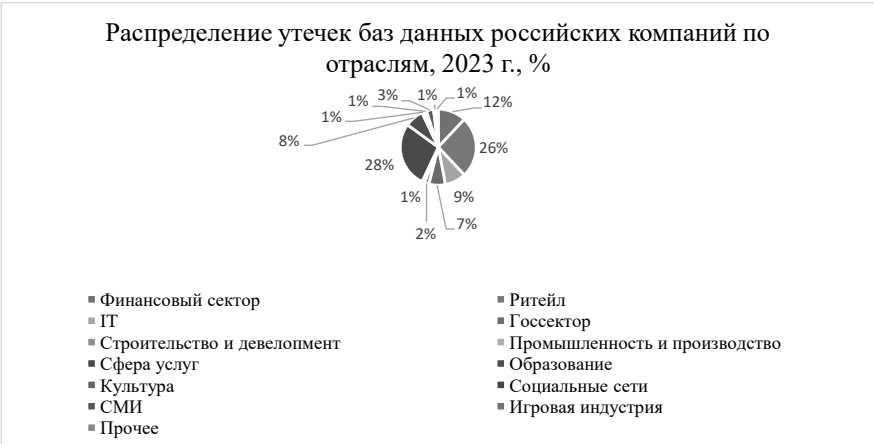

Рисунок 1 – Распределение утечек баз данных российских компаний по отраслям, 2023 г., %

Источник: [8]

В 2023 году было зафиксировано 420 инцидентов утечек баз данных в российских компаниях, распределение этих утечек по отраслям представлено на рисунке 1. Можно сделать вывод, что лидерами по утечке данных является финансовый сектор и сектор сферы услуг (более 20% случаев), в ИТ-отрасли случаев утечек баз данных меньше и составляет 9%. Отчасти объяснить такое распределение возможно тем, что секторы ритейла и услуг значительно уступают ИТ-отрасли в использовании программ по киберзащите, следовательно, уровень информационной безопасности у данных отраслей существенно ниже, чем у ИТ-организаций. При краже данных в 38% случаев преступники более всего нацелены на продажу существующих аккаунтов, вербовку сотрудников ИТ-сектора с целью кражи данных у крупных

российских компаний (в том числе, высокотехнологичных), а в 31% случаев злоумышленники совершают операции с чужими банковскими картами.

Отдельно необходимо проанализировать государственный сектор: объем информации, составляющей государственную тайну в 2023 году, увеличился на 4% (6,6% в 2023 году). Доля этой информации подверглась утечке, что негативно влияет на уровень не только экономической безопасности страны, но и национальной безопасности в целом. Также стоит отметить, что утечка данных из банковского сектора увеличилась в 2023 году на 2,5%. В основном, утечка данных касалась персональных данных клиентов и информации о денежных операциях за рубежом [4].

Рассмотрим основные причины угрозы утечки данных в 2024 году:

1.Рост доли информации, составляющей государственную тайну.

2.Уязвимость российских компаний из-за перехода на отечественные продукты и вынужденную реорганизацию бизнес-систем.

3.Отсутствия механизма контроля о сообщении утечек информации в компаниях.

4.Появление крупных хранилищ данных из-за ускоренной цифровизации экономики.

5.Научно-технологическая отсталость организаций по сравнению с международными стандартами и уровнем технологической оснащенности киберпреступников.

Следующая угроза высокотехнологичных организаций – это нехватка или утечка высококвалифицированных специалистов. Рассмотрим статистику потребности компаний в соискателях за последние годы.

В 2024 году «Коммерсантъ» и Superjob проанализировали кадровый голод, проведя опрос среди 1000 хозяйствующих субъектов. По результатам этого анализа можно сказать, что нехватку специалистов ощущают более 86% анкетируемых, более того, в отрасли IT, связи, телекома эти данные достигают 83%. Общее количество требуемых сотрудников (во всех отраслях) – более 4,5 миллиона человек, а в ИТ-отрасли – 650 тыс. человек.

Выявляют следующие причины нехватки специалистов:

—мобилизация части трудоспособного населения на специальную военную операцию;

—релокация части трудоспособного населения за границу;

—ослабление рубля как денежной единицы;

—демографический кризис (связанный также с пандемией 2020–2021 гг.) [9].

Стоит также отметить, что наблюдается аномально низкий уровень безработицы – ситуация, при которой, с одной стороны, развивается экономика, увеличиваются налоговые отчисления, но с другой стороны: повышается конкуренция среди хозяйствующих субъектов за кадры, тем самым, повышается заработная плата, что приводит к увеличению затрат и себестоимости продукции. Более того, чрезмерно высокие показатели спроса специалистов сферы услуг снижает производство.

Угроза экономической безопасности высокотехнологичных компаний – увеличение количества кибератак, также имеет место быть: рассмотрим динамику кибератак в России.

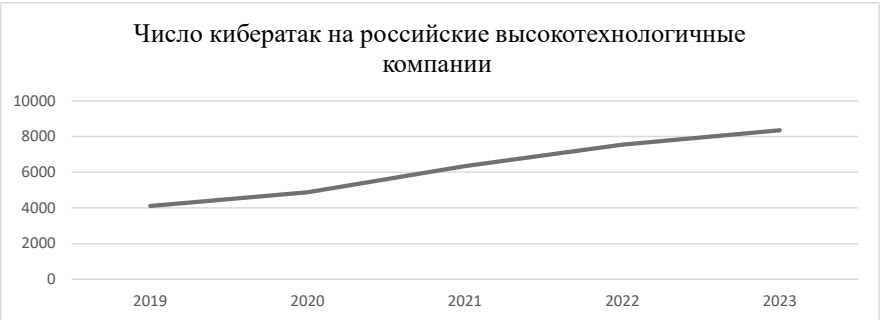

Рисунок 2 – Число кибератак на российские высокотехнологичные компании, 2023 г., ед.

Источник:[5]

Кибератаки – злонамеренные попытки частных лиц или организаций взлома компьютеров, сетей или информационных систем с целью получения несанкционированного доступа к данным, их повреждения, разрушения инфраструктуры и использования в своих целях. Кибератаки могут иметь серьезные последствия для безопасности и функционирования организаций и государств, а статистика на рисунке 2 доказывает, что число кибератак увеличивается с каждым годом. Рассмотрим основные причины положительной динамики количества кибератак (таблица 2).

Таблица 2 – причины увеличения кибератак на российские высокотехнологичные компании

Наименование причины	Описание
Увеличение удаленной работы	Пандемия COVID-19 стимулировала массовый переход сотрудников на удаленный формат работы, а это создало новые уязвимости в корпоративных сетях, к которым организации не были готовы в связи с внезапным увеличением процента сотрудников, которые работают вне офиса.
Усовершенствование методов социальной инженерии	Усложнение схем злоумышленников по получению данных пользователей.
Геополитическая напряженность	В условиях глобальной нестабильности и конфликтов кибератаки становятся инструментом геополитической войны.
Увеличение популярности криптовалют	С ростом криптовалют злоумышленники получают возможность проводить анонимные транзакции.

Источник:[6], [11]

Уязвимости в программном обеспечении, недостаточный уровень безопасности облачных сервисов делают высокотехнологичные компании привлекательной целью для киберпреступников, а использование сложных методов социальной инженерии позволяет киберпреступникам получать несанкционированный доступ к корпоративным системам [14].

Рассмотрим основные методы, которые могут использовать высокотехнологичные компании для минимизации выявленных угроз: в основном, эти методы можно поделить на административно-организационные и технические.

К административно-организационным относятся:

—разработка документации: создание протоколов защиты информации, правил защиты персональных данных, стратегии развития информационной безопасности в организации. В компании должны быть четкие инструкции на любые ситуации, которые могут подвергнуть риску целостность информации [4];

—непрерывная работа с персоналом: в компании все сотрудники должны проходить обязательный инструктаж с целью предотвращения утечки данных, также обязательны тестовые учебные «фишинговые» письма от сотрудников информационной безопасности;

—работа с контрагентами: компаниям следует усилить меры предосторожности в отношении всех партнеров, которые требуют предоставления данных, относящихся к коммерческой тайне, то есть в каждом контракте должны быть прописаны условия, касающиеся ответственности за утечку такой информации [11].

К техническим методам можно отнести 4 группы средств: инженерные, аппаратные, программные, криптографические (таблица 3).

Таблица 3 – технические методы для минимизации угроз высокотехнологичных компаний

Наименование причины	Описание
Инженерные	Использование компаниями устройств, которые будут предотвращать проникновение сторонних лиц на территорию организации (системы видеонаблюдения, сигнализации, электронные замки и другие аналогичные технические приспособления).
Аппаратные	Устройства, которые могут выявить каналы утечки информации (детекторы диктофонов, радиочастотометры и так далее).
Программные	Программное обеспечение, которое предотвращает хакерские атаки: DLP-системы и SIEM-системы. DLP-системы обычно действуют против угроз внутри контура компании, а SIEM-системы воздействуют на управление информационными потоками вне периметра.
Криптографические	Программы шифрования информации компании.

Источник:[10], [12], [15]

Итак, использование только одного метода не будет достаточным для минимизации угроз высокотехнологичной компании, так как только комплексный подход может обеспечить достаточный уровень информационной безопасности организаций.

Заключение

Таким образом, было выявлено, что кибератаки, утечки данных, а также зависимость от иностранных технологий представляют собой наиболее серьезные угрозы для экономической безопасности высокотехнологичных организаций. Необходимо отметить, что недостаток координации между государственными структурами и частным сектором усугубляет ситуацию, а это требует создания комплексной стратегии для преодоления существующих

вызовов, комплексных методик, которые смогут использовать высокотехнологичные организации. Исследование также подчеркивает важность формирования отечественных технологий, усиления нормативно-правового регулирования в этой сфере, повышение уровня осведомленности работников о киберугрозах и внедрение эффективных мер защиты.

Список источников

1. **Гераськин Д.В.** Эталонные стратегии обеспечения конкурентоспособности высокотехнологичных продуктов в России // Бизнес в законе, 2016. № 2. С.54-58.
2. **Главатских О.Б., Соколова И. Н.** Проблемы и тенденции инновационного развития высокотехнологичных предприятий в условиях цифровой экономики // В сб.: Актуальные вопросы экономики и финансов. Сборник статей II международной научно-практической конференции. - Ижевск, 2022. С. 140-153.
3. **Глухов В. В.** Цифровое стратегирование промышленных систем на основе устойчивых экоинновационных и циркулярных бизнес-моделей в условиях перехода к Индустрии 5.0 / В.В. Глухов, А.В. Бабкин, Е.В. Шкарупета // Экономика и управление. 2022. Т. 28, № 10. С. 1006- 1020.
4. **Данилин И. В.** Высокотехнологичные предприятия как ядро экономики региона в условиях реиндустриализации // Проблемы социально-экономической устойчивости региона. Сборник статей XX Международной научно-практической конференции. Под редакцией Г.А. Резник. - Пенза, 2023. С. 125-131.
5. **Козлова Е. В.** Государственная поддержка быстрорастущих высокотехнологичных российских компаний / Е.В. Козлова // Интеллектуальная инженерная экономика и индустрия 5.0 (ЭКОПРОМ): Сборник трудов Международной научно-практической конференции, Санкт-Петербург, 17-18 ноября 2023 года. - Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2023. С. 424-426.
6. **Колмыкова Т. С., Клыкова С.В.** Роль цифровых финансовых сервисов и технологий в развитии современной архитектуры экономического пространства // Регион: системы, экономика, управление. 2021. № 2(53). С. 11–17.
7. **Куприков Н.М.** Проблемы методологии информационно-технологического сопровождения технического обслуживания и ремонта / Н.М. Куприков, М.Ю. Куприков, Ю.В. Будкин // Известия Тульского государственного университета. Технические науки. 2022. № 7. С. 296-302.

8. **Кустова М. Н., Никулина С. М., Шевырева А. Д.** Автоматизированные системы управления персоналом на российском рынке: особенности и тенденции их развития // Военно-экономический вестник. 2023 №3.
9. **Малашкина О. Ф.** Методы и механизмы стратегического управления развитием высокотехнологичных компаний в условиях глобальной цифровизации // BENEFICIUM. 2021. № 1(38). С. 28–33.
10. **Шполянская А.А.** Высокотехнологичные отрасли: определение и условия развития //Молодой ученый. 2015. № 22 (102). С. 518522.
11. **Alfaro L., Antras P., Chor D., and Conconi P.** Internalizing Global Value Chains: A Firm-Level Analysis // National Bureau of Economic Research Working Paper. 2017. Working Paper No. 21558.
12. **Haverila M., Haverila K.C., Twyford J.C.** «Critical variables and constructs in the context of project management: importance-performance analysis»//International Journal of Managing Projects in Business, 2021. Vol. 14. No. 4. pp. 836-864.
13. **Li J., Xia C., Chen X.** A Benchmark Dataset and Saliency-Guided Stacked Autoencoders for Video-Based Salient Object Detection // IEEE Transactions on Image Processing. 2018. Vol. 27. Pp. 349–364.
14. **Miawati T., Sunaryo W., Yusnita N.** Exploratory study of employee engagement // JHSS (Journal of humanities and social studies). 2020. Vol. 04, № 02. pp. 102-106.
15. **Schaufeli W., Bakker A.** Defining and measuring work engagement: Bringing clarity to the concept // Work engagement: A handbook of essential theory and research / eds. A. Bakker, M. Leiter. New York: Psychology Press, 2010. pp. 10-24.

References

1. **Geras'kin D.V.** Etalonnye strategii obespecheniya konkurentosposobnosti vysokotekhnologichnyh produktov v Rossii // Biznes v zakone, 2016. № 2. S.54-58.
2. **Glavatskih O.B., Sokolova I.N. Problemy** i tendencii innovacionnogo razvitiya vysokotekhnologichnyh predpriyatij v usloviyah cifrovoj ekonomiki [Tekst] // V sb.: Aktual'nye voprosy ekonomiki i finansov. Sbornik statej II mezhdunarodnoj nauchno-prakticheskoj konferencii. - Izhevsk, 2022. - S. 140-153.
3. **Gluhov V. V.** Cifrovoe strategirovanie promyshlennyh sistem na osnove ustojchivyh ekoinnovacionnyh i cirkulyarnyh biznes-modelej v usloviyah perekhoda k Industrii 5.0 / V.V. Gluhov, A.V. Babkin, E.V. SHkarupeta // Ekonomika i upravlenie. 2022. T. 28, № 10. S. 1006- 1020.

4. **Danilin I.V.** Vysokotekhnologichnye predpriyatiya kak yadro ekonomiki regiona v usloviyah reindustrializacii // Problemy social'no-ekonomicheskoj ustojchivosti regiona. Sbornik statej XX Mezhdunarodnoj nauchno-prakticheskoj konferencii. Pod redakciej G.A. Reznik. - Penza, 2023. - S. 125-131.
5. **Kozlova E.V.** Gosudarstvennaya podderzhka bystrorastushchih vysokotekhnologichnyh rossijskih kompanij / E.V. Kozlova // Intellektual'naya inzhenernaya ekonomika i industriya 5.0 (EKOPROM): Sbornik trudov Mezhdunarodnoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 17-18 noyabrya 2023 goda. - Sankt-Peterburg: POLITEKH-PRESS, 2023. - S. 424-426.
6. **Kolmykova T.S., Klykova S.V.** Rol' cifrovyh finansovyh servisov i tekhnologij v razvitii sovremennoj arhitektury ekonomicheskogo prostranstva // Region: sistemy, ekonomika, upravlenie. 2021. № 2(53). S. 11-17.
7. **Kuprikov N.M.** Problemy metodologii informacionno-tekhnologicheskogo soprovozhdeniya tekhnicheskogo obsluzhivaniya i remonta / N.M. Kuprikov, M.YU. Kuprikov, YU.V. Budkin // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2022. № 7. S. 296-302.
8. **Kustova M. N., Nikulina S. M., SHevyreva A. D.** Avtomatizirovannye sistemy upravleniya personalom na rossijskom rynke: osobennosti i tendencii ih razvitiya // Voenno-ekonomicheskij vestnik. 2023 №3.
9. **Malashkina O.F.** Metody i mekhanizmy strategicheskogo upravleniya razvitiem vysokotekhnologichnyh kompanij v usloviyah global'noj cifrovizacii // BENEFICIUM. 2021. № 1(38). S. 28-33.
10. **Shpolyanskaya, A.A.** Vysokotekhnologichnye otrasli: opredelenie i usloviya razvitiya //Molodoj uchenyj. 2015. № 22 (102). S. 518522.
11. **Alfaro L., Antras P., Chor D., and Conconi P.** Internalizing Global Value Chains: A Firm-Level Analysis // National Bureau of Economic Research Working Paper. 2017. Working Paper No. 21558.
12. **Haverila M., Haverila K.C., Twyford J.C.** Critical variables and constructs in the context of project management: importance-performance analysis // International Journal of Managing Projects in Business, 2021. Vol. 14. No. 4. pp. 836-864.
13. **Li J., Xia C., Chen X.** A Benchmark Dataset and Saliency-Guided Stacked Autoencoders for Video-Based Salient Object Detection // IEEE Transactions on Image Processing. 2018. Vol. 27. Pp. 349–364.
14. **Miawati T., Sunaryo W., Yusnita N.** Exploratory study of employee engagement // JHSS (Journal of humanities and social studies). 2020. Vol. 04, № 02. pp. 102-106.

15. **Schaufeli W., Bakker A.** Defining and measuring work engagement: Bringing clarity to the concept // Work engagement: A handbook of essential theory and research / eds. A. Bakker, M. Leiter. New York: Psychology Press, 2010. pp. 10-24.