

Ссылка для цитирования этой статьи:

Кузнецов Е.С., Казьмина И.В. Сущность, принципы и методы обеспечения экономической безопасности высокотехнологичных предприятий в условиях цифровой трансформации // Human Progress. 2025. Том 11, Вып. 10. С. 3. URL: http://progress-human.com/images/2025/Tom11_10/Kuznetsov.pdf DOI 10.46320/2073-4506-2025-10a-9.

УДК 332

СУЩНОСТЬ, ПРИНЦИПЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Кузнецов Егор Сергеевич

АНОО ВО «Воронежский экономико-правовой институт»
г. Воронеж, Российская Федерация

Казьмина Ирина Владимировна

доктор экономических наук, доцент
Военно-воздушная академия имени профессора Н.Е. Жуковского и
Ю.А. Гагарина
г. Воронеж, Российская Федерация

Аннотация. Статья посвящена анализу трансформации бизнес-процессов высокотехнологичных предприятий (ВТП) в условиях цифровой экономики, акцентируя внимание проблемах и принципах обеспечения экономической безопасности, а также методологии преодоления угроз. В контексте усиления киберугроз и цифровизации ключевых отраслей обосновывается необходимость перехода к системной архитектуре управления, интегрирующей технологические, организационные и кадровые аспекты. На примере российских кейсов («Сбербанк», «Ростех», «Яндекс») демонстрируется поэтапная модель трансформации, включающая:

1. Формирование цифровых платформ для устранения организационных разрывов;
2. Внедрение ERP-систем и цифровых двойников;
3. Создание единого информационного пространства через API-интеграцию.

Ключевой методологической основой исследования выступает синдика – междисциплинарный подход, сочетающий анализ техногенных рисков, социоинженерные практики и прогнозное моделирование. В исследовании рассматривается возможность применения пятимерной модели безопасности, охватывающую финансы, производство, технологии, кадры и управление. Её апробация выявила ключевое противоречие цифровой

трансформации: технологические инновации, повышая операционную эффективность, одновременно генерируют новые риски. Например, интеграция API-интерфейсов в экосистемы (кейс «Яндекса») сократила время обработки данных на 25%, но увеличила число инцидентов с несанкционированным доступом на 40%. Для решения таких проблем предлагается адаптировать синдинические методы, включая анализ каскадных эффектов и сценарное моделирование угроз.

Выявлены системные ограничения: лишь немногие российские высокотехнологичные компании применяют системный подход к рискам, дефицит финансирования ИТ-инфраструктуры в малом бизнесе, кадровые дисбалансы. Для их преодоления рекомендуется повышение мер государственной поддержки R&D-проектов, а также обращается внимание на необходимость разработки отраслевых стандартов и образовательных программ.

Исследование вносит вклад в теорию экономической безопасности, предлагая адаптацию синдиники к реалиям цифровой трансформации, и имеет практическую значимость для предприятий, стремящихся минимизировать операционные и киберриски. Приведенные данные основаны на анализе отчетов («Гарда», 2024), стратегических документов (Указ Президента № 203) и изученных кейсов.

Ключевые слова: цифровая трансформация, архитектура предприятия, сущность, принципы, экономическая безопасность, высокотехнологичное предприятие, риски цифровой среды, управление рисками, информационные технологии, цифровая зрелость, синдиника.

В условиях современной экономики высокотехнологичные предприятия сталкиваются с новыми вызовами, связанными с процессом цифровой трансформации. Процесс цифровизации не только открывает новые горизонты в развитии бизнеса, но и требует переосмысления традиционных методов обеспечения экономической безопасности. Внедрение цифровых технологий и инноваций создает возможность ускорения бизнес-процессов и производительности, но и влечет за собой увеличение рисков в системах защиты информации и цифровых активов.

В Стратегии экономической безопасности Российской Федерации на период до 2030 года дано определение угрозы экономической безопасности, которое целесообразно спроецировать с макроуровня на микроуровень. Так, согласно Стратегии, «угроза экономической безопасности – совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере».

Как отмечается «целесообразно разделить угрозы по механизму возникновения на внутренние и внешние. К внешним в общем смысле могут быть отнесены изменения законодательства, кризисы, конкуренция на рынке, технологические изменения и др. Ко внутренним чаще относят различного генезиса внутренние конфликты, проблемы в управлении, финансовые трудности, неэффективное использование ресурсов, некачественная продукция или услуги» [3, с. 235].

Более подробную картину угроз представляет отчет за 2024 год компании «Гарда».

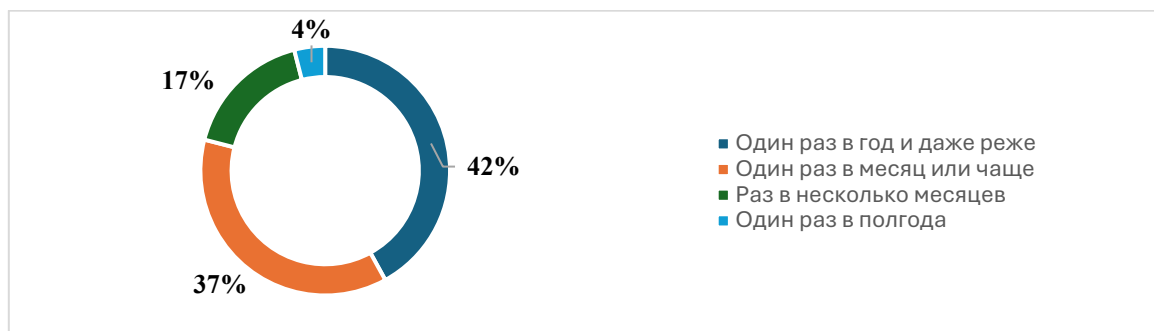


Диаграмма 1. Частота, с которой ВТП подвергаются атакам [2, с. 2]

Согласно проведенному исследованию, большинство респондентов сталкиваются с атаками не реже двух раз в год. Почти 40% испытывают атаки каждый месяц и чаще.

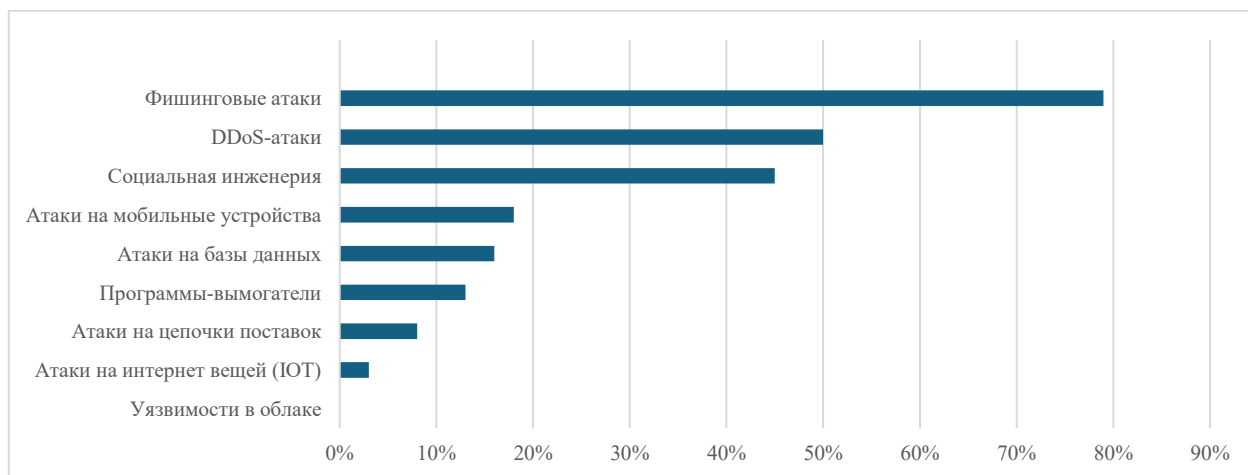


Диаграмма 2. Виды угроз экономической безопасности за 2024 год [2, с. 2]

Самый распространенный тип атак - фишинг, с ним за последний год столкнулось почти 80% компаний, около половины опрошенных испытали на себе влияние DDoS-атак¹ и социальной инженерии.

В этом контексте особое значение приобретает анализ и актуальная интерпретация теоретико-методологических основ реализации экономической безопасности высокотехнологичных компаний в условиях, характеризующихся ускорением процессов цифровой трансформации.

К моменту разработки национальной программы «Цифровая экономика Российской Федерации» наша страна прошла через значительные изменения, от командной системы к реставрации рыночной и постепенной адаптации к новой цифровой экономике. Эти изменения были вызваны необходимостью приспособления к условиям современных экономических тенденций, что требовало разработки и внедрения системных мер и инструментов для необходимой цифровой трансформации экономических реалий. Однако эти процессы крайне затруднены в связи с устаревшей инерцией управления, а также значительным недостатком IT-инфраструктуры

Исследователями сформулированы причины перестройки бизнес-процессов: «Переход к условиям цифровой трансформации был связан с развитием системных мер и инструментов по эффективному встраиванию в новую деловую среду, что в свою очередь выявило проблему обеспечения безопасности организации в условиях интенсивных информационных потоков и многообразия каналов их движения. Это очевидно требует коренной перестройки самих предприятий - поиска новых бизнес-моделей и перехода к ним» [8, с. 17].

Принятие данных мер способствовало становлению новой бизнес-среды, однако в процессе этих изменений была обнаружена основная проблема: низкий уровень обеспечения безопасности предприятий в условиях растущих информационных потоков и широкого распространения каналов передачи данных. В условиях современных вызовов необходимо уделить особое внимание фундаментальной трансформации высокотехнологичных предприятий, затрагивая все аспекты их деятельности. В первую очередь, это касается поиска и внедрения более эффективных бизнес-моделей, которые обеспечат устойчивое развитие и конкурентоспособность в условиях цифровизации. Данную стратегическую задачу ставит перед собой законодательство Российской Федерации.

¹ DDoS-атака (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании») - это тип DoS-атаки, при которой сервер, сервис или сеть перегружаются трафиком, поступающим из множества источников. Как и любая DoS-атака, DDoS нацелена на то, чтобы сделать систему жертвы недоступной.

Стратегия развития информационного общества в Российской Федерации на период с 2017 по 2030 годы, утвержденная Указом Президента РФ от 09.05.2017 № 203 ставит перед собой цели по обеспечению развития информационного общества, формированию национальной цифровой экономики, обеспечению национальных интересов и реализацию национальных приоритетов по цифровой трансформации. Кроме того, стратегия направлена на осуществление безопасности субъектов экономики в условиях функционирования новой цифровой среды. Основная направленность стратегии заключена и выражено в создании цифровых экономических экосистем [8, с. 22], основанных на равенстве между организациями-партнерами по «...взаимодействию принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан» [21].

Для осуществления стратегии по реализации и обеспечению безопасности высокотехнологичных предприятий в цифровом пространстве, необходимо отдать приоритет актуализации понятий, систематизации возможных принципов функционирования экономической безопасности и рассмотрению поэтапной трансформации предприятия, направленной на адаптацию к деятельности в условиях цифровизации.

Немаловажно упомянуть о том, что восприятие информационных технологий должно происходить не в виде «обслуживающего менеджмент инструментария, а должно восприниматься в качестве важного критерия, представляющего собой стратегические средства, позволяющие осуществлять сохранность и работать над улучшением занимаемых рыночных позиций. Информационные технологии также должны способствовать в выполнении такой работы, которая позволит осуществить перестройку всего предприятия в коренной степени, заостряя внимание на цифровой парадигме. Ключевым элементом осуществления данной трансформации будет возлагаться на системный подход в деятельности предприятия» [8, с. 18].

В различных исследованиях приведены разнообразные определения понятия «цифровое пространство», так или иначе отражающие суть, на основе которых необходимо заключить, что цифровое пространство в контексте современной экономики и экономической безопасности ВТП - это многомерная и динамичная среда, в рамках которой действует конкуренция и взаимодействие информационных потоков, включающих создание, восприятие, оценку и распространение информации. Эта среда тесно связана с разнообразными сегментами международного экономического, политического, социального и культурного сообщества. Цифровое пространство оказывает влияние на экономические процессы, мотивацию личности и общественные процессы, отражаясь на культурные,

экономические, политические и технологические аспекты общества. В условиях цифровой трансформации, это пространство становится ключевым элементом для обеспечения экономической безопасности высокотехнологичных предприятий, позволяя им адаптироваться к новым вызовам и угрозам.

Отмечается, что «необходимо учитывать важный фактор для формирования коннотации данного термина, что информационно пространство - исход взаимодействия информационных ресурсов, методов информационного взаимодействия и инфраструктуры. В рамках данного подхода к элементам информационного пространства относятся тип знаний, коммуникаций и субъектов, формирующих особую политику в информационном поле». [9, с. 49].

Таким образом, цифровое пространство формирует новую среду функционирования, в то время как цифровая трансформация представляет собой активный процесс адаптации к этой среде и её использования. Современные тенденции направлены на образование информационных бизнес-пространств и целых кластеров для стартапов и бизнесов, развивающихся в научно-техническом направлении [10, с. 29].

Конкретным выражением цифровой трансформации является то, что происходит интенсивное взаимодействие предприятий с Интернет-ресурсами, которое может носить как краткосрочный, так и долгосрочный характер. Тем или иным образом, оно выстраивается среди всех функционирующих предприятий. На фоне данных процессов каждое предприятие должно уделять внимание обеспечению экономической безопасности такого взаимодействия.

Наиболее распространенным является понимание понятия «экономическая безопасность» как факторы и условия, совокупность которых формирует развитие экономической защиты. В исследовании Страхова В.В. также дополнено, что акцент делается на «способности экономической системы к устойчивому развитию и противостоянию внешним и внутренним угрозам» [19, с. 3].

В современном понимании осуществление экономической безопасности на высокотехнологичных предприятиях понимается как деятельность систем ВТП, функционал которых, сосредоточен на обеспечении устойчивости и защите хозяйственной деятельности данных предприятий от возможных возникающих угроз и рисков, соотносящихся с экономическими факторами. Экономическая безопасность содержит в себе меры, направленные на обеспечение финансовой защищенности, неприкосновенность на технологическую и интеллектуальную собственность предприятия,

Обеспечение экономической безопасности высокотехнологичных предприятий зиждется на определении ключевых принципов [5, с. 5-7], классификация которых

разнообразна. Можно выделить различные группы принципов, которые так или иначе связаны с обеспечением экономической безопасности высокотехнологичных предприятиях в условиях цифровой трансформации.

Таблица 1

Анализ принципов обеспечения экономической безопасности ВТП

1	Принцип управления интеллектуальным капиталом и R&D	Интеллектуальная собственность (ИС) является ключевым активом и источником конкурентных преимуществ ВТП. Стратегические инвестиции в R&D и эффективное управление ИС напрямую определяют уровень экономической безопасности, создавая основу для долгосрочной конкурентоспособности и устойчивости компании.
2	Принцип риск-ориентированного управления	Управление компанией должно строиться на постоянном выявлении, оценке и минимизации рисков во всех видах деятельности (операционной, инвестиционной, финансовой). В условиях цифровизации этот подход становится центральным. Данный принцип находит свою реализацию в разработанном стандарте управления рисками ISO 31000 [12]. Эта модель эффективна для структурированного анализа, но статична и не адаптирована к динамике цифровых рисков.
3	Принцип проактивности и динамического анализа	Обеспечение безопасности требует не ретроспективного, а перспективного подхода, ориентированного на будущее. Необходимо применять динамические методы анализа для прогнозирования долгосрочных трендов и заблаговременного реагирования на угрозы.
4	Принцип цифровой устойчивости	Компания должна активно внедрять цифровые технологии во все сферы деятельности, формируя способность не только противостоять цифровым угрозам, но и использовать открывающиеся возможности (риски-шансы) для роста производительности и конкурентоспособности.
5	Принцип технологического суверенитета	Достижение технологической независимости и глобальной конкурентоспособности обеспечивается через опору на собственные исследования и разработки (R&D). Стратегические инвестиции в R&D позволяют создавать прорывные продукты и технологии, снижая критическую зависимость от иностранных решений и укрепляя экономическую безопасность как компании, так и страны в целом. [1, С.10-11]
6	Принцип правового соответствия	Деятельность ВТП должна строго соответствовать требованиям законодательства, ГОСТов и технических правил. Это позволяет не только избежать санкций со стороны государственных органов, но и использовать систему норм в качестве инструментария для правовой и технической защиты своих интересов, включая вопросы оборота интеллектуальной собственности и цифровых активов [16, С. 324-325].
7	Принцип управления цифровыми компетенциями	Успешная цифровая трансформация невозможна без управления кадровыми рисками. Необходимо целенаправленно развивать цифровые навыки персонала, регулировать текучесть кадров и работать с «цифровым разрывом» в квалификации сотрудников.

На основании изученных принципов можно заключить, что обеспечение экономической безопасности высокотехнологичных предприятий в условиях цифровой трансформации, необходимо соблюдать и выполнять комплекс подходов, что будет способствовать минимизации рисков и обеспечения риска развития бизнеса.

Условия, созданные информационной экономикой, ставят перед предприятиями значительные вызовы. Одной из ключевых проблем является недостаточная связь между бизнес-стратегией и стратегией развития информационных технологий в IT-секторе. Это несоответствие может проявляться в различных аспектах, таких как несоответствие информационных систем потребностям бизнеса и недостаточное использование современных технологий для оптимизации бизнес-процессов. В результате общая производительность и конкурентоспособность компании снижаются. Такая несовместимость может проявляться в различных частностях, например, несоответствии информационных систем потребностям и требованиям бизнеса, недостаточном использовании современных технологий для оптимизации бизнес-процессов и других направлениях развития стратегических направлений компании.

К основным проблемам, проявляющимся в экономической системе и возникающим под воздействием тенденции всеобщей цифровизации стоит отнести:

1) активное внедрение и распространение технологий искусственного интеллекта и автоматизации предприятия, которые нельзя рассматривать как исключительно позитивный фактор трансформации, так как данная тенденция в состоянии породить собой лавинообразные изменения экономики предприятия, выражаясь, например, в снижении уровня контроля над управлением предприятием, а также в повышении безработицы и сокращении рабочих мест - т.н. «технологическая безработица»;

2) угроза кибератак и киберпреступности, что может спровоцировать собой утечку конфиденциальных данных, на фоне чего также может произойти потеря доверия со стороны потребителя и существенные стратегические потери для организации;

3) неравный доступ к цифровым технологиям и ресурсам среди предприятий разных ступеней развития, может в наиболее выраженной форме увеличивать разрыв между развитыми и развивающимися предприятиями, а также в состоянии оставить свой отпечаток на различных слоях населения;

Одним из ключевых факторов, негативно влияющих на этот разрыв, является неполноценное финансирование R&D-проектов² в области цифровых технологий. Например, малые ВТП зачастую не имеют ресурсов для разработки и развития собственных решений в области кибербезопасности или внедрения ИИ, что делает их зависимыми от устаревших

² R&D (Research and Development) проекты – это комплекс мероприятий, направленных на поиск инновационных решений и создание новых технологий

сторонних платформ. Государственные и корпоративные R&D-инициативы, как показывает опыт «Сбербанка» и «Ростеха», позволяют создавать адаптивные инструменты, снижающие риски цифровизации для предприятий любого масштаба.

В частности, это подтверждается проведенными исследованиями Института статистических исследований и экономических знаний НИУ ВШЭ по оценке динамики расходов на НИОКР среди промышленных компаний России.

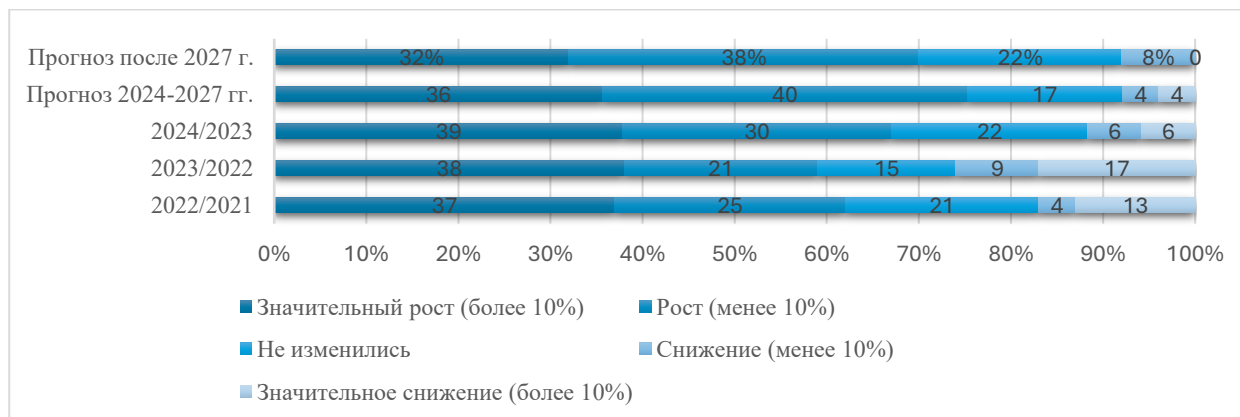


Диаграмма 3. Оценка динамики расходов на НИОКР, %

4) необходимость обновления и развития навыков цифровой среды в процессе кадровой работы, в рамках которой подразумевается систематическое и системное обучение сотрудников предприятия, направленное на повышение и актуализацию их цифровой грамотности, что в текущих условиях уровень цифровых компетенций зачастую не соответствует необходимым стандартам и подчеркивает важность данной инициативы для обеспечения конкурентоспособности предприятия;

5) Ослабление конкуренции на рынке труда и, что еще важнее, в областях высоких технологий и продуктов может быть результатом неравенства в распределении цифровых ресурсов и возможностей. Если ряду компаний удастся получить доступ ко всем новейшим технологиям и высококвалифицированным специалистам, в то время как другие компании используют устаревшие методы, это создает риск создания монополий, а также олигополий, которые в свою очередь снижают инновационную активность, а тем самым уменьшают разнообразие рынка, снижая качество с точки зрения производимых товаров и услуг. Такой сценарий не только снижает перспективы роста отдельного ВТП, но и наносит вред общей экономической системе;

6) Исследователи указывают, что «особое внимание следует уделить формированию культуры управления рисками, предполагающей осознание важности данных процессов всеми сотрудниками организации и их активное вовлечение в идентификацию рисков и реализацию

контрольных процедур. Формирование культуры управления рисками требует систематической работы по повышению осведомленности сотрудников о рисках, развитию необходимых компетенций и созданию условий для открытого обсуждения рисков на всех уровнях организации» [20, с. 4].

7) Существенное фактором по мнению исследователей также является неразвитый потребительский рынок, усиливающий иные негативные факторы, влияющие на экономику предприятия в процессе цифровой трансформации [14, с. 13].

Таким образом, рассмотренные принципы и описанные вызовы формируют комплекс внешних и внутренних условий, в которых эффективное функционирование ВТП невозможно без фундаментальной перестройки их бизнес-модели и систем управления. Данный процесс адаптации к условиям цифровой экономики характеризуется прохождением нескольких ключевых ступеней.

Таблица 2

Поэтапный план трансформации ВТП в условиях цифровой трансформации

Стадия	Условия	Действия	Итог	Пример реализации в российских компаниях
1	Наличие четкой стратегии и необходимых инструментов для ее реализации и адаптации	Внедрение интегрированной системы бизнес-модели, которая объединяет стратегию предприятия и инструменты для ее реализации, а также устраняет организационные разрывы	Процесс модернизации внутренней структуры предприятия для повышения ее эффективности и оптимизацию бизнес-процессов	Сбербанк: переход от традиционного банкинга к экосистеме (SberMarket, SberHealth) через цифровую платформу SberCloud (ныне Cloud) [11]
2	Наличие архитектуры предприятия, включающей системы управления,	Развитие системы управления на основе архитектуры предприятия, объединяющей все компоненты осуществляемой	Формирование целостной системы управления, способствующей более эффективному	Ростех: создание единой ERP-системы (SAP) ³ для 700+ предприятий, включая цифровые двойники

³ ERP (Enterprise Resource Planning) - это система планирования ресурсов предприятия, которая оптимизирует основные бизнес-процессы организации в сфере финансов, кадровых ресурсов, производства, поставок и закупок. Все эти процессы интегрированы в одну единую систему.

	процессы, людей, информацию и инфраструктуру	деятельности, что обеспечивает более эффективное взаимодействие всех элементов предприятия	взаимодействию всех компонентов предприятия и повышению общей производительности	производственных линий [17]
3	Наличие бизнес-стратегии и стратегии информационных технологий	Интеграция архитектуры предприятия с бизнес-стратегией и стратегией информационных технологий, что позволяет создать единое информационное пространство	Преобразование и расширение внешней информационной среды для создания единого информационного пространства, необходимого для цифровой экономики функционирования в условиях цифровой экономики	Яндекс: интеграция сервисов (Такси, Доставка, Маркет) через API ⁴ и Yandex.Cloud, что потенциально сократит время обработки данных на 25% [15]

На основе проведенных исследований [8, с. 20] представленные этапы трансформации демонстрируют, что синтез управленческих и технологических элементов, выраженный в применении цифрового пространства как инструмента управления рисками, реализуется через поэтапную интеграцию стратегических основ. Как справедливо отмечает Докукина А.А., «архитектура предприятия в условиях цифровизации становится не набором технологий, а платформой для трансформации бизнес-моделей и корпоративной культуры» [8, с. 21]. В таблице указано примеры поэтапной реализации изменений в российских компаниях:

Этап 1 иллюстрирует переход к улучшенной структуре предприятия, путем уменьшения и искоренения организационных пробелов. Таким примером послужит экосистемная модель «Сбербанка», где на базе SberCloud - единой IT-платформы позволило интегрировать банковские и нефинансовые сервисы, такие как SberMarket, SberHealth. Это и подтверждает тезис о том, что устранение организационных пробелов между

⁴ API (Application Programming Interface) - интерфейс прикладного программирования, набор правил и протоколов, которые позволяют разным программам взаимодействовать друг с другом, в данном случае с внешними сервисами.

подразделениями способствует созданию адаптивной архитектуры. Однако, как показала практика, даже столь успешный кейс не лишен противоречий: внедрение единой ИТ-платформы потребовало сокращения 14% штата традиционных отделов в 2021-2022 гг., что вызвало социальную напряженность.

Этап 2 направлен на формирование единой ERP-системы и цифровых двойников реализованной «Ростех», иллюстрирует интеграцию «пассивных оснований» через синтез информационных потоков из 700+ предприятий. Этот процесс, однако, выявил «парадокс цифровизации» - автоматизация производственных линий на 23% увеличила киберриски из-за роста уязвимых точек доступа. Как подчеркивают исследователи, «технологическая модернизация без параллельного развития систем безопасности создает эффект цифровой инфантильности предприятия» [14, с. 17].

Этап 3 связанный с созданием единого API-интерфейса, адаптированного в «Яндекс», через Yandex.Cloud отражает переход к динамичному синтезу бизнес-стратегии и ИТ-инфраструктуры. Но, как свидетельствуют данные, масштабирование экосистемы привело к 40-процентному росту инцидентов, связанных с несанкционированным доступом к API-ключам в 2023 году, что подтверждает тезис о необходимости «цифровой зрелости» как обязательного условия трансформации.

Следует отметить, что представленные кейсы отражают опыт крупных корпораций, в то время как малые ВТП могут сталкиваться с дополнительными барьерами (например, дефицит финансирования ИТ-инфраструктуры).

В этом процессе также устанавливаются его структура, контекст и стандарты, которым будет следовать предприятие. Эти основы для осуществления процесса оказывают поддержку корпоративной стратегии организации, направленной на планирование развития бизнес-процессов и ИТ-систем. Таким образом, предприятие проходит через эволюцию, переходя к новой, уникальной архитектуре, в которой интегрированы различные основы. Эти основы включают:

1) структурные основания - основные организационные единицы предприятия, которые отвечают за выполнение ключевых функций и задач. Они обеспечивают структуру и порядок внутри компании, способствуя эффективному управлению и координации деятельности;

2) поведенческие основания - правила и стандарты поведения, которые устанавливаются и поддерживаются внутри организации. Они определяют, как сотрудники должны взаимодействовать друг с другом и с внешними партнерами, создавая гармоничную рабочую среду;

3) пассивные основания - инфраструктурные компоненты и технические ресурсы, которые обеспечивают функционирование бизнес-процессов и IT-систем;

4) основания мотивации и целеполагания- механизмы, правовые нормы, принципы действия, ценности, рыночные драйверы, направленные на стимулирование сотрудников к достижению целей предприятия.

Концепт формирования архитектуры предприятия определяется не только информационными, организационными и функциональными процессами, но также определяет взаимосвязи между структурными и информационными системами организации.

Как указывают исследователи наиболее корректным будет применение дефиниции - архитектура системы, поскольку «архитектура предприятия строится на идеях и методах системного анализа и системной инженерии» [9, с. 194].

Архитектуру предприятия можно рассматривать как аппарат управления, где интегрируются в единую систему все ключевые элементы для обеспечения устойчивого функционирования ВТП и достижения поставленных стратегических целей.

Данная архитектура предусматривает под собой внутреннюю цифровую среду, которая складывается из различных цифровых данных. Эти данные дают всеобъемлющую информацию об экономической, технологической и хозяйственной деятельности компании, а также глубину ресурсного потенциала и состояние технологической среды. Основное назначение внутренней цифровой среды - гарантирование точного и надежного определения основных показателей компании, которые охватывают экономические, финансовые, материальные и трудовые ресурсы.

Поэтому важно разработать стратегии, которые будут поддерживать здоровую конкурентную среду так, чтобы все участники рынка развивались в наиболее из возможных равных условиях, что в то же время усилит импульс для стимулирования инноваций.

Согласно проведенным исследованиям основным проблем, возникающим в цифровой трансформации бизнеса, можно выделить следующее распределение:

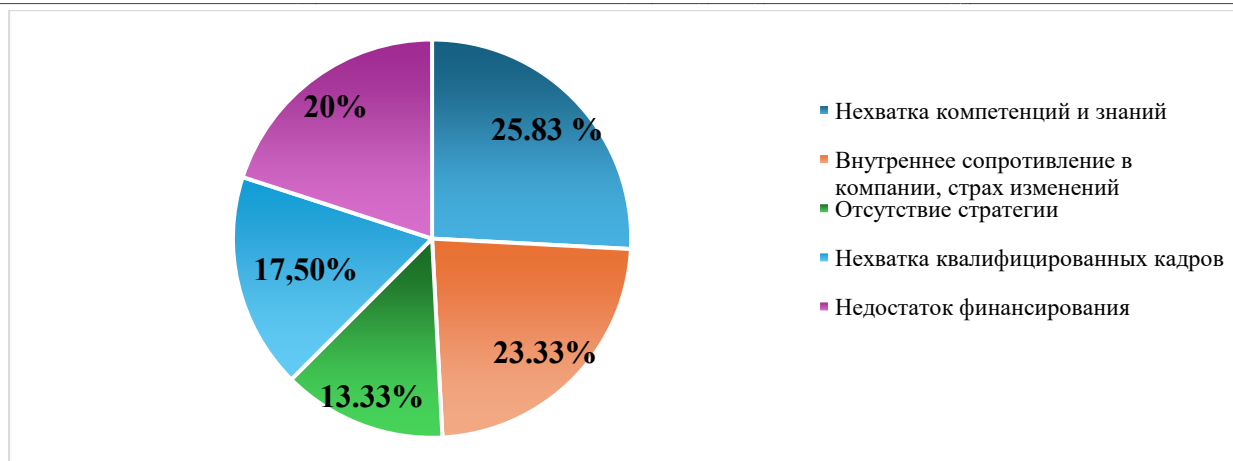


Диаграмма 4. Распределение основных проблем цифровой трансформации бизнеса в российских компаниях [13, с. 6]

В условиях информационной трансформации в связи с выявленными недостатками и необходимостью их исправления высокотехнологичные предприятия должны быть оснащены инструментами, которые помогут им прогнозировать, выявлять и управлять новыми тенденциями. Стремление компаний к формированию экономической системы ярко демонстрирует, что бизнес постоянно ищет эффективные методы, способные обеспечить успех в условиях новой экономической среды. Данные методы должны позволять использовать преимущества цифровизации, одновременно защищая от серьезных угроз, связанных с объемами и способами обмена данными.

Сформировавшиеся бизнес-модели и их модификации, разработанные с учетом возможных угроз новой экономики, сталкиваются с концептуальными проблемами. Эти проблемы приобретают критический характер под воздействием рассмотренных обстоятельств, характеризующих современную хозяйственную деятельность.

Однако «несмотря на высокую степень изученности, в теоретическом и практическом отношении сфера риск-менеджмента не свободна от ряда принципиальных противоречий, которые препятствуют использованию ее положений для целей создания научной платформы экономической безопасности. Это касается, например, отсутствия в экономической науке общепринятого понимания категории риска, объективного определения риск-менеджмента, единого отношения к возможностям прогнозирования и снижения неопределенности» [7, с. 1113].

Возможное решение проблем критического характера, выраженное в разработке теоретических бизнес-моделей и систем оценки экономической безопасности предприятий в условиях цифровой трансформации возможно на основе прикладной науки о безопасности и

рисках – синдиники и ее взаимодействию с другими моделями осуществления экономической безопасности.

Как отмечает в своих исследованиях Докунина А.А, «комплексная задача синдиники состоит в том, чтобы выявлять факторы, которые могут вызвать несчастные случаи, регулярно оценивать и изучать риски и угрозы, а также находить решения, которые могут уменьшить или устранить опасности и улучшить защиту. Методы синдиники можно исследовать с целью, например, приложения моделей анализа в ситуациях несчастных случаев к задачам бизнеса и производства и выявлять условия, на которые можно повлиять. Эта система предполагает формирование универсального инструментария предупреждения рисков, который включает стратегию, производство, финансы, менеджмент, технологии, персонал, информационные ресурсы» [6, с. 152].

Синдиника носит междисциплинарный характер и исследует взаимодействие человека с технологиями на основе социогенной точки зрения, отдавая предпочтение техническим факторам. И также изучает процесс интеграции технологических инноваций в существующие системы с точки зрения их влияния на бизнес-процессы и экономическую безопасность в отношении устойчивого развития. «Она не заменяет, а дополняет классические подходы, переводя анализ рисков на уровень системных взаимодействий» [6, с. 153].

Таким образом, можно сформулировать, что синдиника - научное направление, способное с помощью своей методологии анализировать техногенные риски через призму их взаимосвязей и нелинейного воздействия на экономическую безопасность.

Классическая форма анализа рисков предполагает «формулирование двухмерной модели сочетания вероятности с возможными последствиями, что несмотря на полезность, является недостаточным инструментом. Через призму синдиники риск рассматривается не как изолированное явление, а как элемент, тесно связанный с широким спектром факторов, включая изменения в окружающей среде, технологический прогресс и социально-экономическую динамику. Синдинический метод дает основу для получения последующих ответов на ключевые вопросы управления рисками:

- каким образом можно идентифицировать риск?
- как производится его количественная оценка?
- какие последствия может иметь его материализация?
- какие стратегии существуют для предотвращения, снижения или устранения риска?» [4, с. 506]

Также в контексте рассматриваемой проблемы в отличие от традиционного риск-менеджмента, который фокусируется на локальных угрозах, синдика может применяться следующим образом:

1. В качестве инструмента для анализа техногенных факторов выявление и анализ факторов, которые оказывают непосредственное влияние на экономическую безопасность предприятия, среди них новые технологии, риски и возможности, которые они приносят. Например, исследование новых технологий может выявить возможные риски и угрозы или новые возможности для повышения эффективности и наоборот.

2. Основа, сочетающая подходы из поведенческих и технических наук - разработка методологии для формирования комплексного подхода к оценке экономической безопасности с учетом как технологических, так и экономических аспектов. Это позволяет выявить, как, например, недостаточная цифровая грамотность сотрудников повышает уязвимость систем к фишинговым атакам, даже при наличии современных средств защиты.

3. Разработка стратегии - прогнозирование и разработка стратегий минимизации рисков и максимизации выгод цифровой трансформации. Включает стратегии информационной безопасности, стратегии управления рисками и стратегии финансовой стабильности. Примером может служить стратегия информационной безопасности, которая будет результатом модернизации систем кибербезопасности и поддержания обновленных версий антивирусного программного обеспечения.

4. Расширение применения новых технологий - формирование методологического инструментария для интеграции новых технологий в существующие процессы и методы. При данном внедрении появляется возможность по реинжинирингу всей системы, направленному на наиболее рациональную адаптацию к инновациям, чтобы сделать ВТП более конкурентоспособным на рынке и, таким образом, сохранить свои позиции.

Кроме того, особое внимание в углублении применения новых технологий необходимо обратить на внедрение систем искусственного интеллекта. ИИ может быть использован в достаточно широком спектре операций, направленных не только на наиболее очевидные функции по выявлению аномалий и прогнозированию потенциальных угроз информационного пространства, но также и на внедрение маркетинговых и производственных стратегий, которые помогут оптимизировать производственные процессы и углубить анализ рынка, тем самым повышая эффективность предприятий.

При изучении синдиники как теоретической основы необходимо затронуть рассмотрение актуальной концепции управления предприятием, которая соответствует требованиям цифровой трансформации и основывается на четко определенном алгоритме

реализации, а именно - пятимерной модели обеспечения безопасности - методологии, которая помогает предприятиям обеспечить экономическую безопасность через анализ ключевых элементов предприятия: финансы, производство, технологии, кадры и управление.

Таблица 2

Пятимерная модель в контексте применения инструментов синдиники в качестве ответа на риски и угрозы

Элемент модели	Риски	Инструменты синдиники
Финансы	Потери из-за DDoS-атак	Сценарное моделирование убытков
Производство	Простои автоматизированных линий	Анализ влияния сбоя на цепочку поставок
Технологии	Уязвимости IoT-устройств	Стресс-тестирование в виртуальной среде
Кадры	Ошибки персонала	Тренинги + мониторинг поведения
Управление	Неэффективные решения	Системная динамика для оптимизации

К данной методологии, на наш взгляд, для полноценного обеспечения безопасности ВТП необходимо использовать приведенный ранее алгоритм применения, что в свою очередь, позволит анализировать различные факторы, интегрировать технологии, оценивать и разрабатывать стратегии по каждому из пяти направлений пятимерной модели обеспечения безопасности.

Проведенное исследование позволяет заключить, что обеспечение экономической безопасности высокотехнологичных предприятий (ВТП) в условиях цифровой трансформации требует системного подхода, интегрирующего управленческие, технологические и кадровые аспекты, предполагающего встраивание процессов управления рисками не только в систему контроля рисков, но и в общую систему корпоративного управления на базе информационных платформ, что обусловлено современными тенденциями.

Ключевым инструментом решения этой задачи выступает использование различных инструментов, включая как классический риск-менеджмент, так синдинику – междисциплинарную методологию, которая, фокусируется на анализе каскадных эффектов рисков и их нелинейного влияния на бизнес-процессы.

Основу архитектуры экономической безопасности ВТП может составлять пятимерная модель, охватывающая финансы, производство, технологии, кадры и управление. Реализация этой модели, требует перехода от реактивных к превентивным практикам:

1. Регулярные аудиты «цифровой зрелости», как в случае с внедрением SIEM-платформы, сократившей время восстановления после кибератак с 72 до 8 часов;

2. Создание междисциплинарных команд (ИТ-специалисты, экономисты, психологи) для анализа уязвимостей IoT-устройств;

3. Инвестиции в обучение персонала, учитывая, что примерно 70-80% инцидентов связаны с человеческим фактором.

Научная новизна исследования заключается в предложении адаптации синдиники к задачам ВТП, включая разработку стандартизированных протоколов анализа, апробированных в российских корпорациях. Например, интеграция API-интерфейсов в экосистему Яндекса позволила сократить время обработки данных на 25%, однако выявила рост инцидентов с несанкционированным доступом на 40%, что подтверждает необходимость «цифровой зрелости» как обязательного условия трансформации.

Однако внедрение предложенной модели сталкивается с институциональными барьерами: лишь незначительный процент российских ВТП применяют системный подход к управлению рисками; ощущается дефицит финансирования ИТ-инфраструктуры в малых предприятиях; проявляется недостаток квалифицированных кадров для реализации принципов и методик экономической безопасности, в том числе и на основе синдинической модели.

Для преодоления этих ограничений необходима государственная поддержка, включая: финансирование R&D-проектов в области кибербезопасности; разработку отраслевых стандартов для синдинического анализа; внедрение образовательных программ по цифровой грамотности.

Список литературы

1. Авдеева И.Л., Азиева З.И., Утевская А.П. Развитие технологического предпринимательства для обеспечения технологического суверенитета Российской Федерации // Естественнo-гуманитарные исследования. 2023. № 2 (46). С. 10-16.
2. Аналитика Гарда. Активная защита от киберугроз. Август 2024. URL: <https://garda.ai> (дата обращения: 30.01.2025).
3. Артемьев Н.В., Митяков Е.С. Система экономической безопасности организации в условиях инновационных и цифровых преобразований // Вестник Московского университета МВД России. 2024. № 3. С. 231-239.
4. Бурак П.И., Бауэр В.П. Синдинический метод выявления и анализа опасностей для участников цифровых платформ // Экономическая безопасность. 2024. Т. 7. № 3. С. 499-522.
5. Гундорова М.А. Экономическая безопасность: учеб. пособие. Владимир: Изд-во ВлГУ, 2020. 207 с.

6. Докукина А.А. Пименов В.В. Обеспечение экономической безопасности предприятия через призму синдиники как науки об опасности // Вестник РЭУ им. Г.В. Плеханова. 2024. Т. 21. № 1 (133) С. 148-159.
7. Докукина А.А. Теоретические основы концепции экономической безопасности предприятия в контексте цифровой трансформации // Экономика, предпринимательство и право. 2023. Том 13. № 4. С. 1105-1124.
8. Докукина А.А. Экономическая безопасность предприятий в условиях цифровой трансформации // Вестник Российского экономического университета им. Г.В. Плеханова. 2022. № 3. С. 16-30.
9. Кудрявцев Д.В., Арзуманян М.Ю. Архитектура предприятия: переход от проектирования ИТ-инфраструктуры к трансформации бизнеса // Российский журнал менеджмента. 2017. Т. 15. № 2. С. 193-224.
10. Крикунов И.С. Цифровая экономика как фактор обеспечения экономической безопасности России // Прогрессивная экономика. 2023. № 5. С. 18-31.
11. Материал к конференции ИТ-технологий Cloud.ru. URL: [https://www.tadviser.ru/index.php/Компания\Cloud.ru_\(Облачные_технологии\)_ранее_SberCloud](https://www.tadviser.ru/index.php/Компания\Cloud.ru_(Облачные_технологии)_ранее_SberCloud) (дата обращения: 02.02.2025).
12. Международный стандарт ISO 31000:2018. URL: <https://certgroup.org/wp-content/uploads/2021/01/iso-31000-2018.pdf>.
13. Мозговой А.И. Организационно-экономические проблемы цифровой трансформации бизнеса российских предприятий и пути их решения // Вестник евразийской науки. 2022. Т. 14. № 5. С. 1-12.
14. Петров А.А. Цифровизация экономики: проблемы, вызовы, риски // Торговая политика. 2018. № 3 (15). С. 9-31.
15. Преимущества интеграции API для сайта: повышение эффективности и функциональности. URL: <https://siabit.ru/veb-studiya/preimushhestva-integraczii-api/> (Дата обращения: 27.01.2025).
16. Прилуцкая А.М. Принципы и элементы экономической безопасности организации // Форум молодых ученых. 2021. № 4 (56). С. 322-329.
17. Ростех создал программную платформу для цифровых производств. URL: <https://rostec.ru/media/news/rostekh-sozdal-programmnuyu-platformu-dlya-tsifrovyykh-proizvodstv/> (дата обращения: 01.02.2025).

18. Сидорова А.П. Понятие цифрового пространства и его характеристики. Возможности и угрозы использования цифрового пространства // Научный диалог: молодой ученый. 2021. № 4. С. 48-55.
19. Страхов В.В. Цифровизация как инструмент обеспечения экономической безопасности // Вестник евразийской науки. 2025. Т. 17. № 1. С. 1-13.
20. Тургаева А.А. Системный подход к управлению рисками, основанный на системе внутреннего контроля // Вестник евразийской науки. 2025. Т. 17. № 3. URL: <https://esj.today/PDF/06FAVN325.pdf> (Дата обращения: 19.09.2025).
21. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // КонсультантПлюс.

ESSENCE, PRINCIPLES AND METHODS OF ECONOMIC SECURITY OF HIGH-TECH ENTERPRISES IN THE CONDITIONS OF DIGITAL TRANSFORMATION

Kuznetsov Egor Sergeevich

Voronezh Institute of Economics and Law
Voronezh, Russian Federation

Kazmina Irina Vladimirovna

Doctor of Economics, Associate Professor
Air Force Academy named after. Prof. N.E. Zhukovsky and Y.A. Gagarin,
Voronezh, Russian Federation

Abstract. The article analyses the transformation of business processes of high-tech enterprise in the digital economy, focusing on the problems and principles of economic security, as well as the methodology for overcoming threats. In the context of increasing cyber threats and digitalisation of key industries, the paper substantiates the need to transition to a systemic management architecture that integrates technological, organisational and human resources aspects. Using the example of Russian cases (Sberbank, Rostec, Yandex), a step-by-step transformation model is demonstrated, including:

1. Formation of digital platforms to bridge organisational gaps;
2. Implementation of ERP systems and digital twins;
3. Creation of a unified information space through API integration.

The key methodological basis of the study is syndinics - a multidisciplinary approach that combines technogenic risk analysis, social engineering practices and predictive modelling. The study considers the possibility of applying a five-dimensional safety model covering finance, production, technology, human resources and management. Its testing revealed a key contradiction of digital transformation: technological innovation, while increasing operational efficiency, simultaneously generates new risks. For example, the integration of API interfaces into ecosystems (Yandex case) reduced data processing time by 25%, but increased the number of unauthorised access incidents by 40%. Syndonic methods, including cascading effects analysis and scenario-based threat modelling, are proposed to be adapted to address such problems.

Systemic limitations have been identified: only a few Russian high-tech companies apply a systemic approach to risks, a shortage of IT infrastructure financing in small businesses, and personnel imbalances. To overcome them, it is recommended to increase the measures of state support

for R&D projects, and also draws attention to the need to develop industry standards and educational programmes.

The study contributes to the theory of economic security by proposing an adaptation of syndinics to the realities of digital transformation, and has practical relevance for businesses seeking to minimise operational and cyber risks. The data presented are based on analyses of reports (Garda, 2024), strategic documents (Presidential Decree № 203) and cases studied.

Key words: digital transformation, enterprise architecture, essence, principles, economic security, high-tech enterprise, digital environment risks, risk management, information technology, digital maturity, and syndinics.

References

1. Avdeeva I.L., Azieva Z.I., Utevsкая A.P. Development of technological entrepreneurship to ensure technological sovereignty of the Russian Federation // Natural sciences and humanities research. 2023. № 2 (46). P. 10-16.
2. Garda Analytics. Active protection against cyber threats. August 2024. URL: <https://garda.ai> (Date of access: 30.01.2025).
3. Artemyev N.V., Mityakov E.S. The system of economic security of an organization in the context of innovative and digital transformations // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2024. № 3. P. 231-239.
4. Burak P.I., Bauer V.P. Syndic method of identification and analysis of hazards for participants of digital platforms // Economic security. 2024. Vol. 7. № 3. P. 499-522.
5. Gundorova M.A. Economic security: textbook. stipend. Vladimir: Publishing House of the All-Russian State University, 2020. 207 p.
6. Dokukina A.A. Pimenov V.V. Ensuring the economic security of an enterprise through the prism of syndinics as a science of danger // Bulletin of the Plekhanov Russian University of Economics. 2024. Vol. 21. № 1(133). P. 148-159.
7. Dokukina A.A. Theoretical foundations of the concept of economic security of an enterprise in the context of digital transformation // Economics, entrepreneurship and law. 2023. Volume 13. № 4. P. 1105-1124.
8. Dokukina A.A. Economic security of enterprises in the context of digital transformation // Bulletin of the Plekhanov Russian University of Economics. 2022. № 3. P. 16-30.
9. Kudryavtsev D.V., Arzumanyan M.Y. Enterprise architecture: transition from IT infrastructure design to business transformation // Russian Journal of Management. 2017. Vol. 15. № 2. P. 193-224.
10. Krikunov I.S. Digital economy as a factor of ensuring Russia's economic security // Progressive Economics. 2023. № 5. P. 18-31.
11. Material for the IT Technology Conference Cloud.ru. URL: [https://www.tadviser.ru/index.php/Компания\Cloud.ru \(Cloudtechnologies\) RANE_SBERCLOUD](https://www.tadviser.ru/index.php/Компания\Cloud.ru (Cloudtechnologies) RANE_SBERCLOUD) (accessed 02.02.2025).
12. International standard ISO 31000:2018. URL: <https://certgroup.org/wp-content/uploads/2021/01/iso-31000-2018.pdf>.
13. Mozgovoy A.I. Organizational and economic problems of digital business transformation of Russian enterprises and ways to solve them // Bulletin of Eurasian Science. 2022. Vol. 14. № 5. P. 1-12.
14. Petrov A.A. Digitalization of the economy: problems, challenges, risks // Trade policy. 2018. № 3 (15). P. 9-31.
15. Advantages of API integration for a website: increased efficiency and functionality. URL: <https://siabit.ru/veb-studiya/preimushhestva-integraczii-api/> (date of access: 27.01.2025).
16. Prilutskaya A.M. Principles and elements of economic security of the organization // Forum of young scientists. 2021. № 4 (56). P. 322-329.

17. Rostec has created a software platform for digital production. URL: <https://rostec.ru/media/news/rostekh-sozdal-programmnuyu-platformu-dlya-tsifrovyykh-proizvodstv/> (date of access: 01.02.2025).
18. Sidorova A.P. The concept of digital space and its characteristics. Opportunities and threats of using digital space // Scientific dialogue: a young scientist. 2021. № 4. P. 48-55.
19. Strakhov V.V. Digitalization as a tool for ensuring economic security // Bulletin of Eurasian Science. 2025. Vol. 17. № 1. P. 1-13.
20. Turgaeva A.A. A systematic approach to risk management based on the internal control system // Bulletin of Eurasian Science. 2025. Vol. 17. № 3. URL: <https://esj.today/PDF/06FAVN325.pdf> (Date of reference: 19.09.2025).
21. Decree of the President of the Russian Federation dated May 9, 2017 № 203 «On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030» // Consultant Plus.