

МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Тверской государственный технический университет»  
(ТвГТУ)

**И.В. Вякина, А.В. Бойкова**

**ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ БИЗНЕСА  
В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

*Монография*

Тверь 2023

УДК 338.242:004.9  
ББК 65.29-983:32.97

Рецензенты: доктор экономических наук, доцент, проректор по научной и инновационной деятельности, декан инженерно-строительного факультета ФГБОУ ВО «Тверской государственный технический университет» Артемьев А.А.; доктор экономических наук, кандидат философских наук, доцент, заведующий кафедрой экономики предприятия и менеджмента ФГБОУ ВО «Тверской государственный университет» Беденко Н.Н.

Вякина И.В., Бойкова А.В. Экономическая безопасность бизнеса в условиях цифровизации: монография. Тверь: Тверской государственный технический университет, 2023. 172 с.

Раскрыты теоретические и практические аспекты обеспечения экономической безопасности бизнеса в условиях цифровой трансформации. Исследованы основные проблемы безопасности современного российского бизнеса, угрозы и риски хозяйственной деятельности. Особое внимание уделено оценке влияния цифровой трансформации контрольно-надзорной деятельности государства на экономическую безопасность бизнеса.

Рассчитана на работников научных организаций, государственных и региональных органов управления, преподавателей, студентов, магистрантов и аспирантов экономических направлений специальностей. Может быть использована в образовательном процессе студентами специальности 38.05.01 Экономическая безопасность и других направлений подготовки.

ISBN 978-5-7995-1297-2

© Тверской государственный  
технический университет, 2023  
© Вякина И.В., 2023  
© Бойкова А.В., 2023

## Оглавление

<b>Введение.....</b>	<b>5</b>
<b>Раздел 1. Экономическая безопасность хозяйствующего субъекта: теоретические основы.....</b>	<b>7</b>
1.1. Понятие экономической безопасности хозяйствующего субъекта.....	7
1.2. Ресурсы и функциональные составляющие экономической безопасности предприятия.....	14
1.3. Угрозы и риски хозяйственной деятельности.....	22
1.4. Оценка внешней среды и условий ведения бизнеса.....	32
<b>Раздел 2. Ведение бизнеса в условиях цифровизации.....</b>	<b>44</b>
2.1. Особенности цифровой трансформации экономики.....	44
2.2. Подходы к оценке уровня цифровизации.....	52
2.3. Цифровые угрозы экономической безопасности бизнеса.....	62
2.4. Методика оценки экономической безопасности хозяйствующих субъектов в условиях цифровизации.....	72
<b>Раздел 3. Цифровая трансформация контрольно-надзорной деятельности государства и ее влияние на бизнес.....</b>	<b>91</b>
3.1. Контрольно-надзорная деятельность государства в условиях цифровой трансформации.....	91

3.2. Взаимодействие бизнеса с контрольно-надзорными органами в контексте цифровизации.....	97
3.3. Оценка влияния реформы контрольно-надзорной деятельности на бизнес .....	102
3.4. Мнение бизнеса о результатах реформирования и цифровой трансформации контрольно-надзорной деятельности государства.....	108
<b>Раздел 4. Повышение уровня экономической безопасности бизнеса в условиях цифровой трансформации.....</b>	<b>114</b>
4.1. Государственная политика обеспечения экономической безопасности в условиях цифровизации.....	114
4.2. Перспективные направления повышения экономической безопасности на основе цифровизации: международный опыт.....	120
4.3. Направления повышения экономической безопасности предприятия в условиях цифровой трансформации.....	127
<b>Заключение.....</b>	<b>149</b>
<b>Библиографический список.....</b>	<b>151</b>
<b>Приложения.....</b>	<b>162</b>

## ВВЕДЕНИЕ

Переход к цифровой экономике сегодня становится неотвратимым явлением хозяйственной жизни. Согласно Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, под цифровой экономикой понимается хозяйственная деятельность, где ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг [6].

Стремительной цифровизации всех сфер хозяйственной жизни способствовала пандемия и вынужденное применение различных способов бесконтактного взаимодействия. Активное использование цифровых технологий, реестров, баз данных и различных систем для обработки, хранения данных и раскрытия информации, по всей видимости, в ближайшем будущем вызовет существенное изменение условий ведения бизнеса, что потребует развития методологии экономического анализа.

Цифровизация экономики порождает новые аналитические инструменты для мониторинга рыночной ситуации и выявления конкурентных преимуществ компаний, а также предоставляет дополнительные функциональные возможности для идентификации рисков и угроз. Адекватная оценка внешних рисков и угроз деловой среды позволяет обеспечивать безопасность хозяйственной деятельности компании и повышает качество управления.

Экономическая безопасность отражает возможности конкретного хозяйствующего субъекта использовать имеющиеся у него экономические преимущества и ресурсы для обеспечения своего устойчивого развития и противодействия потенциальным угрозам и рискам внешнего и внутреннего характера. Безусловно, достаточный финансовый потенциал дает возможность более эффективно решать эти задачи. Однако влияние внешних факторов на экономическую безопасность компании чрезвычайно велико. Сюда можно отнести не только сложившиеся в пространственной деловой среде условия ведения бизнеса, но и положение компании на рынке, особенности взаимоотношений с

контрагентами и конкурентами, ее конкурентные преимущества и потенциал для лидерства на рынке. Кроме того, большое значение при диагностике состояния экономической безопасности имеют качество и профессионализм менеджмента, степень финансовой прозрачности, соблюдение принципов корпоративного управления и норм права, особенности структуры собственности и др.

Таким образом, современные информационные технологии, с одной стороны, обеспечивают информационно-эмпирическую базу исследования. С другой стороны, использование современных информационных технологий и методик работы с базами данных, а также программных средств обработки экономической информации позволяет реализовать на практике предложенную автором методику и повысить достоверность полученных результатов.

Новая геополитическая реальность характеризуется беспрецедентным санкционным давлением на Российскую Федерацию практически во всех сферах жизни общества (международной дипломатии, экономике, культуре и т.д.), но наряду с новыми угрозами появляются новые возможности и потребности.

В условиях цифровой трансформации экономики, активного применения реестров, баз данных и различных систем для обработки, хранения данных и раскрытия информации создаются и новые возможности для развития методологии оценки экономической безопасности в части разработки аналитических методов идентификации потенциальных угроз и рисков, а также выявления конкурентных преимуществ и направлений развития компании с помощью современных информационных технологий.

Руководители предприятий и представители бизнеса до сих пор не понимают сути самой категории «экономическая безопасность предприятия» и не видят смысла в практическом применении методов ее оценки для выработки управленческих решений в отношении функционирования и развития конкретного хозяйствующего субъекта. Остаются нерешенными и весьма дискуссионные вопросы о методах диагностирования угроз, обуславливающих экономическую безопасность, а также о методических подходах к оценке ее уровня. Наличие комплекса нерешенных проблем (методологических, теоретических, эмпирических) означает необходимость дальнейшего исследования феномена цифровизации в рамках теории экономической безопасности и разработки методологии ее оценки.

# РАЗДЕЛ 1. ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА: ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

## 1.1. Понятие экономической безопасности хозяйствующего субъекта

Экономическая политика в современных условиях включает в себя взаимосвязь между безопасностью человека, пространственным развитием и обеспечением безопасности в широком смысле этого слова. Немалую роль в закреплении в сознании соответствующих представлений играет обсуждение проблем безопасности в средствах массовой информации.

Опасность – это возможность возникновения обстоятельств, которые могут привести к ухудшению состояния объекта, субъекта или системы, прекращению их дальнейшего функционирования и развития. Ни в одном виде деятельности абсолютная безопасность недостижима, поскольку сама жизнь потенциально опасна. Тем не менее для того чтобы иметь возможность развития и качественного улучшения, необходимо принятие мер, предупреждающих нежелательные события и дающих возможность обновления и поступательного движения.

Новая геополитическая реальность, беспрецедентное санкционное давление на Российскую Федерацию, пандемия и связанные с ней ограничения, мировой экономический кризис обусловили резкую смену социально-экономической парадигмы, которая займет доминирующую позицию в обозримом будущем. Несмотря на все различия отдельных стран и регионов, необходимость обеспечения безопасности и защиты собственных интересов определяет выбор механизмов и инструментов государственного управления. В настоящее время экономическая политика большинства стран во многом определяется повышением внимания к вопросам национальной безопасности. При этом все более актуальной становится проблема обеспечения баланса между сохранением национального суверенитета, достижением максимального общественного благосостояния и развитием рынка. Рынок, по своей сути, изначально предполагает наличие противоречий и несовпадение интересов различных агентов и их групп. Стоит отметить, что сегодня происходит формирование новой модели глобализации, характеризующейся ростом национализма, протекционизма, децентрализацией мировой экономики и политики при усилении цифровой интеграции.

В целом постановка проблемы безопасности зависит от выбора теоретического базиса и концептуального подхода к теории и предлагаемым способам решения.

В.К. Сенчагов [60, с. 101] выделяет три ключевые характеристики экономической безопасности – развитие, устойчивость и защищенность.

Развитие обеспечивает возможность выживания, сопротивляемость и приспособляемость к внутренним и внешним угрозам. «Устойчивость экономики характеризует прочность и надежность ее элементов, вертикальных, горизонтальных и других связей внутри системы, способность выдерживать внутренние и внешние нагрузки» [60, с. 98]. Защищенность представляет собой состояние, определяющее способность к выживанию и развитию в условиях внутренних и внешних угроз, под воздействием непредсказуемых и неопределенных факторов.

Ли Эндресс понимает под безопасностью экономических систем защиту от риска потери благосостояния [106, с. 49–66]. Он рассматривает взаимосвязь между дефицитом природных ресурсов, безопасностью и устойчивым развитием. Так, в его трактовке безопасность и экономическое благополучие базируются на следующих принципах устойчивого развития:

- моделировании воспроизводства ресурсов на основе определения динамической эффективности сложных систем;

- поддержании эффективных способов потребления и использования природных ресурсов;

- справедливом распределении благосостояния между поколениями в настоящем и будущем.

Развитие экономической системы представляет собой процесс направленных и закономерных технических, технологических, финансовых изменений, социальных, институциональных и правовых усовершенствований системы, приводящих к ее качественно новому состоянию, при котором отсутствует недопустимый риск.

Безопасность, с одной стороны, является многогранным понятием, исследование которого носит междисциплинарный характер, затрагивая социальные, технологические, экологические, правовые, политические, финансовые и экономические аспекты. С другой стороны, это многоуровневый концепт, включающий в себя международный, национальный, региональный, отраслевой, корпоративный, личностный уровни ее обеспечения.

Первое определение экономической безопасности в нормативных актах появилось в Федеральном законе от 13 октября 1995 года № 157-ФЗ «О государственном регулировании внешнеторговой деятельности» (утратил силу), где она трактуется как «состояние экономики, обеспечивающее достаточный уровень социального, политического и оборонного существования и прогрессивного развития Российской Федерации, неуязвимость и независимость ее экономических интересов по отношению к возможным внешним и внутренним угрозам и воздействиям» [3]. Впоследствии Указом Президента РФ от 29 апреля 1996 года № 608 была утверждена «Государственная стратегия экономической безопасности Российской Федерации (основные положения)» [2]. Сегодня понятие экономической безопасности прочно вошло в нормативные



документы и заняло значимое место в общественно-политических дискуссиях.

В настоящий момент принципы обеспечения национальной и экономической безопасности определяются Стратегией национальной безопасности [7] и Стратегией экономической безопасности Российской Федерации на период до 2030 года [9] (табл. 1).

*Таблица 1*

**Основные понятия и определения,  
приведенные в действующих нормативных документах  
по экономической и национальной безопасности**

Понятие	Стратегия национальной безопасности Российской Федерации [7]	Стратегия экономической безопасности Российской Федерации на период до 2030 года [9]
Национальная и экономическая безопасность	Национальная безопасность – состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются: реализация конституционных прав и свобод граждан; достойные качество и уровень жизни; гражданский мир и согласие в стране; охрана суверенитета Российской Федерации, ее независимости и государственной целостности; социально-экономическое развитие страны	Экономическая безопасность – состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются: экономический суверенитет страны; единство ее экономического пространства; условия для реализации стратегических национальных приоритетов
Национальные интересы	Национальные интересы – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития	Национальные интересы в экономической сфере – объективно значимые экономические потребности страны, удовлетворение которых обеспечивает реализацию стратегических национальных приоритетов
Обеспечение безопасности	Обеспечение национальной безопасности – реализация органами публичной власти во взаимодействии с институтами гражданского общества и организациями политических, правовых, военных, социально-экономических, информационных, организационных и иных мер, направленных на противодействие угрозам национальной безопасности	Обеспечение экономической безопасности – реализация мер, направленных на противодействие вызовам и угрозам экономической безопасности и защиту национальных интересов в экономической сфере

Проблема безопасности хозяйственной деятельности характерна для систем различного уровня и связана с процессами накопления, потребления и воспроизводства ресурсов, а также предполагает возможность и особенность собственного целеполагания и управления. Сбалансированность внутренних и внешних условий ее существования позволяет экономической системе реализовывать интересы текущего и будущего ее развития. Невозможность восстанавливать сбалансированность и равновесие системы в режиме авторегуляции вызывает необходимость управления. Наличие среди внешних условий экономической конкуренции, рыночной неопределенности и коммерческого риска приводит к необходимости создания системы экономической защищенности.

Концептуальные подходы к определению сущности категории «экономическая безопасность» можно систематизировать в рамках четырех нижеперечисленных целевых установок:

защищенность от угроз [62, с. 45; 23, с. 84];

эффективное использование ресурсов [34, с. 49; 35, с. 50];

способность к стабильному функционированию и устойчивому развитию [60, с. 98; 64, с. 29];

наличие конкурентных преимуществ и конкурентоспособность [23, с. 45; 28, с. 97].

Отметим, что понятие экономической безопасности на макроуровне достаточно широко применяется в научных и политических дискуссиях и закреплено в законодательных и нормативно-правовых актах, где определены и индикаторы для ее мониторинга и оценки. При этом вопросы четкого обоснования сущности и методологии мониторинга экономической безопасности на микроуровне остаются дискуссионными. Некоторые исследователи, например С.А. Афонцев [17, с. 20], полагают, что не имеет практического смысла использовать понятие «экономическая безопасность» на региональном и микроуровне.

Представляется, что на всех уровнях хозяйственной иерархии понятие экономической безопасности выражает то общее, что ему присуще, приобретая на каждом из них специфический характер, обусловленный особенностями соответствующего уровня управления экономическими системами.

На микроуровне, помимо факторов устойчивости экономического развития и безопасности экономических систем, диктуемых естественными требованиями конкурентной рыночной среды, связанными с обеспечением их конкурентоспособности и сохранения рыночных позиций, возникают специфические угрозы и риски, вызванные недобросовестной конкуренцией, деятельностью криминальных формирований и отдельных лиц, периодическим переделом собственности, борьбой за контроль над активами и пр.

Экономическую безопасность бизнеса целесообразно рассматривать непосредственно через восприятие предпринимателем данной категории, принимая во внимание, что он еще на стадии предпринимательского выбора оценивает потенциальные риски и угрозы, а также свою способность им противодействовать или нивелировать их. С этих позиций безопасность самой деловой среды оказывает влияние на экономическую безопасность предприятия, обуславливая определенный уровень внешних угроз и вызовов.

Экономическая безопасность хозяйствующего субъекта, по мнению Е.А. Олейникова, – это такое состояние юридических, производственных отношений и организационных связей, материальных и интеллектуальных ресурсов, при котором обеспечиваются стабильность функционирования, финансово-коммерческий успех, прогрессивное научно-техническое и социальное развитие [46, с. 129]. В.Л. Поздеев характеризует экономическую безопасность предприятия как способность его функционирования в заданных пределах ключевых параметров, или коридоре безопасности [51, с. 115], что позволяет обеспечить его прогрессивное развитие, неуязвимость и независимость экономических интересов по отношению к возможным внешним и внутренним угрозам и воздействиям.

В работе Р.В. Белозерцева и В.Н. Белозерцева экономическая безопасность предприятия определяется как «состояние, при котором обеспечивается наиболее эффективное использование всех видов ресурсов, устойчивое его развитие, осуществляется защита от имеющихся и потенциальных угроз и опасностей в условиях рынка» [19, с. 5].

В статье [16, с. 2274] отмечено, что экономическая безопасность предприятия рассматривается со стороны как того общего, что свойственно данной экономической категории (состояние экономической системы, при котором она имеет возможность эффективно функционировать и развиваться, обладая устойчивостью к различного рода угрозам и вызовам, а также способностью противодействовать им), так и того специфического, что характеризует первичные звенья экономики.

Л.М. Ширко рассматривает экономическую безопасность предприятия как состояние, при котором обеспечивается [67] устойчивость бизнес-процессов и рыночной позиции, а также эффективность решений, принимаемых в финансовой сфере, и действий персонала при выполнении хозяйственных операций.

Динамические изменения внешней среды закономерно требуют от российских предприятий бизнес-стратегии, направленной на организацию управления финансовыми потоками, материальными, информационными и человеческими ресурсами и позволяющей защищать собственные интересы и обеспечивать долгосрочное развитие. Иными словами, предприятия вынуждены совершенствовать свою внутреннюю организацию с целью достижения большей степени безопасности развития и экономического роста.

Для построения системы эффективного и безопасного развития предприятия нужно обеспечить четкость механизма управления через взаимоувязку стратегических, тактических и оперативных (текущих) планов с генеральной целью предприятия. Тем не менее на практике зачастую наблюдается частичная или даже полная нереализованность данного механизма управления предприятием, что связано с конфликтом интересов различных социальных, экономических и административных субъектов. Умелое управление процессами функционирования и развития определяет эффективность менеджмента предприятия, безопасность и перспективы развития.

Подходы к определению экономической безопасности предприятия, представленные в табл. 2, зависят от опыта, компетенции и субъективных предпочтений авторов.

*Таблица 2*

Подходы к сущности экономической безопасности предприятия [66]

Подход	Суть
Системный	Система мер, позволяющих обеспечить равновесие ресурсов и результатов функционирования предприятия; система управленческих решений на основе анализа внутренних и внешних по отношению к предприятию фактов действительности
Ресурсный	Обеспеченность предприятия ресурсами, поддержание должного уровня организации ресурсного обеспечения, позволяющего говорить о внутреннем равновесии всех систем предприятия
Информационно-правовой	Совокупность требований, предъявляемых к информации, источникам данных о состоянии и результатах финансово-хозяйственной деятельности предприятия; инструментарий для оценки информации о рыночной позиции предприятия, определяющий в совокупности уровень экономической безопасности, а также юридические последствия для самого предприятия и заинтересованных сторон
Организационный	Совокупность способов организации финансовых потоков на предприятии, обеспечивающих эффективность его деятельности
Рисковый	Способность успешно реагировать на условия, создающие риск, учитывать все вероятные проявления риска при выборе стратегии, оценивать последствия негативных событий в условиях динамики внешней среды

Мы понимаем под экономической безопасностью хозяйствующего субъекта такое состояние, при котором обеспечивается устойчивость его функционирования в пределах допустимого риска и развития, а также сохраняется его конкурентоспособность и способность сохранять и приумножать свой потенциал при наличии внешних и внутренних угроз.

Если экономическая система не развивается, то с течением времени она утрачивает способность адекватно реагировать на динамично

изменяющиеся условия внешней среды, сокращаются возможности ее выживания и сопротивляемости внутренним и внешним угрозам.

*Экономическое развитие* – процесс целенаправленных качественных или структурных положительных изменений и усовершенствований производственной, финансовой, коммерческой и иной деятельности, финансового положения, методов организации и управления, приводящий к новому, качественно лучшему их состоянию, повышению эффективности использования ресурсов в соответствии с поставленными целями.

Устойчивость экономической системы отражает прочность и надежность ее элементов, вертикальных, горизонтальных и других связей внутри системы, способность выдерживать внутренние и внешние нагрузки, восстанавливать нормальное состояние, нарушенное каким-либо внешним или внутренним фактором.

*Устойчивость* – способность сохранять целостность и качественно совершенствоваться в условиях изменяющейся внешней и внутренней среды, случайных или преднамеренных трансформаций (внутренних и внешних угроз).

*Финансовая устойчивость предприятия* – такое состояние процесса формирования и использования финансовых ресурсов экономического субъекта, которое обеспечивает его развитие на основе увеличения прибыли и стоимости капитала при сохранении соответствующего уровня платеже- и кредитоспособности. Финансовая устойчивость связана со способностью предприятия отвечать по своим долгосрочным финансовым обязательствам.

Специфика и различия экономических интересов разных участников рынка приводят к конфликтным ситуациям, связанным со столкновением этих интересов. Конкурентная борьба в условиях ограниченности экономических ресурсов – свойство, имманентно присущее рыночной экономике. Наличие среди внешних условий экономической конкуренции, рыночной неопределенности и коммерческого риска означает необходимость обеспечения конкурентоспособности хозяйствующего субъекта.

*Конкурентоспособность* – способность выдерживать конкуренцию в сравнении с аналогичными объектами на данном рынке. Конкурентоспособность предприятия обеспечивается конкурентной позицией, которую занимает фирма на рынке. Рыночное положение предприятия определяет наличие или отсутствие конкурентного преимущества, долю производимого вида продукции в российской экономике, известность торговой марки и т.п.

Рыночные позиции конкретного предприятия, его конкурентоспособность и экономическая устойчивость, особенности производственной, финансово-хозяйственной деятельности, стадии жизненного цикла и перспективы развития (внутренние условия) оказывают постоянное и непосредственное воздействие на его функционирование в

целом, обуславливают потенциал и возможности развития и уровень экономической безопасности.

Взаимосвязь между экономической безопасностью предприятия, возможностями его развития, финансовой устойчивостью и конкурентоспособностью заключается в следующем: низкий уровень экономической безопасности предприятия и недостаточный внутренний потенциал препятствуют поступательному и устойчивому развитию предприятия и негативно влияют на его способность противодействовать внешним и внутренним угрозам, тогда как при высоком уровне экономической безопасности предприятие способно поддерживать конкурентоспособность на более высоком уровне по сравнению с конкурентами и чувствовать себя в относительной безопасности при изменяющейся конъюнктуре рынка.

Категории «экономическая безопасность», «экономическое развитие», «финансовая устойчивость» и «конкурентоспособность» объединяют долговременный характер и стратегическую направленность на реализацию поставленных целей в будущем. Экономическая безопасность предприятия обеспечена, если независимо от состояния внешней среды оно может функционировать, имея при этом достаточную степень финансовой независимости, устойчивости и сбалансированности финансовых потоков; не допускать ущерба, связанного с утратой рыночных позиций и кадрового, имущественного или иного потенциала либо срывом достижения стратегических целей развития.

## **1.2. Ресурсы и функциональные составляющие экономической безопасности предприятия**

Ресурсно-функциональный подход к определению экономической безопасности и методологии ее оценки основан на предположении, что наиболее эффективное использование корпоративных ресурсов позволяет предотвратить опасности за счет укрепления внутреннего потенциала и создания условий для устойчивого развития.

Критерием оценки выступает уровень эффективности использования ресурсов по всем функциональным составляющим экономической безопасности (финансовой, технико-технологической, интеллектуальной, кадровой, нормативно-правовой, экологической, информационной, силовой и т.д.), то есть рациональное использование ресурсов рассматривается как основа для предотвращения угроз экономической безопасности. Оценка уровня экономической безопасности предлагается в виде системы функциональных составляющих, причем каждая из функциональных групп также представляет собой систему показателей.

В зависимости от целей исследования, научных интересов и компетенции авторы делают упор на различные аспекты обеспечения экономической безопасности, виды ресурсов и функциональные составляющие. Подобный подход применяется для определения и оценки экономической безопасности предприятия в работах [29, 32, 54, 71].

Под совокупностью корпоративных ресурсов обычно понимают факторы, используемые владельцами и менеджерами предприятия для достижения поставленных целей:

1. *Капитал.* Акционерный капитал в сочетании с заемными финансовыми ресурсами формирует «кровеносную систему» предприятия, позволяет приобретать и поддерживать остальные корпоративные ресурсы, изначально отсутствующие у данного предприятия.

2. *Персонал.* Менеджеры предприятия, штат инженерного персонала, производственных рабочих и служащих с их знаниями, опытом и навыками являются основными звеньями, связующими воедино все факторы данного бизнеса, и обеспечивают проведение в жизнь идеологии бизнеса и достижение целей.

3. *Информация и технологии.* Информация, касающаяся всех сторон деятельности предприятия, в настоящее время считается наиболее ценным и дорогостоящим ресурсом предприятия. Именно информация об изменении политической, социальной, экономической и экологической ситуации, рынков предприятия, научно-техническая и технологическая информация, конкретные ноу-хау, касающиеся каких-либо аспектов данного бизнеса, новые методы организации и управления бизнесом позволяют предприятию адекватно реагировать на любые изменения внешней среды бизнеса, эффективно планировать и осуществлять свою хозяйственную деятельность.

4. *Техника и оборудование.* Используя имеющиеся финансовые, информационно-технологические и кадровые возможности, предприятие приобретает технологическое и другое оборудование, необходимое (по мнению менеджеров предприятия) и доступное (исходя из имеющихся ресурсов).

5. *Права.* С развитием цивилизации, истощением природных ресурсов и повышением ценности для бизнеса нематериальных активов резко выросла роль правового ресурса. Этот ресурс включает в себя права на использование патентов, лицензии и квоты на применение природных ресурсов, а также экспортные квоты, права на пользование землей.

Функциональные составляющие экономической безопасности предприятия – это совокупность основных направлений его экономической безопасности, существенно отличающихся друг от друга по своему содержанию.

Наиболее часто используемая примерная структура функциональных составляющих экономической безопасности предприятия включает в себя

финансовую, кадровую и интеллектуальную, технико-технологическую, экологическую, информационную и силовую составляющие [70].

#### ***Финансовая составляющая***

Процесс обеспечения финансовой составляющей экономической безопасности предприятия может быть определен как совокупность работ по созданию максимально высокого уровня платежеспособности предприятия и ликвидности его оборотных средств, наиболее эффективной структуры капитала предприятия, повышению качества планирования и осуществления финансово-хозяйственной деятельности предприятия.

Значительной угрозой финансовой безопасности предприятия может служить недостаточный контроль за структурой вложений предприятия, соотношением частей финансового портфеля по рискованности и доходности его составляющих. Важным направлением обеспечения финансовой составляющей экономической безопасности предприятия является контроль всех сторон его хозяйственной деятельности с точки зрения повышения текущей рентабельности бизнеса, а также развития. Кроме того, большое значение для финансовой безопасности предприятия имеют, помимо платеже- и кредитоспособности, эффективность использования финансовых ресурсов и капитала, выполнение обязательств перед государством и другими хозяйствующими субъектами. С практической точки зрения следует учитывать, что диагностика факторов финансовой безопасности включает в себя также анализ способов привлечения капитала для поддержания платежеспособности компании на приемлемом уровне, рентабельности деятельности и роста стоимости компании или ее капитализации в долгосрочной перспективе.

#### ***Кадровая и интеллектуальная составляющая***

Обеспечение кадровой безопасности предприятия включает в себя два тесно связанных между собой направления деятельности:

1) ориентированность на работу с персоналом фирмы, на повышение эффективности работы сотрудников. Включает в себя мероприятия по планированию и управлению персоналом предприятия, предотвращению угроз негативных воздействий на экономическую безопасность предприятия за счет недостаточной квалификации сотрудников, слабой организации системы управления персоналом и т.п.;

2) сохранение и развитие интеллектуального потенциала предприятия. Среди основных объектов интеллектуальной собственности следует выделить изобретения, технические новации, ноу-хау, дизайнерские разработки, компьютерные программы и др. Негативными факторами для экономической безопасности фирмы являются недостаточная квалификация персонала, нежелание или неспособность работников приносить максимальную пользу предприятию. В связи с этим необходимы планирование и организация системы подбора, найма,



обучения, мотивации труда (в том числе денежной), чувство социальной защищенности работников фирмы и их обеспеченность социальными благами. Важно обеспечить соответствие квалификационного уровня персонала требованиям выполняемых ими работ, а также сочетать наем персонала на рынке труда с обучением и повышением квалификации собственных специалистов. С рисками в сфере управления персоналом связаны основные угрозы возникновения негативных воздействий в кадровой составляющей экономической безопасности предприятия.

Исследования показывают, что самое сложное звено в системе безопасности – это человек и что именно человеческий фактор может оказать значительное влияние на успешность деятельности и само существование компании. Поэтому в структуре экономической безопасности главную роль играет кадровая безопасность, которую можно определить как процесс предотвращения потенциальных и реальных угроз (рисков), связанных с персоналом (использованием трудового потенциала, развитием человеческого капитала, управлением человеческими ресурсами, совершенствованием трудовых отношений и т.д.). Иными словами, речь может идти, с одной стороны, о неосознанной угрозе со стороны персонала (в силу некомпетентности, халатности, случайной ошибки), а с другой – об осознанных действиях, связанных с воровством, мошенничеством, саботажем, взяточничеством, разглашением коммерческой тайны и другими противоправными действиями.

#### ***Технико-технологическая составляющая***

Сущность технико-технологической составляющей экономической безопасности предприятия заключается в установлении того, насколько уровень используемых на данном предприятии технологий и техническое оснащение соответствуют лучшим мировым аналогам. Важным моментом здесь является наличие у этих технологий потенциала развития и их будущей способности конкурировать с технологиями-заместителями и передовыми достижениями науки и техники.

Процесс обеспечения технико-технологической составляющей экономической безопасности предприятия нематериальной сферы тесно связан с обеспечением кадровой и информационной составляющих, так как увеличение производительности техники и оборудования предполагает повышение квалификации сотрудников, сбор и анализ информации о наиболее успешных практиках и достижениях.

#### ***Экологическая составляющая***

Фактор осознания необходимости сохранения окружающей среды далеко не всегда превалирует над коммерческими интересами организации. Поэтому для обеспечения соблюдения организациями норм экологической безопасности в большинстве стран мирового сообщества применяются

системы штрафов, налагаемых государственными организациями на предпринимателей, не соблюдающих экологическое законодательство.

С точки зрения хозяйствующего субъекта основная сущность экологической составляющей экономической безопасности состоит в стремлении оптимизировать финансовые затраты таким образом, чтобы при минимальном расходовании средств на соблюдение экологических норм уменьшить свои убытки от административных санкций за загрязнение окружающей среды и потери рынков стран с более жесткими нормами экологического законодательства.

Экологическая безопасность на предприятии – это целый комплекс мер, направленных на выявление негативных факторов, которые могут причинить вред здоровью работников. С экологической безопасностью непосредственно связан производственный контроль, предполагающий создание оптимальных условий в целях снижения вредности производства и сокращения ресурсоемкости технологических процессов. Такой контроль позволяет оперативно обеспечить модернизацию комплекса защитных мероприятий, нацеленных на снижение объема вредных выбросов, а также разработку комплекса необходимых действий, предупреждающего возникновение нештатных ситуаций. Кроме того, экологический контроль помогает обеспечивать техническую исправность оборудования, поскольку от этого зависят безопасность работников и соблюдение требований по охране труда.

### ***Информационная составляющая***

В современных условиях перед предприятиями и организациями остро стоит задача сохранения как материальных ценностей, так и информации, в том числе сведений, составляющих коммерческую или государственную тайну.

Успех производственной и предпринимательской деятельности в немалой степени зависит от умения распоряжаться таким ценнейшим ресурсом, как информация, но выгодно использовать можно лишь те сведения, которые востребованы рынком, но неизвестны ему. Поэтому в условиях ужесточения конкуренции успех предпринимательства, гарантия получения прибыли все в большей мере зависят от сохранения в тайне секретов производства, опирающихся на определенный интеллектуальный потенциал и конкретную технологию. Защите подлежит информация, представляющая ценность для бизнеса. При определении ценности предпринимательской информации необходимо руководствоваться такими критериями (свойствами), как полезность, своевременность и достоверность поступивших сведений.

К конфиденциальной информации предприятия относятся планово-аналитические материалы и отчеты за текущий период времени, а также другая информация о деятельности учреждения, разглашение которой

может привести к снижению эффективности функционирования одной из систем, обеспечивающих жизнедеятельность и развитие учреждения.

К строго конфиденциальной информации относятся сведения стратегического характера, разглашение которых может привести к срыву выполнения функций одной или нескольких систем предприятия, прямо влияющих или способных повлиять на его жизнедеятельность и развитие.

Кроме того, к информации ограниченного доступа относят персональные данные, которые должны быть защищены в соответствии с законодательством РФ. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» определяет механизм получения, использования и хранения персональных данных сотрудников.

Хозяиствующие субъекты при найме сотрудников выступают в качестве операторов персональных данных и несут ответственность за их защиту в соответствии с действующим законодательством РФ. В связи с этим в компаниях рекомендуется, с одной стороны, утвердить положение о защите персональных данных работников, а с другой – обязать работников, допущенных к обработке, передаче и хранению персональной информации, не разглашать персональные данные сотрудников.

### ***Силовая составляющая***

Негативные воздействия, затрагивающие силовую составляющую экономической безопасности организации, можно разделить на физические и моральные воздействия личностной направленности; воздействия, направленные на нанесение ущерба имуществу организации, в том числе угрозы снижения стоимости активов организации и потери ею финансовой независимости; воздействия на информационную среду организации, в том числе промышленный шпионаж.

Силовая составляющая экономической безопасности организации включает в себя совокупность направлений:

1. Физическая безопасность сотрудников и руководителей предприятия. К физической безопасности сотрудников относятся как непосредственно сохранность их жизни и здоровья от физических воздействий, направленных на причинение вреда здоровью и жизни, так и злонамеренные поступки третьих лиц или организаций, совершенные с целью нанесения морального ущерба (угрозы жизни и здоровью работников, членов их семей, родственников, нанесение ущерба их репутации и материальному благополучию и т.п.).

2. Сохранность имущества предприятия от негативных воздействий, которые могут привести к его потере или снижению его стоимости. Сюда относятся защита имущества организации от преступных действий заинтересованных лиц или организаций с целью причинения вреда имуществу; обеспечение сохранности принадлежащих предприятию

ценностей от обстоятельств непреодолимой силы, таких как стихийные бедствия, вооруженные конфликты, изменения законодательства.

3. Силловые аспекты защиты информации. В условиях возрастающей роли информации для успеха любого бизнеса возникают проблемы сбора данных и защиты собственной информационной среды от действий внешних организаций и лиц, в том числе от промышленного шпионажа.

4. Защита от возможных угроз, порождаемых внешней средой бизнеса. Субъектами этих действий могут быть организации-конкуренты, криминальные и террористические организации, а также другие источники возможных угроз. Кроме того, превентивные действия по обеспечению благоприятной для предприятия бизнес-среды могут быть направлены на формирование положительного имиджа организации и улучшение взаимоотношений как с государственными и общественными структурами, так и с контрагентами.

В статье [66] функциональные составляющие экономической безопасности связаны с общей стратегией предприятия. Предложенные автором детерминанты экономической безопасности коррелируют со сбалансированной системой показателей стратегического управления предприятием, разработанной Р. Капланом и Д. Нортоном [38].

Перечень функциональных составляющих экономической безопасности предприятия может быть дополнен в зависимости от целей анализа и субъективных предпочтений автора. Однако в целом можно констатировать, что в настоящее время какой-либо общепринятый их набор отсутствует. Каждая из вышеперечисленных составляющих характеризуется собственным содержанием, набором функциональных критериев и способами обеспечения.

Отметим, что в изложенном выше ресурсно-функциональном подходе к определению сущности экономической безопасности предприятия и детерминант оценки ее уровня авторы, как правило, делают акцент на оценке внутренних факторов и угроз. Внутренние факторы связаны с хозяйственной деятельностью предприятия, его персонала, они обусловлены процессами производства и реализации продукции и могут оказать влияние на их результаты.

В табл. 3 представлены различные трактовки содержания экономической безопасности хозяйствующего субъекта и детерминант, определяющих ее состояние.

Представляется, что акцент исключительно на ресурсы и имеющийся потенциал дает одностороннее представление об экономической безопасности хозяйствующего субъекта. Очевидно, что администрация предприятия имеет возможность оказывать воздействие на внутренние дестабилизирующие факторы и потенциальные угрозы за счет использования различных инструментов управления, тогда как управление внешними угрозами и рисками практически невозможно.

Таблица 3

Функциональные составляющие (детерминанты)  
экономической безопасности хозяйствующего субъекта

Авторы	Составляющие экономической безопасности
М.А. Бендиков [20]	Производственная, финансовая, социальная
М.М. Гайфуллина, Е.В. Костомарова [25]	Финансовая, социальная, производственная, инвестиционная, ресурсная, промышленно-экологическая
М.Т. Гильфанов [26]	Финансовая, интеллектуально-кадровая, техничко-технологическая, информационная, ресурсно-производственная, управленческая, сбытовая
О.В. Говорина [27]	Производственная активность, финансовое состояние, социальное развитие, рыночное положение
Л.П. Гончаренко [70]	Финансовая, интеллектуально-кадровая, техничко-технологическая, экологическая, информационная, силовая
В.В. Григорьева, В.В. Шумейко [29]	Финансовая, основные средства, оборотные средства, кадровый потенциал
И.Н. Ермакова, Н.Б. Михеева, Д.С. Хандогина [32]	Финансовая, производственно-сбытовая, техничко-технологическая, кадровая
А.И. Примакин, Л.В. Большакова [54]	Техничко-технологическая, финансовая, ресурсная, интеллектуально-кадровая, информационная, социальная, политико-правовая, экологическая, силовая

Авторы	Составляющие экономической безопасности
Роберт С. Каплан, Дейвид П. Нортон [38], Л.М. Ширко [66]	Финансы, клиенты, внутренние бизнес-процессы, кадры
Н.Н. Яркина, А.Н. Вершинина [71]	Финансовая, технико-технологическая, кадровая и интеллектуальная, конкурентоспособность

### 1.3. Угрозы и риски хозяйственной деятельности

Применительно к экономической безопасности предприятия угрозы и вызовы обусловлены наличием факторов, способных нанести ущерб предприятию или привести к частичной или полной утрате его потенциала. Их обычно разделяют на внешние и внутренние.

К основным субъектам, которые являются потенциальными носителями внешних угроз, относятся:

государство, определяющее экономическую политику, вырабатывающее «правила игры» и формирующее систему организационно-экономических отношений;

контрольно-надзорные органы, осуществляющие проверку и надзор за деятельностью хозяйствующих субъектов;

контрагенты предприятия, поставщики и потребители, определяющие условия договоров и их изменения;

партнеры и конкуренты, применяющие различные методы, в том числе прямое давление, экономический шпионаж и другие меры недобросовестной конкуренции;

специалисты по информационным технологиям, которые могут получить несанкционированный доступ к системе информационных ресурсов;

финансово-кредитные учреждения в случаях отказа предприятию в получении кредита или просрочки им платежей и т.д.

Существующие и вновь возникающие угрозы ограничивают, демотивируют предпринимательскую инициативу и представляют собой серьезные барьеры для внешних инвесторов, оказывают значительное негативное влияние на безопасность ведения бизнеса, ухудшают возможности развития предприятия.

Угрозы экономической безопасности имманентно присущи естественной среде развития производительных сил, следовательно, полностью устранить их невозможно. Хозяйственные процессы

обеспечиваются через взаимодействие органов власти, формирующих условия и приоритеты экономической политики, и предпринимательских структур, непосредственно функционирующих в различных секторах экономики. Вопрос приоритетности личных или коллективных интересов вызывает полемику в экономических исследованиях и до сих пор остается предметом теоретического изучения.

Оценка экономической безопасности предприятия основана на использовании ретроспективного и прогнозного анализа с целью выявления наиболее значимых угроз, установления пороговых границ допустимого риска и прогнозирования его развития. В отличие от государственного уровня, выбор критериев безопасности и их пороговых значений для конкретного предприятия значительно усложняется. Это обусловлено как особенностями управления на микроуровне, так и специфическими особенностями каждого предприятия: его размером, отраслевой принадлежностью, технологичностью производства и т.п.

В нашем понимании экономическая система любого уровня сохраняет свойства целостной саморазвивающейся системы до тех пор, пока ее комплексный потенциал и способность к защите от возникающих угроз превышают совокупное влияние негативных факторов и рисков (рис. 1).



Рис. 1. Обеспечение безопасности экономической системы

Безопасное развитие экономической системы, по нашему мнению, включает в себя следующие базовые условия:

наличие достаточного внутреннего потенциала и стабильного роста уровня дохода для поддержания способности противостоять внутренним и внешним угрозам, ослаблять влияние негативных факторов;

способность к защите от возникающих угроз и дестабилизирующих факторов, обеспечиваемая, кроме всего прочего, наличием конкурентных преимуществ и достаточным уровнем конкурентоспособности;

способность системы к эффективному взаимодействию с внешней институциональной и природной средой, высокую скорость реагирования на изменение внешних условий при условии сохранения окружающей природной среды и обеспечения достойного качества жизни будущих поколений.

Общие угрозы безопасности экономических систем на любом уровне хозяйственной иерархии связаны с ситуацией, в которой существует реальная возможность нанесения ущерба функционированию и развитию экономической системы. Она теряет свою устойчивость и возрастает вероятность ее разрушения. Общие угрозы нарушают целенаправленность развития экономической системы, не позволяют системе в целом и ее отдельным подсистемам противостоять влиянию дестабилизирующих факторов.

К общим угрозам безопасности экономических систем относятся:

1) рыночные: резкие колебания рыночной конъюнктуры и структуры потребления, потеря рынков сбыта, недобросовестная конкуренция, ослабление рыночных позиций; утрата конкурентоспособности и конкурентных преимуществ, усиление монополизации рынка и т.д.;

2) финансовые: ухудшение финансового состояния, утрата платежеспособности, усиление долговой зависимости, снижение финансовой устойчивости и др.;

3) социальные: высокий уровень бедности, снижение качества и доступности образования, медицинской помощи, снижение качества человеческого потенциала, ухудшение социальной обстановки, ослабление трудовой мотивации, рост социальных конфликтов и т.п.;

4) экологические: ухудшение состояния природной среды, нарушение равновесия природных комплексов, дефицит и истощение природных ресурсов, изменение требований экологических стандартов, санитарных норм и правил, рост затрат на их обеспечение и т.д.;

5) технологические: научно-технологические изменения, уязвимость информационной инфраструктуры, слабая инновационная активность, отставание в области разработки и внедрения новых и перспективных технологий; инфраструктурные ограничения, старение материальной технической и технологической базы, снижение производственно-технического потенциала;



б) институциональные: неэффективное государственное управление; высокий уровень коррупции, качество и противоречивость законов, сохранение значительной доли теневой экономики, снижение правовой защищенности, частые изменения нормативно-правовой базы, смена руководства, принципов экономической политики и т.п.;

7) воспроизводственные: недостаточный объем инвестиций в основной капитал и вложений в человеческий капитал, низкое качество подготовки кадров, недостаточный уровень квалификации и ключевых компетенций специалистов;

8) структурные: усиление структурных дисбалансов, относящихся как к уровню и темпам пространственного экономического развития территорий, так и к усилению дифференциации по уровню благосостояния и качества жизни.

Безусловно, любая классификация и систематизация несет на себе отпечаток субъективных оценок. Перечень общих угроз безопасности развития экономических систем может быть расширен, а выбор приоритетных угроз зависит от специфики и аспектов конкретного исследования.

Экономические системы любого уровня отличает возможность собственного целеполагания и управления, наличие механизмов потребления ресурсов и необходимость их воспроизводства, при этом безопасность экономической системы связана со сбалансированностью ее структуры, позволяющей системе реализовывать интересы своего текущего и будущего развития.

Обеспечение экономической безопасности основывается, с одной стороны, на наличии у объекта управления сил, средств, ресурсов и материальных возможностей, гарантирующих защиту от внешних и внутренних угроз, а с другой – на способности субъектов принятия решений к анализу и прогнозированию развития ситуации и превентивной защите собственных экономических интересов.

Эффективность управления экономической системой связывается с рациональной структурой использования всех видов материальных, трудовых и информационных ресурсов для максимального достижения целевых установок системы и характеризуется соотношением между результатами функционирования системы и затраченными ресурсами. При этом оценивается не только результативность хозяйственной деятельности, но и организационно-функциональная структура управления.

Угрозы безопасности могут быть связаны с регрессом экономической системы любого уровня и недостаточным уровнем воспроизводства израсходованных факторов производства, отсутствием достаточного количества ресурсов развития и качественного совершенствования системы. Таким образом, возможность развития экономической системы связана с ее способностью устойчиво

функционировать в режиме расширенного воспроизводства при максимальной независимости от активного или усиливающегося воздействия дестабилизирующих факторов.

В работе С. Баззи и К. Блатмана как ключевой фактор безопасности экономической системы на макроуровне исследуется размер дохода. Авторы доказывают связь между уровнем дохода и стабильностью. Рост доходов уменьшает накал внутренних угроз, оппозиционных движений и снижает личные стимулы к продолжению существующих социальных конфликтов [76, с. 36].

Структурные дисбалансы и диспропорции развития, выходящие за пределы допустимых пороговых значений и препятствующие целенаправленности функционирования системы, повышают уязвимость самой системы и отдельных ее подсистем к действию дестабилизирующих факторов.

Особенность сложных экономических систем составляет наличие специальных механизмов самонастройки и целенаправленного регулирования, одна из функций которых – поддержание оптимальных пропорций между всеми компонентами системы и ее подсистемами. «Сбалансированность экономической системы проявляется в рациональных пропорциях всех ее составляющих, в разумных соотношениях качественного уровня различных подсистем, в оптимальных соотношениях темпов их изменения во времени» [21, с. 147].

Можно привести множество общеизвестных примеров структурных дисбалансов экономической системы. В результате глобализационных процессов усиливается разрыв между уровнем жизни населения и благосостоянием разных стран, что приводит к обострению межгосударственных противоречий, связанных с неравномерностью развития. На протяжении последнего столетия происходит значительное изменение пространственного распределения мирового хозяйства. Структурные диспропорции в экономической системе можно наблюдать, например, в демографической динамике, что проявляется в старении населения промышленно развитых стран и неравномерном росте численности населения развивающихся стран. Пример дисбаланса качественных параметров экономической системы – чрезмерно большая дифференциация населения по уровню доходов и усиление имущественного неравенства и дифференциации качества жизни [40, с. 598].

О.Д. Проценко и М.Н. Дудин выделяют следующие виды диспропорций развития сферы малого и среднего предпринимательства [55, с. 37–39]:

1. Диспропорция эффективности. Выражается в существенных различиях между показателями эффективности деятельности предпринимателей разных видов экономической деятельности.

2. Территориальные диспропорции. Являются следствием неравномерности распределения субъектов малого и среднего предпринимательства и их сосредоточения в крупных городах.

3. Отраслевые диспропорции. Связаны с преобладанием субъектов малого и среднего предпринимательства в сферах быстрого оборота капитала (торговле и сфере услуг) и, как правило, с относительно невысокой долей добавленной стоимости. При этом невысок удельный вес малых и средних компаний, осуществляющих свою деятельность в производственной, инновационной сферах (в том числе ориентированных на экспорт).

4. Структурные диспропорции. Сопряжены с практически полным отсутствием средних предприятий в общем числе зарегистрированных субъектов малого и среднего предпринимательства, что создает высокую угрозу стабильности и устойчивости бизнеса в условиях колебаний рыночной конъюнктуры.

5. Снижение популярности предпринимательства. Выражается в уменьшении количества субъектов малого и среднего бизнеса в последние годы, что связано с более высоким уровнем риска предпринимательской деятельности по сравнению с занятостью на крупных предприятиях с прочной репутацией, а также на предприятиях государственной или муниципальной формы собственности.

А.А. Кузлин и соавторы [41, с. 167] связывают наличие структурных диспропорций и нарушение структуры составляющих социально-экономической системы с состоянием «псевдобезопасности», при котором она может утратить возможность устойчивого развития при отсутствии явно выраженных сигналов о предстоящей угрозе. Сюда же авторы относят несоответствие объемов производства и потребления факторов производства (это относится к соотношению спроса на труд и его предложения на рынке, производству и потреблению энергетических, продовольственных ресурсов и т.д.).

Феномен нестабильности и циклического развития имманентно присущ рыночной экономике, причем характер нестабильности экономической системы необходимо рассматривать на различных уровнях, отличая «деструктивную нестабильность» хозяйственной системы от структурной и технологической ее перестройки.

В контексте обеспечения безопасности экономической системы речь идет о структурных дисбалансах, способных при неблагоприятных условиях достигать столь значительных масштабов, что возникнет угроза безопасности функционирования и развития системы.

Так, слабовыраженные умеренные структурные диспропорции представляют собой «двигатель прогресса», импульс к развитию, в ряде случаев сам его механизм. Диспропорции в экономических системах, превышающие допустимые пороговые значения, являются структурными

дисбалансами, которые становятся факторами регресса, рецессии, перехода экономической системы в кризисное состояние и порождают угрозы безопасности экономической системы. В данном случае под структурными дисбалансами понимается такая степень нарушения пропорций отдельных элементов, при которой возникают риски существенных негативных последствий для развития и функционирования всей системы.

Специфические угрозы безопасности экономической системы проявляются на разных уровнях хозяйственной иерархии и связаны со спецификой внешнего окружения и особенностями внутреннего потенциала экономических систем на макро-, мезо- и микроуровне.

Специфические макроэкономические угрозы проявляются также в нарушении государственной, территориальной целостности и экономического суверенитета, усилении финансовой и технологической зависимости национального хозяйства. Значимой угрозой для экономической системы на макроуровне является зависимость страны от импорта. Так, А.П. Градов и И.В. Ильин предлагают в качестве интегрального показателя оценки уровня безопасности на макроуровне использовать предельную (маржинальную) склонность к импорту, которая определяется отношением прироста стоимости импорта к вызванному им изменению национального дохода [28, с. 91].

Сегодня в мире складывается система экономических отношений, в основе которой лежит экономическая экспансия в виде косвенного контроля, основанного на использовании финансовых механизмов (инвестиций, кредитов и субсидий) в сочетании с методами политического давления [69, с. 8]. Экономическая зависимость и экономические санкции приводят к политическим требованиям и условиям, которые могут рассматриваться как специфические угрозы безопасности экономической системы на макроуровне.

В российских условиях трансформации системы экономических отношений, помимо факторов безопасности бизнеса, диктуемых естественными требованиями конкурентной рыночной среды, обеспечением конкурентоспособности и сохранения рыночных позиций, на микроуровне функционирования экономических систем возникают специфические угрозы, обусловленные низким уровнем защиты прав собственности и контроля над активами, отсутствием эффективной защиты интересов инвесторов и безопасности деловой среды.

Угрозы снижают эффективность и надежность функционирования организаций, а в отдельных случаях приводят к прекращению их деятельности из-за опасности экономического, социального, правового, организационного, информационного, экологического, технического и криминального характера. Кроме того, экономическая безопасность

является базовым условием для разработки и реализации любых планов роста и развития организации.

Внутренние и внешние угрозы экономической безопасности предприятия тесно взаимосвязаны. Например, тенденция к криминализации хозяйственной деятельности ведет к снижению морально-этических норм сотрудников всех рангов, часто толкает их на действия, наносящие урон компании.

Классификация угроз экономической безопасности хозяйствующего субъекта в зависимости от возможности управляющего воздействия представлена на рис. 2.

В качестве угроз экономической безопасности рассматриваются факторы, способствующие ухудшению существующего положения или препятствующие его улучшению. Это может привести к неустойчивости поступательного развития экономики, спаду производства, убыткам, затруднять осуществление инвестиционной деятельности, ухудшать благосостояние и качество жизни людей.

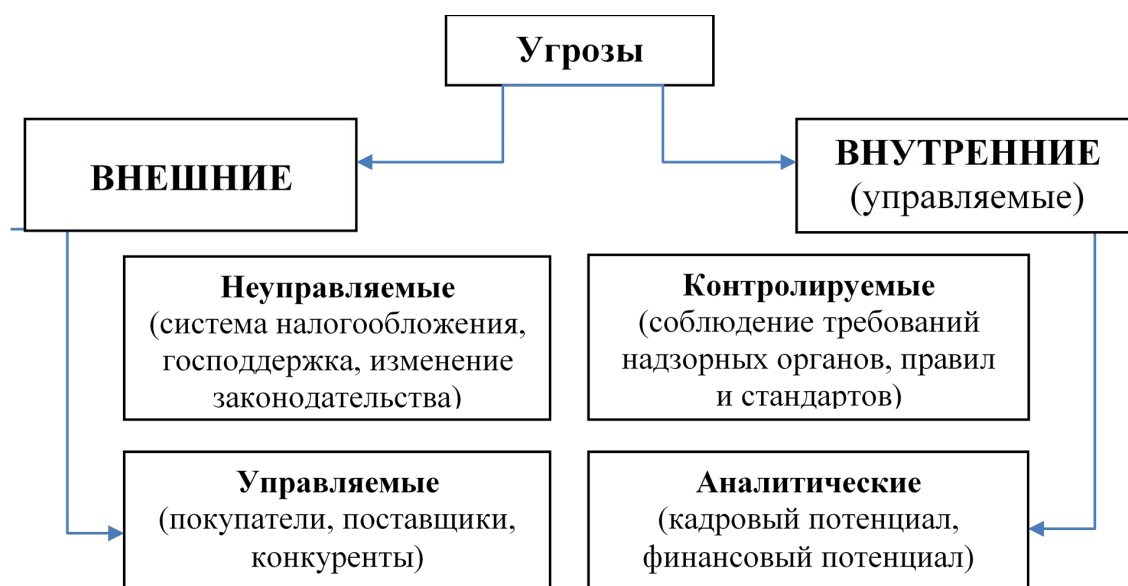


Рис. 2. Внутренние и внешние угрозы экономической безопасности предприятия

По нашему мнению, уровень экономической безопасности предприятия определяется следующими факторами:

1) рыночным положением предприятия и его конкурентными позициями; долей рынка, которую оно занимает, возможностями доступа к отечественным и зарубежным рынкам сбыта;

2) наличием устойчивых связей и контактов во внешней среде, взаимоотношениями с деловыми партнерами, клиентами, покупателями и органами власти; репутацией предприятия, его местом в экономическом и политическом пространстве региона и страны и т.д.;

3) параметрами отраслевого и регионального характера, связанными со стратегической значимостью и государственной поддержкой отрасли и региона либо их положением в экономическом пространстве страны; наличием системы налогового стимулирования и установленным размером обязательных платежей и сборов;

4) социально-демографической обстановкой (социальными и демографическими условиями), уровнем преступности, криминальной обстановкой, уровнем бедности и качества жизни, а также ограничениями, связанными с географическим положением, климатом, инфраструктурой, наличием природного сырья, экологическими условиями и т.д.;

5) наличием имущественных, финансовых и информационных ресурсов, достаточных для достижения поставленных целей, а также резервов стратегически важных материальных и финансовых благ в объемах, обеспечивающих экономическую безопасность в условиях форс-мажора;

6) качеством управления и организации, сложившейся внутри предприятия совокупностью формальных и неформальных норм, правил, регламентов, традиций, определяющих устойчивость и стабильность бесперебойного функционирования предприятия в целом и его подразделений;

7) трудовым коллективом (квалификацией персонала, его опытом, возрастом) и системой мотивации работников (наличием определенного психологического климата внутри коллектива, уровнем доверия, взаимопомощи и деловой коммуникации);

8) финансовым положением и приоритетами инвестиционной деятельности, устойчивостью поступления финансовых потоков, структурой капитала, источниками его финансирования, наличием интересов и мотивов к развитию, уверенности в завтрашнем дне и желания расширить имущественный комплекс, планировать обновление и воспроизводство основного капитала;

9) величиной и структурой транзакционных издержек, связанных с выявлением внешних и внутренних угроз, разработкой и реализацией стратегии развития и обеспечения экономической безопасности.

Таким образом, перечисленные факторы отражают спектр внешних и внутренних угроз экономической безопасности предприятия (рис. 3). Каждая из этих угроз характеризуется определенной степенью опасности для предприятия, что обуславливает приоритеты противодействия угрозам.

Внутренние (эндогенные) угрозы представляют собой возможность кризисных проявлений внутри хозяйственной системы, связанных со сбоями в ее функционировании, неспособностью обеспечить достаточную доходность своей деятельности или адаптироваться к меняющимся условиям. Изменения экономических условий и условий внешней среды не обязательно представляют реальную угрозу дестабилизации

экономической системы и являются неотъемлемым элементом развития рыночной хозяйственной системы. Опасность дестабилизации экономической системы связана не с действием самих этих факторов, а с отсутствием эффективной системы защиты. Например, изменение технологического базиса и резкий переход к цифровым технологиям окажутся опасными факторами для развития экономической системы в том случае, если она не обладает достаточным потенциалом, чтобы воспринять изменения и выработать адекватный механизм реагирования.



Рис. 3. Угрозы экономической безопасности предприятия

Уровень развития бизнеса, наличие достаточного запаса финансовой прочности, внутреннего кадрового, имущественного и финансового потенциала, восприятие предпринимателями рисков определяют устойчивость бизнеса в агрессивных условиях внешней среды. Безопасность бизнеса связывается с возможностями его развития, способностью противостоять возможным внешним и внутренним угрозам.

При этом деловая среда в пространственном аспекте характеризуется множеством специфических параметров, которые определяются особенностями конкретной территории.

Риски современного российского предприятия сопряжены также с возрастанием сложности и стоимости системного мониторинга рыночного и административного окружения в микросреде бизнеса, что требует от предприятия существенного изменения маркетинговой и менеджерской деятельности, расширения круга знаний о структуре его социально-экономического и административно-политического окружения.

Основные задачи разработки мер защиты бизнеса заключаются в предотвращении вероятных угроз внешней среды и реализации потенциальных возможностей компании, выстраивании долгосрочной и устойчивой системы отношений в рамках взаимодействия с другими субъектами деловой среды.

#### **1.4. Оценка внешней среды и условий ведения бизнеса**

Любая социально-экономическая система функционирует в определенной среде, которая может оказывать как благоприятное, так и дестабилизирующее воздействие на ее деятельность. Одной из тенденций развития экономических систем на современном этапе является резкое повышение динамичности деловой среды, увеличение скорости научно-технического, экономического, политического, социального прогресса. В результате сокращаются не только жизненные циклы товаров и услуг, но и сроки на их разработку.

Изменчивость внешней среды не дает предприятию развиваться с использованием шаблонных форм управления. Нестабильная внешняя среда определяет колебательные процессы хозяйственной деятельности, что обуславливает необходимость постоянной адаптации предприятия к новым условиям на основе тщательного анализа рисков и угроз.

От способности администрации предприятия своевременно реагировать на изменения среды зависят качество менеджмента, скорость и адекватность реакции на изменения. Эта способность имеет важнейшее значение для обеспечения безопасного функционирования организации. Внешние опасности и угрозы возникают за пределами предприятия и не связаны с его производственной деятельностью. Как правило, это такое изменение окружающей внешней среды, которое может нанести предприятию ущерб. Внешние угрозы для бизнеса обусловлены, как правило, объективными факторами – негативными воздействиями, которые появляются независимо от самих компаний и предпринимателей.



В.Л. Тамбовцев утверждает, что конкурентоспособность и потенциал развития экономики страны, обуславливающие условия для ведения бизнеса, определяются следующими факторами [62, с. 36–40]:

- диверсификацией отраслевой структуры экономики;
- инновационностью;
- уровнем развития предпринимательства;
- оптимальным соотношением крупных, средних и малых фирм;
- сложностью производимой и экспортируемой продукции.

При оценке пространственных экономических систем, определяющих условия ведения бизнеса или характеризующих деловую среду на определенной территории, активно используются различные рейтинги.

Согласно определению, приведенному в описании методологии одного из первых рейтингов глобальной конкурентоспособности (IMD World Competitiveness Ranking)<sup>1</sup>, конкурентоспособность деловой среды на национальном или субнациональном уровне понимается как «способность экономики страны создавать и поддерживать среду, в которой возникает конкурентоспособный бизнес». Подразумевается, что создание материальных ценностей происходит главным образом на уровне частных или государственных предприятий, однако предприятия существуют в деловой среде, которая повышает либо снижает их способность конкурировать внутри страны или за рубежом.

Центр мировой конкурентоспособности (IMD World Competitiveness Center) оценивает не только конкурентоспособность деловой среды (IMD World Competitiveness Ranking), но и цифровую конкурентоспособность страны (IMD World Digital Competitiveness Ranking)<sup>2</sup>.

По мнению В.Н. Украинского, использование рейтингов позволяет упростить процедуру оценки и создает возможности для как можно более частого обновления индексов, однако плохо согласуется с «полнотой и глубиной измерений для поиска истины», принятых в научном сообществе. В данном случае, по мнению автора, в большей степени решается «задача регулярного выпуска интеллектуального продукта, предназначенного для широкого распространения в ненаучных кругах», но результаты, полученные в итоге ряда упрощений, являются несопоставимыми во времени и пространстве [65, с. 122–123].

Представляется, что указанные выводы имеют под собой определенные основания, что подтверждается диаметрально противоположными оценками одних и тех же условий деловой среды на одной и той же территории, полученными в результате проведения разных

---

<sup>1</sup> Мировой рейтинг конкурентоспособности. URL: <https://www.imd.org/centers/world-competitiveness-center/rankings/world-competitiveness/> (дата обращения: 17.01.2023).

<sup>2</sup> Мировой рейтинг цифровой конкурентоспособности. URL: <https://www.content.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/> (дата обращения: 17.01.2023).

рейтингов. Однако активное использование рейтингов и их популярность оказывают существенное влияние на формирование общественного мнения и привлекательность деловой среды для инвесторов. Кроме того, создатели широко применяемых сегодня рейтингов и индексов в зависимости от выбранного аспекта исследования анализируют и выделяют наиболее значимые факторы, определяющие качество деловой среды и условия для функционирования и развития бизнеса. В связи с этим при исследовании методологии оценки качества деловой среды нельзя игнорировать использование рейтингов и индексов.

О.Д. Проценко и И.О. Проценко для оценки конкурентоспособности бизнеса на макроуровне предлагают использовать несколько основных параметров [55, с. 38]:

- повышение производительности,
- ценовую конкурентоспособность,
- инновационную деятельность,
- инвестиционную привлекательность.

Одним из первых наиболее известных исследований в глобальном масштабе в данной сфере является рейтинг конкурентоспособности страны, выполненный экспертами Международного института развития менеджмента (International Institute for Management Development (IMD)).

Рейтинг конкурентоспособности деловой среды (IMD World Competitiveness Ranking) оценивает четыре группы факторов:

- эффективность экономики,
- эффективность государства,
- эффективность бизнеса,
- инфраструктуру.

Критериями могут быть данные статистики, которые оценивают конкурентоспособность деловой среды по мере ее измерения, или субъективные данные, представляющие собой результаты опросов руководителей крупных корпораций и специалистов в области управления, которые анализируют восприятие качества деловой среды предпринимателями.

При определении комплексного показателя используется соотношение объективных и субъективных оценок с преобладанием объективных показателей: две трети приходится на статистические данные и одна треть – на экспертные оценки.

Агрегирование результатов оценки факторов приводит к общей консолидации, выраженной в общем рейтинге конкурентоспособности деловой среды IMD World. Данный рейтинг позволяет определить положение страны в сравнении с эталонной экономикой (государством, занявшим первое место), но не отражает динамику ее изменений. Это означает, что потеря позиций в рейтинге не всегда говорит о том, что качество деловой среды ухудшилось.

Рейтинг цифровой конкурентоспособности (IMD World Digital Competitiveness Ranking) оценивает способность и готовность экономики к внедрению и изучению цифровых технологий в качестве ключевого фактора экономических преобразований в бизнесе и обществе в целом. Согласно методологии рейтинга WDC определяет цифровую конкурентоспособность, оценивая следующие основные факторы:

1) знания (поддержка талантов, обучение и образование; научная концентрация);

2) технологии (нормативно-правовая база, капитал, технологическая база);

3) готовность к будущему (адаптивное отношение, бизнес-гибкость, ИТ-интеграция).

Основанные на сочетании объективных данных и ответов на вопросы руководителей предприятий и государственных органов, цифровые рейтинги помогают правительствам и компаниям определить, на чем сосредоточить свои ресурсы и какие методы целесообразно использовать в процессе цифровой трансформации.

Для оценки условий ведения бизнеса на уровне регионов Российской Федерации используют «Итоговый рейтинг регионов РФ»<sup>3</sup>, «Социально-экономическое положение регионов России»<sup>4</sup> (составитель – «РИА Рейтинг»), «Рейтинг регионов SMART версии»<sup>5</sup> (Ассоциация инновационных регионов России), «Рейтинг инновационного развития субъектов РФ»<sup>6</sup> (НИУ ВШЭ). Кроме того, качество деловой среды оценивается на основе опросов представителей бизнеса. Опросы проводятся как официальными органами статистики, так и рейтинговыми агентствами. Среди подобных исследований можно назвать, например, ежеквартальный «Индекс малого и среднего бизнеса RSBI»<sup>7</sup>, который составляется Общероссийской общественной организацией малого и среднего предпринимательства «Опора России» на основе опросов российских предпринимателей и представляет собой отражение «бизнес-настроений» по вопросам развития малых и средних предприятий. На основе рейтинга рассчитывается индикатор, оценивающий деловую активность малого и среднего бизнеса RSBI (Russian Small Business Index). Замер проводится по девяти компонентам: бизнес-ожидания, продажи, прибыль, цены

<sup>3</sup> Итоговый рейтинг регионов РФ-2022. URL: <https://riarating.ru/regions/20221226/630235161.html> (дата обращения: 17.01.2023).

<sup>4</sup> Рейтинг социально-экономического положения регионов по итогам 2021 г. URL: <https://riarating.ru/infografika/20220516/630222174.html> (дата обращения: 17.01.2023).

<sup>5</sup> Рейтинг регионов SMART версии 2022 г. URL: <https://i-regions.org/reiting/rejting-regionov-smart/> (дата обращения: 17.01.2023).

<sup>6</sup> Рейтинг инновационного развития субъектов Российской Федерации. URL: <https://www.hse.ru/primarydata/rir2021> (дата обращения: 17.01.2023).

<sup>7</sup> Индекс Опоры RSBI. URL: <http://opora.ru/projects/indeks-opory-rsbi/> (дата обращения: 17.01.2023).

реализации, себестоимость, кадры, количество клиентов, доступность финансирования, баланс запасов.

Условия ведения бизнеса и качество деловой среды с точки зрения их привлекательности для инвестора чаще всего оцениваются с помощью рейтингов «Национальный рейтинг состояния инвестиционного климата» (Агентство стратегических инициатив, АСИ)<sup>8</sup>, «Инвестиционная привлекательность регионов»<sup>9</sup> (рейтинговое агентство «Эксперт РА»).

Национальный рейтинг состояния инвестиционного климата в субъектах РФ (АСИ) рассчитывается по 67 показателям в следующих направлениях:

- 1) регуляторная среда;
- 2) институты для бизнеса;
- 3) инфраструктура и ресурсы;
- 4) поддержка малого предпринимательства.

Получение информации по показателям осуществляется путем проведения опросов предпринимателей и экспертов, а также с использованием статистических данных.

Известны три различных подхода к формированию выборок для опросов, в соответствии с которыми выделяют показатели, оцениваемые экспертным путем, на основе опроса предпринимателей из общей генеральной совокупности и предпринимателей из специальных генеральных совокупностей.

Во время проведения рейтинга собираются исходные данные, необходимые для расчета результатов, статистические данные в натуральных величинах, оценки экспертов.

Рейтинг инвестиционной привлекательности регионов России, составляемый агентством «Эксперт РА», рассчитывается на основе показателей, сгруппированных в пять блоков: инфраструктурные, экономические, социальные, финансовые ресурсы, состояние окружающей среды. Наибольший вес имеют инфраструктурные и социальные ресурсы, так как для инвесторов большую роль играет сочетание развитой инфраструктуры и производительной и квалифицированной рабочей силы. Расчет каждого интегрального показателя производится путем сравнительного анализа. Для расчетов применялись последние годовые статистические данные Федеральной службы государственной статистики, Центрального банка Российской Федерации, Федерального казначейства, Минфина России, МВД России, ЕМИСС.

Н.З. Солодилова, К.Е. Гришин, Р.И. Маликов для исследования условий деловой среды на уровне регионов Российской Федерации

---

<sup>8</sup> Национальный инвестиционный рейтинг. URL: [https://asi.ru/government\\_officials/rating/](https://asi.ru/government_officials/rating/) (дата обращения: 17.01.2023).

<sup>9</sup> Инвестиционная привлекательность регионов. URL: [https://www.raexpert.ru/researches/regions/regions\\_invest\\_2022/](https://www.raexpert.ru/researches/regions/regions_invest_2022/) (дата обращения: 17.01.2023).

используют экосистемный подход, поскольку, по их мнению, он позволяет «фокусироваться на конкретном пространственно-временном контексте развития предпринимательства, в рамках которого учитывается характер взаимодействий экономических агентов и их взаимоотношений со средой функционирования» [61, с. 134].

Авторы предлагают трактовать региональную экосистему предпринимательства как «совокупность взаимосвязанных субъектов предпринимательства (как потенциальных, так и существующих), среды их функционирования и взаимодействий между ними (системы обмена), определяющих интенсивность генерации, развития и затухания предпринимательских процессов в локальной пространственной среде» [61, с. 139–140].

В данном контексте успех субъекта предпринимательства зависит от того, насколько его внутренняя конфигурация входит в резонанс с конфигурацией региональной экосистемы бизнеса. Успешное развитие предпринимательства связывается с ситуацией, при которой внутренние конфигурации субъектов предпринимательства (предпринимательские способности, потенциал, ресурсы) соответствуют конфигурации внешнего окружения (доступ к финансовым ресурсам, инфраструктура, институциональная среда). Конфигурация внешнего окружения (внешняя конфигурация экосистемы) задает формат взаимодействий и интенсивность развития и затухания деловой активности в локальной пространственной среде.

Институциональную конфигурацию региональной деловой среды исследователи оценивают на основе действенности формальных институтов, которая «определяется характером их интерпретации и применения экономическими агентами в ходе взаимодействия» [61, с. 134].

Упомянутым авторским коллективом предложено следующее определение: «Институциональная конфигурация региональной деловой среды представляет собой набор опосредующих деловые отношения взаимосвязанных и взаимодействующих базовых и дополнительных региональных формальных и неформальных институтов, упорядоченных и структурированных в определенной иерархической комбинации» [61, с. 138]. При этом институты деловой среды рассматриваются авторами с позиции взаимодействия между экономическими агентами, определяющего условия ведения бизнеса, а также размер и структуру вознаграждения субъекта предпринимательства. Конфигурация институтов определяет совокупность политических, социальных, юридических правил и неформальных норм, опосредующих деловые отношения в регионе, и исследуется с учетом характера их интерпретации и применения экономическими агентами в деловой практике.

В.А. Барина и ее соавторы для выявления значимых институциональных факторов предпринимательского климата используют в качестве результативного показателя предпринимательской активности в регионах России отношение числа малых предприятий в регионе к численности экономически активного населения, рассматривая данный критерий как «прокси-переменную уровня предпринимательского капитала» [18, с. 95]. По оценкам авторов, уровень активности предпринимателей выше в регионах с крупнейшими агломерациями, выгодным географическим положением, большим потребительским рынком, высокой диверсификацией экономики и относительно благоприятными институциональными условиями. В связи с этим деловую среду предложено оценивать с помощью четырех базовых факторов, определяющих предпринимательскую активность (доступность человеческого капитала, уровень экономического развития, агломерационные эффекты и структура экономики), а также учитывать шесть институциональных факторов (уровень инвестиционного риска, качество правовой среды, доступность финансирования, уровень административной нагрузки, качество человеческого капитала, качество государственной поддержки малого и среднего предпринимательства) [18, с. 105]. По результатам оценки установлена высокая значимость институциональных факторов для роста предпринимательской активности.

Хозяйственная деятельность всех участников рынка находится под воздействием институциональных факторов, формирующих институциональную среду, и представляет собой совокупность институциональных условий предпринимательской деятельности, определяющих специфику и содержание динамических хозяйственных процессов, которые формируют предпринимательский климат.

Факторы, оказывающие воздействие на ведение хозяйственной деятельности, могут стать потенциальным источником угроз для функционирования и развития бизнеса. Представляется, что предложенный в статье [15] методологический подход, основанный на использовании ABC-матрицы, можно использовать для выявления рисков и угроз внешней среды и выработки управляющих воздействий, направленных на укрепление ресурсного потенциала предприятия (рис. 4).

В этой связи целесообразно сгруппировать условия институциональной среды, выделив административно-правовые (А), экономические и финансовые (Е), социально-экологические (S), материально-технические и инфраструктурные (Т) факторы.



Рис. 4. Модель конфигурации деловой среды как экосистемы (составлена авторами на основе статьи [61])

М.Т. Гильфанов в статье [26] по аналогии с принятым в маркетинге подходом к анализу внешней среды выделяет два уровня внешней среды бизнеса: микро- и макросреду. Подобное разделение определяется характером воздействия внешней среды на бизнес-процессы: бизнес не в состоянии оказывать непосредственное воздействие на факторы макросреды и может только приспособиться к их влиянию; воздействие микросреды определяется участниками хозяйственной деятельности, с которыми фирма находится в непосредственном взаимодействии. Внешняя макросреда оказывает косвенное воздействие на бизнес и микросреду, объединяющую агентов и субъектов рынка, прямо взаимодействующих между собой и оказывающих влияние друг на друга.

По мнению М.Т. Гильфанова, воздействие микросреды на экономическую безопасность бизнеса определяется отраслевыми и региональными факторами. В качестве факторов, выступающих либо угрозой, либо возможностью для развития, автор берет характеристики конкретного вида экономической деятельности. В территориальном аспекте детерминанты экономической безопасности представлены в табл. 4.

Таблица 4

**Параметры оценки микросреды  
в системе экономической безопасности предприятия  
(составлено авторами на основе статьи [26])**

Ключевые детерминанты	Характеристика ключевых детерминант	Факторы
Вид экономической деятельности	Характеристика контрагентов; специфика и особенности развития вида экономической деятельности	Надежность партнеров; надежность инвесторов; объем и перспективность развития рынка; характер конкуренции на рынке; сезонные колебания; инновационное развитие конкурентов; привлекательность бизнеса
Характеристики территории	Ресурсный потенциал региона; уровень развития инфраструктуры территории; инвестиционный климат региона	Уровень жизни населения в регионе; инвестиционная привлекательность территории; границы рынка сбыта; наличие местных ресурсов; транспортно-логистическая инфраструктура

В зависимости от характера воздействия каждый из факторов внешней среды может рассматриваться как угроза для бизнеса либо возможность его развития. При этом степень влияния факторов на бизнес-процессы может варьироваться в широком диапазоне.

Для оценки макросреды используется экспертная оценка по аналогии с PEST-анализом [15, 25, 26]. В статьях [25] и [26] макросреда оценивается по шести составляющим (к четырем компонентам классического PEST-анализа добавлены еще экологическая и институциональная). В табл. 5 представлены детерминанты макросреды бизнеса.

Таблица 5

**Параметры оценки макросреды  
в системе экономической безопасности предприятия  
(составлено авторами на основе статей [25] и [26])**

Ключевые детерминанты	Характеристика ключевых детерминантов	Факторы
Политические	Характер воздействия конкретных изменений в политической сфере	Объемы поставок зарубежным потребителям; ресурсы, получаемые из-за рубежа



Окончание табл. 5

Ключевые детерминанты	Характеристика ключевых детерминантов	Факторы
Экономические	Характеристика макроэкономической ситуации; воздействие изменения макроэкономических процессов	Инфляция; безработица; фаза экономического роста; валютный курс
Социальные	Характер воздействия на экономическую деятельность изменений социального характера	Уровень жизни населения; объемы потребления; потребительские предпочтения
Технологические	Технологический уровень; темпы научно-технического прогресса; уровень цифровизации	Появление инновационных технологий; соответствие этапу технологического развития страны
Институциональные	Характер влияния на предприятие конкретных изменений в законодательстве; взаимодействие с контрольно-надзорными органами	Изменения в налоговом законодательстве; изменение ставки рефинансирования; изменения в политике государственной поддержки бизнеса
Природно-экологические	Характер влияния изменения природных условий; экологическая обстановка	Изменение климатических условий; изменение параметров экологического контроля

Развитие любого бизнеса неразрывно связано с безопасностью его функционирования, ростом капитала, благоприятной рыночной конъюнктурой и эффективностью использования имеющихся внутренних и внешних факторов. Внешняя среда может оказывать как благоприятное, так и дестабилизирующее воздействие на деятельность хозяйствующих субъектов. Она определяет условия для функционирования предприятий, обуславливает возможности для роста бизнеса и является источником угроз для безопасности предпринимательской деятельности.

Институциональные ограничения и угрозы деловой среды представляют собой серьезные барьеры для внешних инвесторов, оказывают существенное влияние на безопасность ведения бизнеса, сокращают возможности развития и снижают предпринимательскую активность. Повышение деловой активности хозяйствующих субъектов считается фактором выхода на траекторию устойчивого развития и обеспечения экономической безопасности государства в целом, при этом активизация бизнеса напрямую связана с качеством деловой среды и существующими формальными и неформальными барьерами для функционирования и развития бизнеса.

В табл. 6 приведены институциональные ограничения предпринимательской деятельности.

Таблица 6

Система ограничений предпринимательской деятельности

Группа факторов	Ограничения	Формальные	Неформальные
Административно-правовые (А)	Административные	Бюджетные ограничения и принятые органами власти административные акты	Взаимоотношения власти и бизнеса, административные барьеры
	Правовая система	Конституция РФ, законодательные, нормативные и правовые акты	Действенность механизмов исполнения законодательных актов, криминализация общественных отношений и нарушение прав собственности
	Обеспечение правосудия	Судебная система	Уровень доверия бизнеса правовым институтам и судебной системе
Экономические и финансовые (Е)	Рыночные	Система антимонопольного законодательства	Конкурентные механизмы
	Контрактная система	Установленные правила контрактных отношений и государственных закупок	Сложившиеся неформальные механизмы распределения государственных заказов
	Финансовые	Механизмы регулирования финансового рынка и получения кредитов	Теневые финансовые отношения
	Фискальная нагрузка	Налоговая система и правила налогообложения	Налоговая культура, отношение предпринимателей к уклонению от налогов и сокрытию доходов
Социально-экологические (S)	Социально-политические	Демократическое устройство общества, выборная система	Интересы влиятельных политических группировок
	Социально-культурные	Образовательная система и политика в области образования и воспитания	Этические бизнес-нормы, поведенческие стереотипы и менталитет
	Экологические	Требования экологического законодательства	Стремление бизнеса снизить затраты на соблюдение экологических требований
Технические и инфраструктурные (Т)	Доступ к объектам инфраструктуры	Технические условия, регламентирующие правила подключения к энерго-, водоснабжению и водоотведению/канализации; отсутствие технологической возможности предоставления доступа к объекту инфраструктуры	Нарушение прозрачности информации об условиях и порядке доступа к инфраструктуре, формировании тарифов за предоставление доступа, экономически необоснованная цена доступа

Угрозы для развития экономики Российской Федерации и повышения экономической активности хозяйствующих субъектов в долгосрочной перспективе, с учетом геополитической обстановки, усиливающегося санкционного давления на Российскую Федерацию и высокого уровня неопределенности, связаны с низким качеством деловой среды, в которой высокий уровень предпринимательских и инвестиционных рисков сочетается с демографическими вызовами и усилением рисков ухудшения качества человеческого капитала, состояния окружающей среды, а также здоровья населения. Все это отрицательно сказывается на устойчивости воспроизводства ресурсов, материального и человеческого капитала, темпах роста ВВП и модернизации экономики, что в конечном счете отражается не только на конкурентных позициях страны в мировой экономике и ее национальной безопасности, но и на безопасности развития экономических систем на микроуровне.

Изменчивость российской деловой среды и присущие ей специфические опасности и риски не позволяют предприятиям развиваться с применением шаблонных форм управления. Нестабильная деловая среда определяет колебательные процессы хозяйственной деятельности, что обуславливает необходимость постоянной адаптации предприятия к новым условиям на основе тщательного анализа рисков и угроз.

От способности администрации предприятия своевременно реагировать на угрозы и трансформации деловой среды зависят качество менеджмента, скорость и адекватность реакции на изменения; эта способность имеет важнейшее значение для обеспечения безопасного функционирования и развития.

Цифровизация сегодня происходит в общемировом масштабе, что позволяет говорить о цифровой трансформации всех отраслей экономики, жизни социума в целом и о формировании нового хозяйственного уклада – цифровой экономики. Цифровые технологии меняют саму операционную систему функционирования бизнеса, повышают эффективность хозяйственной деятельности и выявляют новые возможности на рынке. Набирающий темп процесс преобразования стал необратимым даже в наиболее традиционных отраслях экономики.

## **РАЗДЕЛ 2. ВЕДЕНИЕ БИЗНЕСА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

### **2.1. Особенности цифровой трансформации экономики**

Использование цифровых технологий за последние два десятилетия привело к кардинальной трансформации общества. Изменилось то, как мы живем, работаем, проводим досуг и общаемся. В настоящее время именно цифровые технологии могут вызвать широкомасштабные социальные изменения и в значительной степени способствовать экономическому прогрессу. Соответственно, в сложившейся ситуации важнейшим условием выживания национальной экономики является внедрение экономических конструкций, основанных на цифровых технологиях.

Пандемия ускорила цифровизацию и вызвала резкий скачок в сфере цифровых технологий и бесконтактных отраслей. Быстрота и радикальность распространения цифровых технологий в ближайшем будущем приведут к новым глубоким изменениям условий деловой среды. Следовательно, цифровизацию можно рассматривать не только как фактор повышения производительности и экономического роста, но и как источник институциональной модернизации деловой среды, то есть как технологическую предпосылку трансформации организационных соглашений и способов взаимодействия экономических агентов. В этих условиях необходим системный пересмотр правовых норм, регулирующих механизмов, условий конкуренции на рынках с учетом особенностей происходящей цифровой трансформации.

Цифровизация коренным образом меняет экономику страны и общество в целом: стимулирует предпринимательскую инновационную деятельность, повышает производительность труда и способствует экономическому росту в регионах.

Поступательное развитие регионов как открытых многоуровневых систем в условиях обострения противоречий между интересами экономических агентов на этапах ухудшения макроэкономических условий и усиление конкуренции на глобальном и национальном уровнях определяют необходимость формирования эффективной системы экономической безопасности на мезоуровне с учетом многочисленных угроз и рискообразующих факторов [13]. С одной стороны, цифровая трансформация предприятия обеспечивает ему конкурентные преимущества на рынке, с другой – это вызов, угрожающий самому существованию предприятия.

Высокий интерес к данному феномену со стороны политиков, бизнесменов, журналистов обуславливает появление в средствах массовой информации и научных трудах большого количества синонимов термина

«цифровизация», наиболее популярными из которых являются «цифровая экономика» и «цифровая трансформация». Однако, как отмечают В.В. Камнева и Е.А. Гнатышина, эти термины по своей сути имеют разную природу. Представители европейского научного сообщества, как и российские экономисты, в большей степени используют понятие «цифровая экономика» [37].

Цифровая экономика представляет собой совокупность видов экономической деятельности, коммерческих сделок и профессиональное взаимодействие посредством информационно-коммуникационных технологий. В узком смысле ее можно трактовать как экономику, основанную на цифровых технологиях.

Цифровые технологии обладают значительным прорывным потенциалом, делают производство более гибким, а информацию – более доступной.

Определение того или иного понятия является отражением времени и соответствующих ему трендов, особенно в сфере технологий. Например, в ранних трактовках термина исследователи делали акцент на интернет-технологиях.

Одним из первых термин «цифровая экономика» употребил Дон Тапскотт в своем бестселлере 1995 года «Электронно-цифровое общество: плюсы и минусы эпохи сетевого интеллекта» [63]. Он заявлял, что цифровая экономика охватывает два типа экономической активности:

информационный, подразумевающий выполнение базовых задач, таких как загрузка статичной информации на сетевые ресурсы;

связанный с коммуникациями, включающий виды деятельности, ставшие доступными благодаря интернету.

Николас Негропonte, основатель медиалаборатории Массачусетского технологического института и автор книги "Being Digital", идентифицировал цифровую экономику как использование «битов вместо атомов» [116]. Среди неоспоримых преимуществ цифровизации перед традиционным рынком исследователь отмечал:

отсутствие физического веса товара, который можно заменить информационным объемом;

значительно меньшие затраты на производство электронных товаров и меньшую площадь, занимаемую электронными носителями;

виртуальный характер экономических отношений, приводящий к снижению потребности в сырье;

появление цифровых валют, что сегодня наглядно подтверждает растущий рынок криптовалют;

мгновенное глобальное перемещение товаров и услуг через интернет.

Первоначально наряду с термином «цифровая экономика» использовались понятия «интернет-экономика», «новая экономика» и «веб-экономика», подчеркивающие ее тесную связь с глобальной сетью.

Кроме того, в начале цифровой эры для обозначения сочетания сектора информационно-коммуникационных технологий (ИКТ), цифровых медиа и электронной коммерции широко применялся термин «экономика знаний».

Тем не менее по мере накопления знаний специалисты пришли к выводу, что данное понятие намного сложнее и глубже, чем простая экономическая выгода, полученная с помощью интернета.

Авторы более поздних определений обращают внимание на развитие мобильных и беспроводных сетей, а также облачных технологий и технологий работы с большими данными. Кроме того, они столкнулись с проблемой, возникающей из-за обилия типов экономической активности, которые задействуют цифровые технологии.

Анализ источников позволил выделить ряд подходов к интерпретации данного термина (табл. 7).

Таблица 7

Подходы к определению понятия «цифровая экономика»  
(составлено на основе статьи [22])

Подход	Описание	Представители
Ресурсоориентированный	Опирается на технологии, составляющие основу цифровой экономики: информационные ресурсы, человеческие ресурсы	Э. Бринольфссон, Б. Кахин, Д. Тапскотт
Процессуальный / поточный	Представители подхода относят к цифровой экономике использование технологий для осуществления отдельных хозяйственных операций. При этом новые потоки информации и данных, создаваемые при помощи ИКТ, как элемент цифровой экономики рассматриваются не во всех работах. Следуя логике данного подхода, к цифровой экономике нужно также отнести трансформации в технологических процессах	Р. Клинг, Р. Лэмб, Н. Лейн, М. Бахл
Структурный	Цифровая экономика трактуется в широком смысле как трансформация экономики в целом, а в узком – как трансформация отдельных ее составляющих	Э. Бринольфссон, Б. Кахин
Бизнес-ориентированный (бизнес-модели)	Среднее между процессуальным и структурным подходами	Т.Л. Мезенбург

Цифровая революция, происходящая на протяжении последних двух десятилетий, привела к тому, что цифровые бизнес-модели получили

широкое распространение. Согласно определению Организации экономического сотрудничества и развития (ОЭСР), цифровая экономика включает в себя все виды экономической деятельности, которые зависят от использования цифровых ресурсов, включая цифровые технологии, цифровую инфраструктуру, цифровые услуги и данные, или способны благодаря им повышать свою эффективность [72].

Трактовки понятия «цифровая экономика», используемые в работах ряда зарубежных и отечественных авторов, приведены в прил. А.

Таким образом, выделяют как минимум два подхода к определению понятия «цифровая экономика»:

1) узкий подход, согласно которому цифровая экономика – это экономика, основанная на цифровых технологиях производства товаров, выполнения работ и оказания услуг;

2) расширенный подход, в соответствии с которым под цифровой экономикой понимают производство товаров и услуг с преимущественным использованием цифровых технологий, а цифровые данные рассматривают как ключевой фактор.

Цифровая экономика ознаменовала собой переход от третьей промышленной революции к четвертой. Третья промышленная революция (автором ее концепции является Дж. Рифкин), именуемая также цифровой революцией, была обусловлена изменениями, произошедшими в конце XX века в связи с переходом от аналоговых электронных и механических устройств к цифровым технологиям. Четвертая промышленная революция (Индустрия 4.0) основывается на цифровой революции, поскольку современные технологии продолжают соединять физический и кибермир [56].

Основным трендом эффективного развития цифровой экономики выступает цифровизация. Именно она служит основой цифровой экономики и обуславливает перестройку традиционных форматов представления информации на цифровые в целях обеспечения роста эффективности бизнес-процессов и улучшения качества жизни посредством увеличения скорости взаимообмена, доступности и защищенности информации, возрастания роли автоматизации.

Цифровизация определяет создание в экономическом пространстве цифровых платформ, которые позволяют решать вопросы стратегического характера в сферах образования и науки, медицины, транспорта, государственного управления, промышленности, то есть происходит трансформация природы экономико-производственных отношений.

В исследовании Европейского фонда улучшения условий жизни и труда (Eurofound), опубликованном в мае 2018 года, отмечено следующее [89]:

применительно к социальным системам или организациям цифровизация в широком смысле относится к трансформации, вызванной широким внедрением цифровых технологий (робототехники, машинного обучения, датчиков, виртуальной реальности и т.д.);

применительно к конкретным фрагментам информации оцифровка относится к процессу их преобразования в цифровую форму, которая может быть обработана компьютером (или наоборот). Оцифровка также включает в себя действия, выполняемые с помощью таких технологий, как датчики, 3D-печать или дополненная реальность и виртуальная реальность.

Цифровая трансформация означает внедрение цифровых технологий для преобразования бизнес-процессов. Это достигается заменой ручных (нецифровых) процессов цифровыми или устаревших цифровых технологий модернизированными цифровыми технологиями.

В соответствии с Приказом Минкомсвязи России от 1 августа 2018 года № 428 «Об утверждении разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы “Цифровая экономика Российской Федерации”» цифровизация (цифровое развитие) определяется как «процесс организации выполнения в цифровой среде функций и деятельности (бизнес-процессов), ранее выполнявшихся людьми и организациями без использования цифровых продуктов. Цифровизация предполагает внедрение в каждый отдельный аспект деятельности информационных технологий» [13].

Цифровая экономика давно уже вышла за рамки исключительно цифровизации и автоматизации производственного процесса. Новая парадигма включает в себя множество передовых технологий и современных технологических платформ: сквозные технологии и гиперсвязность, интернет вещей (IoT), большие данные (big data), расширенную аналитику, беспроводные сети, мобильные устройства и социальные сети.

Р. Клинга и Р. Лэмб выделяют следующие компоненты цифровой экономики (рис. 5).





Рис. 5. Составляющие цифровой экономики [108]

Как отметил в 2015 году Т. Гудвин – старший вице-президент по стратегии и инновациям в Navas Media: «Uber, крупнейшая в мире компания такси, не владеет автомобилями. Facebook, самый популярный в мире владелец СМИ, не создает никакого контента. Alibaba, самый дорогой ритейлер, не имеет запасов. А Airbnb, крупнейший в мире поставщик жилья, не владеет недвижимостью... Происходит что-то интересное» [92].

Все многообразие компаний, чья деятельность связана с электронным бизнесом, основано на разработке и поставке смарт-устройств на рынок, экономике совместного потребления (Sharing Economy) и использовании социальных платформ [87].

По мнению американского экономиста Т. Мезенбурга, отличительными чертами цифровой экономики являются [114]:

1) инфраструктура – предприятия должны быть обеспечены необходимым программным обеспечением, оборудованием, а также квалифицированными специалистами;

2) электронный бизнес – компьютерные приложения, онлайн-инструменты и цифровые платформы, используемые при осуществлении бизнес-процессов;

3) электронная коммерция – реализация товаров и услуг в интернете.

Согласно исследованиям специалистов американской платформы онлайн-образования Master Class, к ключевым характеристикам цифровой экономики следует отнести:

1. Искусственный интеллект (ИИ). Как государственный, так и частный сектор активно используют ИИ для повышения эффективности своей деятельности (в частности, посредством уменьшения затрат). С другой стороны, это происходит в первую очередь за счет снижения потребности в персонале, что приводит к сокращению рабочих мест, а следовательно, снижению платежеспособного спроса населения.

2. Big Data (большие данные). Цифровые платформы ежеминутно получают сотни килобайтов информации от пользователей, в результате чего формируется гигантский массив персональных данных каждого клиента. Это позволяет компаниям обеспечивать индивидуальный подход к ним, предлагать товар и (или) услуги, соответствующие их потребностям. Однако есть и те, кто расценивает это как вторжение в частную жизнь, даже несмотря на согласие пользователя предоставить информацию.

3. Цифровые цепочки поставок. По мере роста количества отраслей, использующих онлайн-среду, возрастает значимость цифрового взаимодействия (социальных сетей, мобильных приложений, стриминговых площадок и т.д.).

4. Гиперсвязь. Технология широкополосного беспроводного доступа обеспечивает динамическую связь между абонентами, интернет-ресурсами и т.д.

5. Интернет вещей (IoT). Цифровой мир выходит за рамки традиционных компьютеров и мобильных телефонов и реализуется в виде повсеместно используемых физических устройств, подключенных к интернету.

6. Мобильные технологии и рекламу. На данный момент смартфоны являются, пожалуй, наиболее доступными вычислительными системами в мире. Одновременно компании могут осуществлять рекламную рассылку на мобильное устройство [87].

Несмотря на отсутствие общепринятых критериев цифровой экономики, Р. Бухт и Р. Хикс на основе имеющихся данных выделили присущие ей характерные черты:

1. Имеет место неравномерное распределение стран с цифровой экономикой в мире. Роль цифровой экономики в странах глобального Севера отличается от ее роли в странах глобального Юга. Распределение внутри регионов также неравномерно. Так, например, среди стран глобального Севера лидирующую позицию в ИТ-секторе занимают США, на долю которых по состоянию на 2017 год приходилась почти четверть мирового объема электронной торговли. Аналогичную картину можно обнаружить и среди стран глобального Юга. Так, по данным 2016 года, среди стран, где на долю ИТ-сектора приходится более 7 % ВВП, лидируют Индия и Филиппины.

2. Темпы роста цифровой экономики превышают интенсивность роста экономики в целом, особенно в странах глобального Юга. Так, согласно данным компании McKinsey, использование ресурсов сети в период с 2006 по 2011 годы способствовало приросту ВВП в развитых странах примерно на 20 %, в развивающихся странах – более чем на 10 %, в прочих странах – более чем на 5 %.

3. Цифровая экономика способствует созданию дополнительных рабочих мест. Согласно данным, приведенным в статье [22], доля занятых

в цифровом секторе в 2014–2016 годы в развивающихся странах составила около 1 %, а в развитых экономиках глобального Севера – порядка 4 %.

Отечественные авторы Ж.Д. Кулагина и О.В. Мамателашвили среди характерных признаков цифровой экономики выделяют [111]:

- виртуальность;
- опору на информационные и телекоммуникационные технологии;
- персонификацию;
- непосредственное взаимодействие между производителем и потребителем;
- высокие темпы роста;
- электронные деньги, цифровую валюту;
- цифровые товары.

В свою очередь, Е.В. Попов и К.А. Семячков [52] выделяют следующие особенности цифровой экономики:

1. Наличие интеллектуальных активов, которые используются для повышения экономической эффективности. Например, такие яркие представители интернет-экономики, как Facebook, Uber, Airbnb, не располагая значительными физическими активами, имеют рыночную капитализацию выше, чем у многих промышленных гигантов.

2. Увеличение значимости данных в процессе осуществления экономической деятельности. Тенденцией в области управления данными, заслуживающей особого внимания, являются «облачные» технологии. Поскольку «облачные» технологии трансформируют вычисления в услугу, компаниям не требуется осуществлять серьезные капиталовложения для закупки вычислительных мощностей.

3. Основной организационной структурой становится сеть, а не иерархия. Гибридные формы организации более приспособлены к быстрым изменениям на рынке, что сказывается на их эффективности. Многие крупные организации с жесткой иерархической структурой адаптируются к новым реалиям, снижая число уровней иерархии, размывая границы подразделений и отказываясь от непрофильных направлений деятельности (прибегая к аутсорсингу).

4. Основным инструментом поиска информации и связи служит интернет. Развитие широкополосного и мобильного интернета, интернет-приложений и гаджетов коренным образом изменило способы коммуникации в обществе.

5. Обмен данными носит глобальный характер. Экономические агенты, не имеющие доступа к глобальной сети передачи данных, рынкам и технологиям других стран и функционирующие лишь на ограниченных локальных рынках, неизбежно уступают в конкурентной борьбе.

6. Основным подходом к управлению является самоорганизация. Экономика, основанная на децентрализации и глобализации, служит основой для формирования сетевых структур по принципу «снизу вверх» и

перехода бюрократических структур к более гибким и эффективным формам. Другими примерами процессов самоорганизации являются краудсорсинг, краудфандинг и т.д.

Таким образом, термин «цифровая экономика» относится исключительно к происходящей сейчас и еще не завершенной трансформации всех секторов экономики благодаря цифровизации информации при помощи компьютерных технологий.

Для того чтобы количественно оценить уровень развития цифровой экономики государства, его вклад в ВВП страны, построить рейтинги развития цифровой экономики и оценить место своего государства в глобальном мире цифровой экономики, необходимо понять, какой сегмент экономики является цифровым и как он измеряется. Степень цифровизации экономики определяется различными показателями и критериями, как общепризнанными мировым сообществом, так и менее известными. Более подробно данный вопрос будет рассмотрен в следующем разделе.

## **2.2. Подходы к оценке уровня цифровизации**

Принимая во внимание все увеличивающееся количество видов экономической деятельности, основанных на использовании цифровых технологий, и их растущую вследствие этого экономическую значимость, можно считать измерение цифровой экономики первоочередной задачей. Однако, как показывает практика, на данный момент не выработан универсальный, общепризнанный подход к оценке, что в значительной степени обусловлено отсутствием среди исследователей единой позиции относительно самого понятия «цифровая экономика». К основным методологическим проблемам оценки уровня цифровизации обычно относят [22]:

- проблему качества данных;
- проблему оценки стоимости и эффекта;
- виртуальный характер цифровой экономики;
- неприменимость в ряде случаев методов традиционного экономического анализа.

В 2018 году американцы тратили в среднем 6,3 часа в день на цифровые медиа, такие как Google, Wikipedia, социальные сети, онлайн-курсы, навигаторы. Они обменивались сообщениями, устраивали видеоконференции, слушали музыку, проводили время в приложениях для смартфонов и делали многое другое. Однако данный факт практически не учитывается в официальных показателях экономической деятельности государства, таких, например, как ВВП и производительность труда [78].

Для того чтобы определить вклад интернета в экономику, необходимы более эффективные способы измерения бесплатных сервисов, таких как Facebook, Google и Wikipedia. Э. Бринольфссон (старший научный сотрудник Стэнфордского университета) совместно с Ф. Эггерсом из Университета Гронингена разработал методы, позволяющие оценить вклад интернета в развитие экономики. В частности, их исследование показало, что происходит существенное повышение благосостояния населения. При этом в хозяйственной практике ВВП прочно занял место если не единственного, то важнейшего измерителя общественного прогресса [78].

Например, концепция потребительского излишка представляла собой разницу между тем, что мы готовы заплатить за товар, и тем, что мы действительно должны заплатить. Так, если мы были готовы заплатить за товар 100 рублей, но заплатили только 40, то излишек потребителя оценивается в 60 рублей. Неудобство заключается в том, что в масштабе всей страны получить достоверную оценку потребительского излишка затруднительно.

В отличие от ВВП, который зависит от того, сколько мы фактически платим за товары и услуги (соответствующая сумма отражается на терминале кассового аппарата и, следовательно, в отчетах о доходах компании), потребительский излишек, как правило, явным образом не фиксируется. Однако наряду с трудностями цифровая революция открыла и новые инструменты. В частности, Э. Бринольфссон и Ф. Эггерс воспользовались методом онлайн-опроса. Данный метод позволил им провести социологический опрос сотен тысяч потребителей при помощи интернет-технологий. Респондентам был задан вопрос об их предпочтениях, что дало возможность получить оценки потребительского излишка для различных категорий товаров, в том числе бесплатных, которые отсутствуют в экономической статистике.

Предложенный подход позволил авторам напрямую оценить масштаб потребительского излишка, предлагая покупателям сделать выбор в пользу приобретения товара или отказа от него в обмен на денежную компенсацию. Поскольку предлагалось получить реальные деньги, результатам проведенного опроса можно доверять.

Потребительский излишек представляет собой чистый выигрыш потребителя, характеризующий прирост его благосостояния. Такая мера особенно важна, когда физические товары, которые потребителю приходилось покупать ранее, переходят в категорию цифровых.

Э. Бринольфссон и Ф. Эггерс в качестве наглядного примера подтверждения справедливости своей гипотезы приводят сравнение старейшей англоязычной универсальной Британской энциклопедии (стоимостью несколько тысяч долларов) и общедоступной многоязычной

универсальной интернет-энциклопедии со свободным контентом Wikipedia (Википедия).

В то время как издатели отмечают сокращение спроса на печатную продукцию, в том числе энциклопедии, количество обращений к ресурсу Wikipedia повсеместно растет. В ходе исследования авторы установили, что среднестатистический потребитель в США оценивает Википедию примерно в 150 долларов в год, при этом пользуясь ею бесплатно.

Чтобы оценить потребительский излишек, генерируемый Facebook (деятельность Facebook в России признана экстремистской и запрещена), авторы построили репрезентативную выборку пользователей этой социальной сети из США. Им был задан вопрос о том, за какие деньги они готовы отказаться от использования Facebook в течение месяца. Полученным данным можно доверять, поскольку в случае отказа респонденты получали требуемую сумму.

Согласно результатам исследования, среднестатистический пользователь Facebook в США готов отказаться от использования социальной сети на месяц за 48 долларов, 20 % отказались бы всего за один доллар, а 20 % – более чем за 1 000 долларов. В целом, по оценкам Э. Бринольфссона и Ф. Эггерса, в период с 2004 по 2017 годы потребители получали от Facebook в среднем 16 миллиардов долларов в год. При этом данный показатель не учитывался в составе ВВП [78].

Тем не менее фирмы находятся в менее выгодном положении по сравнению с потребителями. Так, согласно исследованию, проведенному У. Нордхаусом, максимальная степень поглощения фирмой потребительского излишка от технологических инноваций в течение XX века оценивается в 2,2 %, в то время как остальные 97,8 % приходятся на потребителей [117]. Например, компания Facebook зарабатывает деньги на рекламе, но если бы она начала взимать хотя бы один доллар с пользователей, то они массово перешли бы на альтернативные платформы, такие как Snapchat, Instagram или YouTube.

Отечественные авторы Ж.Д. Кулагина и О.В. Мамателашвили [111] к ключевым показателям цифровизации экономики относят:

- глубину проникновения интернет-технологий в общество;
- многоканальные модели доставки товаров и услуг;
- облачные технологии и сервисы;
- автоматизацию и роботизацию производства и домашних хозяйств;
- простоту предоставления услуги в цифровом поле;
- анализ bigdata;
- доступность интернет-соединения в любое время и в любом месте.

Европейская комиссия разработала Индекс цифровой экономики и общества DESI (The Digital Economy and Society Index) для отслеживания прогресса государств-членов на пути к цифровизации экономики и ее влияния на социум. Оценка готовности стран к цифровой экономике

основана на расчете таких показателей [79], как возможность подключения, человеческий капитал, использование интернета, интеграция цифровых технологий и цифровых госуслуг.

Результаты расчета DESI за 2017 год показывают, что наиболее развитые цифровые экономики в ЕС имеют Дания, Финляндия, Швеция и Нидерланды, за ними следуют Люксембург, Бельгия, Великобритания и Ирландия. Румыния, Болгария, Греция и Италия получили самые низкие баллы по DESI [79].

Индекс цифровой эволюции DEI (Digital Evolution Index) отражает, насколько страны открыты к внедрению инноваций, а также оценивает уровень доверия к цифровым технологиям по всему миру. Индекс разработан MasterCard совместно со Школой Флетчера при Университете Тафтса.

Индекс за 2017 год рассчитывался на основе изучения уровня цифровизации 60 стран. Всего было проанализировано 170 показателей, сгруппированных следующим образом [88]:

- 1) уровень предложения ИКТ (наличие доступа к интернету и степень развития инфраструктуры);
- 2) спрос на цифровые технологии;
- 3) уровень развития институциональной среды (политика государства, законодательство, ресурсы);
- 4) инновационный климат (инвестиции в НИОКР, digital-стартапы).

Продолжение сотрудничества компании MasterCard и Школы права и дипломатии Флетчера привело к разработке Индекса цифрового развития DII (Digital Intelligence Index) [88].

В 2020 году индекс базировался на двух показателях: цифровое развитие и цифровое доверие. Уровень цифрового развития отражает динамику перехода экономики от материального прошлого к цифровому настоящему. Цифровое доверие служит связующим элементом между настоящим и будущим на основе цифровых технологий и инклюзивности.

Индекс цифрового развития составляется активными пользователями интернета из 90 стран мира и основывается на анализе 160 показателей, сгруппированных следующим образом: показатели институциональной среды, факторы спроса, условия поставщиков и потенциал для осуществления инноваций.

В ходе исследования были выделены четыре категории стран [88]:

ведущие экономики с развитой цифровой средой (Сингапур, США, Гонконг, Южная Корея, Тайвань, Германия, Эстония, ОАЭ, Израиль, Чешская Республика, Малайзия, Литва и Катар);

стабильные экономики с высоким уровнем внедрения электронных технологий, несмотря на некоторое замедление темпов цифрового развития (Швеция, Великобритания, Нидерланды, Япония и Канада);

прогрессивные экономики, привлекательные для инвесторов в основном за счет активной динамики и большого потенциала в плане цифрового развития (Россия, Китай, Индия, Индонезия и Польша);

нестабильно развивающиеся экономики с проблемами в сфере инфраструктуры (Нигерия, Уганда, Колумбия, Перу, Пакистан, Шри-Ланка). Тем не менее молодое население в этих странах проявляет энтузиазм в отношении цифрового будущего и активно пользуется социальными сетями и системами электронных платежей.

Оценка уровня «цифрового доверия» базируется на анализе 198 показателей, характеризующих поведение и отношение населения, условия жизни, а также пользовательский опыт. В выборку вошли 42 страны, разделенные на четыре категории [88]:

1) страны, в которых повышается пользовательская активность (Бразилия, Колумбия и Мексика). В них отмечается значительная активность в социальных сетях;

2) страны с наиболее позитивным восприятием цифрового будущего (Китай, Индонезия и Вьетнам). Такому отношению способствует активное внедрение цифровых технологий и осознание новых возможностей от их применения;

3) страны с устоявшимся подходом к цифровизации, в том числе на государственном уровне, такие как Швеция, Нидерланды и Дания. Они придерживаются мер, направленных на укрепление доверия населения к новым технологиям (политика конфиденциальности, безопасности и подотчетности). Жители этих стран, как правило, положительно относятся к цифровому будущему;

4) страны с высоким уровнем охвата жителей цифровыми технологиями, что является гарантом лидерства в постцифровом будущем (США, Гонконг, Тайвань, Южная Корея и Сингапур). Они предоставляют пользователям широкие возможности взаимодействия в цифровой среде.

Согласно результатам исследования 2020 года, экономики стран Восточной Европы продемонстрировали наиболее высокие показатели, чему во многом способствовало упрощение доступа в интернет, модернизация инфраструктуры для проведения цифровых транзакций, улучшение ситуации с электроснабжением [88].

Индекс цифровизации экономики, разработанный Boston Consulting Group (e-Intensity), оценивает влияние интернета на развитие бизнеса и общества по 28 показателям, распределенным на три субиндекса.

Интегральный индекс e-Intensity рассчитывается как среднее арифметическое следующих трех субиндексов с учетом их весовых коэффициентов [99]:



1) развитие инфраструктуры – отражает наличие и скорость мобильного и стационарного доступа в интернет; его вес в интегральном индексе e-Intensity определен экспертами Boston Consulting Group (BCG) на уровне 50 %;

2) онлайн-расходы – включают расходы на электронную коммерцию и интернет-рекламу;

3) активность пользователей – рассчитывается как средневзвешенное значение показателей активности компаний, потребителей и государственных органов.

Индекс развития ИКТ (ICT Development Index – IDI) – это составной индекс, который используется для мониторинга развития ИКТ в стране с течением времени и сравнения их между собой. IDI объединил ряд показателей, которые распределились по следующим трем субиндексам [99]:

1) доступность – отражает готовность страны использовать ИКТ и включает показатели инфраструктуры и доступа (объем подписок на стационарную и сотовую телефонную связь, пропускная способность интернета на одного пользователя; доля домохозяйств, имеющих компьютер, и домохозяйств, имеющих доступ в интернет);

2) использование – оценивает интенсивность использования ИКТ и включает такие показатели, как численность физических лиц, использующих интернет, объемы подписок на фиксированную и подвижную широкополосную связь;

3) практические навыки – характеризует наличие компетенций и навыков, необходимых для работы с ИКТ. Он включает такие косвенные показатели, как средняя продолжительность обучения, общий охват средним образованием и общий охват высшим образованием. Поскольку это косвенные показатели, а не напрямую измеряющие навыки работы с ИКТ, они имеют меньший вес при расчете IDI.

В настоящее время данный индекс не публикуется из-за разногласий между разработчиками.

Индекс мировой цифровой конкурентоспособности WDCI (World Digital Competitiveness Index<sup>10</sup>) составляется Центром мировой конкурентоспособности (World Competitiveness Center) начиная с 2017 года. Он оценивает способность и готовность 63 стран внедрять и использовать цифровые технологии в качестве ключевого фактора экономических преобразований в бизнесе, правительстве и обществе в целом.

В версии отчета за 2022 год было изучено 54 показателя, сгруппированных в три блока:

---

<sup>10</sup> Индекс мировой цифровой конкурентоспособности – World Digital Competitiveness Index. URL: <https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/> (дата обращения: 17.01.2023).

- 1) знания (эксперты, образование, наука);
- 2) технологии (регулирование, инвестиции, уровень развития связи);
- 3) готовность (способность к адаптации, гибкость управления, уровень интеграции ИТ-бизнеса).

Часть показателей определяется на основе статистических данных, часть базируется на экспертных оценках.

Так, например, согласно данным ежегодного рейтинга за 2022 год, по значению Индекса мировой цифровой конкурентоспособности впервые за весь период наблюдений лидирует Дания, а США (также впервые) заняли второе место. Это во многом обусловлено лучшей подготовленностью Дании к будущему цифровому миру. Дания остается одной из ведущих экономик мира по уровню подготовки специалистов для сферы ИТ. В пятерку лидеров вошли также Швеция, Сингапур и Швейцария, заняв соответственно третье, четвертое и пятое места [115].

Коллектив авторов в составе Н.Г. Каримова, Ф.А. Хамидовой и Р.А. Парпиевой [99] исследовал влияние цифровизации на экономическую безопасность страны. При этом исследователи анализировали следующие макроэкономические показатели:

ВВП на душу населения. Рассчитывается путем деления ВВП на численность населения соответствующего региона;

средний уровень инфляции. Наиболее распространенным параметром инфляции является индекс потребительских цен (ИПЦ). Он отражает изменение цены фиксированной потребительской корзины, содержащей ряд потребительских товаров и услуг, приобретаемых типичным горожанином. Индекс равен отношению цены потребительской корзины в текущем году к цене потребительской корзины в базисном году;

уровень безработицы по методологии Международной организации труда (МОТ). Определяется как отношение численности безработных к численности экономически активного населения в процентах.

На данном этапе исследования необходимо изучить российский опыт оценки цифровизации на уровне страны в целом, а также по отдельным видам экономической деятельности.

В целях обеспечения расчета значений целевых показателей, установленных для достижения национальной цели развития Российской Федерации «Цифровая трансформация», определенной Указом Президента Российской Федерации от 21 июля 2020 года № 474 «О национальных

целях развития Российской Федерации на период до 2030 года», в декабре 2020 года Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18 ноября 2020 года № 600 были утверждены методики расчета ряда целевых показателей:

достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления;

увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95 %;

рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к информационно-телекоммуникационной сети Интернет, до 97 %;

увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 года;

увеличение вложений в отечественные решения в сфере информационных технологий на уровне субъектов Российской Федерации.

Целевой показатель «достижение “цифровой зрелости”» предназначен для формирования возможности определения целевых значений целевого показателя в ключевых отраслях экономики и социальной сферы, в том числе здравоохранении, образовании и государственном управлении.

Данный показатель базируется на определении трех составляющих:

численности специалистов, интенсивно использующих ИКТ (к 2030 году запланирована на уровне 125 % от значения 2019 года);

объема расходов организаций на внедрение и использование современных цифровых решений (к 2030 году запланирован на уровне 200 % от значения 2019 года);

доли достижения целевого значения цифровой зрелости отраслей экономики и социальной сферы (к 2030 году запланирована на уровне 100 % от значения 2019 года).

Методика расчета целевого показателя увеличения вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 года предназначена для определения целевых значений показателя «доля массовых социально значимых услуг, доступных в электронном виде в рамках достижения национальной цели “Увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95 %”».

Методика расчета целевого показателя увеличения вложений в отечественные решения в сфере информационных технологий на уровне субъектов Российской Федерации предназначена для определения целевых значений показателя «доля домохозяйств, которым обеспечена

возможность широкополосного доступа к сети Интернет» в рамках достижения целевого показателя «рост доли домохозяйств, которым обеспечена возможность широкополосного доступа в сеть Интернет, до 97 %», используемого для мониторинга достижения национальной цели развития Российской Федерации «Цифровая трансформация», установленной Указом Президента Российской Федерации от 21 июля 2020 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года», по каждому субъекту Российской Федерации.

Во исполнение протокола заседания Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 октября 2018 года № 1, поручения Правительства Российской Федерации от 10 ноября 2018 года № ДМ-П6-7776, а также с учетом Постановления Правительства Российской Федерации от 2 марта 2019 года № 234 «О системе управления реализацией национальной программы “Цифровая экономика Российской Федерации”» Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 428 от 1 августа 2018 года утверждены разъяснения (методические рекомендации) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации». В частности, в них приведены показатели, на основе которых оценивается развитие цифровой экономики на уровне регионов.

Уровень развития информационной инфраструктуры предложено оценивать (в процентах), определяя долю подключенных к сети Интернет медицинских организаций государственной и муниципальной систем здравоохранения субъекта РФ (больниц и поликлиник), фельдшерских и фельдшерско-акушерских пунктов медицинских организаций государственной и муниципальной систем здравоохранения субъекта РФ, образовательных организаций государственной собственности субъекта РФ и муниципальной собственности, реализующих образовательные программы общего образования и/или среднего профессионального образования; органов власти субъекта Российской Федерации и органов местного самоуправления.

Уровень обеспеченности цифровой экономики кадрами предложено оценивать на основе определения следующих показателей:

количества выпускников организаций профессионального образования государственной собственности субъекта РФ и муниципальной собственности с ключевыми компетенциями цифровой экономики (человек);

количества трудоспособных жителей субъекта РФ, прошедших переобучение по компетенциям цифровой экономики в рамках дополнительного образования (человек).

Оценку уровня информационной безопасности предложено проводить на основе расчета трех показателей:

среднего срока простоя информационных систем органов власти субъекта РФ и органов местного самоуправления в результате компьютерных атак (часов);

количества специалистов, подготовленных по образовательным программам в области информационной безопасности в организациях высшего профессионального образования и организациях среднего профессионального образования, расположенных в субъекте РФ (человек);

стоимостной доли закупаемого и (или) арендуемого органами исполнительной власти субъекта РФ, органами местного самоуправления отечественного программного обеспечения (%).

Оценку обеспеченности цифровыми технологиями рекомендуется проводить на основе такого показателя, как увеличение затрат (в процентном выражении) на развитие «сквозных» цифровых технологий компаниями, зарегистрированными на территории субъекта РФ.

Для определения уровня развития цифрового государственного управления рассчитываются следующие показатели, %:

доля взаимодействий граждан и коммерческих организаций с органами власти субъекта РФ, органами местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, осуществляемых в цифровом виде;

доля приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, соответствующих целевой модели цифровой трансформации (предоставление без необходимости личного посещения государственных органов и иных организаций, с применением реестровой модели, онлайн (в автоматическом режиме), проактивно);

доля отказов при предоставлении приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, от числа отказов в 2018 году;

доля внутриведомственного и межведомственного юридически значимого электронного документооборота органов власти субъекта РФ и местного самоуправления и организаций государственной собственности субъекта РФ и муниципальной собственности.

Более подробное описание методики расчета показателей приведено в прил. Б.

Несмотря на пристальное внимание к проблемам цифровизации, вопросы влияния цифровых технологий на экономическую безопасность изучены и разработаны недостаточно.

На наш взгляд, цифровизация экономики влияет на экономическую безопасность как на стыке системных, структурных и отраслевых групп, так и для отдельных личностей. Вследствие этого происходит изменение материального положения в семье в результате увеличения или уменьшения доходов отдельных лиц, усиливается расслоение трудоспособного населения по уровню знаний, достатка, социальному положению вследствие автоматизации производства. Более подробно данный вопрос рассмотрен в следующем разделе монографии.

### **2.3. Цифровые угрозы экономической безопасности бизнеса**

В условиях цифровой трансформации в деятельности любого хозяйствующего субъекта присутствуют информационные ресурсы – данные в цифровом формате, которые, наряду с человеческими, финансовыми и материальными ресурсами, становятся одним из важнейших ресурсов менеджмента. Их накопление и потребление составляет основу эффективного функционирования и развития цифровой экономики предприятия, а целостность и достоверность информации как цифрового нематериального актива выступает одним из главных элементов управления бизнес-процессами предприятия.

Цифровая экономика создает условия для миграции рабочей силы, жизни в виртуальном пространстве, где человек-профессионал становится эволюционно устаревшим, неконкурентоспособным.

Будущий киберчеловек (интегрированный в виртуальную среду) осуществляет свою деятельность и обустроивает жизнь в виртуальном пространстве, полностью зависящем от него. Принципы, положения, постулаты существования и деятельности человека в условиях цифровой мировой экономики, по мнению П.А. Левчаева [108], заключаются в следующем:

- 1) виртуальный, цифровой мир предполагает доминирование цифровых технологий, цифровизацию всех сфер деятельности;
- 2) цифровая среда требует не только смены носителя (диск, флешка, винчестер, облачные хранилища), но и улучшения передаваемого образа (например, перехода от стандартов мобильной связи 3G к 5G);
- 3) цифровые технологии, составляющие основу общества, определяют его надстройку;
- 4) цифровой мир, экономика развиваются по законам разработчика технологий;
- 5) в цифровом мире экономики имеются все возможности развития, трудоустройства, создания стоимости;

6) в цифровой экономике гораздо проще превратиться в «фичу», «приложение», использующее возможности, чем осуществлять творческий процесс;

7) факторы производства, такие как труд, земля, капитал, предпринимательские навыки и информация, не определяют доминирование в виртуальной экономике. Решающее значение имеют здесь объем и скорость обработки информации, создание многомерных цифровых образов действительности;

8) виртуальная реальность предполагает доминирование цифровых технологий в жизни человека;

9) в цифровой экономике классические составляющие производительных сил и производственных отношений подвергаются существенной модификации;

10) развитие цифрового мира обусловлено синергетическими эффектами бифуркации и характера эволюции;

11) создаются условия для минимизации всех видов затрат и максимизации прибыли;

12) происходит замена человека даже в творческой сфере.

В данном контексте риски и угрозы, связанные с информацией и данными в цифровом формате, технологиями их получения, обработки, хранения и предоставления, становятся одними из основных и значимых рисков экономической безопасности в условиях цифровой экономики, поскольку их составляющая проецируется на все прочие риски основной деятельности. Возникают трудности с использованием новых возможностей (например, из-за низкого уровня цифровых навыков и недостаточного уровня проникновения технологий внутри стран).

Несомненно, цифровизация имеет большое количество преимуществ, проявляющихся в виде многочисленных мультипликативных эффектов от включения всех производственных цепочек в единое информационное пространство. Однако ее влияние на общество и экономическую безопасность государства неоднозначно [99].

Во-первых, обеспечение перехода экономического развития на новый уровень определяет разрушение прежней системы производства и распределения товаров. И это уже характеризует цифровые технологии как «подрывные».

Во-вторых, внедрение новых технологий характеризуется чрезмерным оптимизмом, когда кумулятивный эффект от использования цифровых преимуществ гораздо слабее ожидаемого.

В-третьих, наблюдается неравномерное распределение положительного эффекта от внедрения цифровой экономики как между странами, так и между группами населения внутри стран.

В-четвертых, цифровизация наиболее выгодна в финансовой сфере. В то же время «сквозные технологии» (роботизация, блокчейн-технология,

нейронные сети, ИИ, квантовая виртуальная и дополненная реальность) оптимизируют производство, автоматизируют производственные процессы, осуществляют дистанционное управление, приводят к сокращению количества рабочих мест вплоть до их полной ликвидации.

Наряду с положительными моментами цифровизация несет в себе и определенные риски. Здесь следует различать риски цифровой трансформации и риски цифровизации, вызванные внедрением цифровых технологий в экономику. Основным риском цифровой трансформации для экономической безопасности государства является рост уровня безработицы. В то же время могут возникать новые потребности и запросы рынка на новые профессии (кинезиолог, специалист по солнечным технологиям, аналитик транспортных средств, личный веб-менеджер, посол корпоративной культуры, городской фермер, аудитор экосистемы, консультант по роботам, цифровой мемуарист, дизайнер геймификации, архитектор виртуальной реальности, инженер по 3D-печати, консультант по цифровой валюте) и происходить трансформации существующих (учитель, школьный диетолог, библиотекарь).

Анализ источников позволил систематизировать цифровые угрозы и вызовы, существенно влияющие на экономическую безопасность. Например, Е.В. Попов и К.А. Семячков предлагают разделить всю совокупность угроз как минимум на следующие группы (табл. 8) [52].

*Таблица 8*

**Проблемы экономической безопасности цифрового общества**

Угрозы	Пояснения и примеры
Системные	Проблемы, касающиеся экономики в целом или ее отдельных подсистем (зависимость от цифровых технологий других государств, отсутствие собственной элементной базы, проблема «цифрового неравенства»)
Структурные	Структурные проблемы, вызванные цифровизацией (например, существенные изменения на рынке труда и рост безработицы)
Отраслевые	Отсутствие цифровых решений для отдельных отраслей (например, отсутствие собственной платежной системы)
Деятельность отдельных предприятий	Хищение корпоративных данных, промышленный шпионаж, хакерские атаки, недостаточная обеспеченность цифровыми технологиями, компетентными кадрами и т.д.
Деятельность отдельных граждан	Кража личных данных, манипулирование

Согласно М.И. Дроздовой и Д.А. Осетрову [31], внедрение цифровых технологий влечет за собой риски, которые напрямую воздействуют на экономическую безопасность государства:

безработицу, сокращение рабочих мест, ликвидацию отдельных специальностей;



зависимость от импортных технологий;  
исчезновение приватности;  
утечку конфиденциальной информации и персональных данных;  
снижение уровня безопасности данных;  
проблемы правового регулирования.

Бизнес-процессы остаются уязвимыми, системы безопасности не в состоянии защитить их. Под влиянием этих обстоятельств возникают различные угрозы и риски экономической безопасности на микроуровне.

Среди рисков и угроз экономической безопасности, которые влечет за собой цифровая трансформация предприятия, И. Кирищева, М. Скорев, О. Мищенко, Т. Графова выделяют [100]:

информационные риски и угрозы;  
риски и угрозы информационной безопасности (кибербезопасности);  
риски, связанные с использованием технологий цифровой экономики;  
инвестиционные риски и угрозы;  
риски и угрозы человеческим ресурсам;  
риски и угрозы, связанные с удаленным управлением;  
организационно-управленческие риски;  
риски и угрозы правового характера.

Риски и угрозы информационной безопасности, в отличие от информационных угроз и рисков, являются результатом преднамеренного воздействия на информацию, данные в цифровой форме, функционирование информационных ресурсов и систем в цифровом пространстве.

В зависимости от механизма воздействия рисков информационной безопасности при цифровой трансформации экономики предприятий предлагается следующая классификация информационных угроз и рисков [100]:

потеря информационного ресурса;  
потеря доступа к информационному ресурсу, нарушение его целостности, доступности в результате умышленного воздействия;  
кража информации и данных в цифровом формате;  
умышленное искажение информации;  
сбои и отказы технических и программных средств автоматизированных систем управления и информационных систем, а также нарушение функционирования программных средств и средств защиты в результате умышленного воздействия;  
распространение вредоносных программ и закладок;  
шпионское программное обеспечение;  
несанкционированный доступ;  
нарушение авторского права.

Угрозы экономической безопасности бизнеса в условиях цифровой трансформации представлены в табл. 9, составленной по материалам источника [100].

Таблица 9

Угрозы экономической безопасности цифрового предприятия

Информационный капитал	Организационный капитал	Человеческий капитал
Неэффективное использование информационных и коммуникационных технологий	«Обвал» уровней структуры при снижении барьеров и задержек в распространении информации	Снижение уровня компетентности персонала при применении новых цифровых технологий
Наличие «незрелых» цифровых технологий, использование несовершенных технологий и каналов связи	Саботаж, аварии, кибератаки, виртуальные грабежи	Психологическое неприятие цифровых технологий работниками разного уровня
Изменения в законодательстве в сфере информации, цифровых технологий, лицензий и патентов, в отношении интеллектуальной собственности	Вытеснение человека из системы управления, появление ИИ, роботизация	Неумение персонала ориентироваться в быстро меняющейся среде, консервативность мышления
Выход из строя машин и оборудования, нарушение техники безопасности		
Растущая технологическая зависимость от зарубежных поставщиков цифровых технологий		

Все многообразие рисков и угроз для бизнеса в условиях цифровизации авторы работы [100] условно подразделяют на пять групп:

**1. Программные** – вызваны внедрением и воздействием вредоносных программ («вирусов»), программных «закладок»; уничтожение или изменение данных в информационных системах; умышленное изменение параметров, состава и конфигурации информационной системы и ресурса, приводящее к их несоответствию таковым при испытаниях и сертификации.

**2. Технические** – внешнее воздействие на информационно-управляющие системы и каналы передачи информации с целью нарушения их нормальной работы; сбои и нарушения в работе аппаратно-программных средств цифровой среды предприятия на всех этапах их использования, вызванные целенаправленным воздействием.

**3. Физические** – уничтожение средств обработки и носителей информации; кража носителей, а также аппаратных или программных электронных ключей доступа и аутентификации.

**4. Информационные** – нарушение правил обмена информацией; несанкционированный доступ, сбор, хищение, использование и распространение информационных ресурсов; незаконное копирование данных в информационных системах; дезинформация, сокрытие или искажение информации; преднамеренное искажение и недопустимое изменение характеристик информационных потоков в цифровых каналах, поступающих от источников и передаваемых потребителям.

**5. Организационные** – обусловлены неэффективностью мероприятий по обеспечению киберзащиты; несоблюдением и нарушением требований документов и нормативных актов, регулирующих сферу информационной безопасности; недостаточной эффективностью применяемых методов и средств оперативной защиты программ и данных и обеспечения безопасности функционирования информационной системы в условиях случайных негативных воздействий.

**Программные риски** непосредственно связаны со сбоями и системными ошибками в функционировании программного обеспечения.

**Технические риски** связаны с аппаратно-программной средой информационной системы или цифрового ресурса и их эксплуатацией, то есть с жизненным циклом информационной системы. Включают в себя:

**аппаратные риски**, вызванные выходом из строя компонентов информационной системы, таких как серверы, персональные компьютеры, сетевые коммутаторы и маршрутизаторы, производственное оборудование, станки и т.д.;

**проектные риски** – системные ошибки в постановке целей и задач проектирования информационной системы, формулировании требований к функциям и характеристикам решения задач цифровизации процесса или объекта, определении условий и параметров внешней среды; ошибки алгоритмического проектирования при непосредственной алгоритмизации функций программных средств и баз данных, при определении структуры и взаимодействия компонентов программных комплексов, а также при использовании информации из баз данных; ошибки программирования в текстах программ и описаниях данных, а также в исходной и результирующей документации на компоненты информационной системы.

Источниками **информационных рисков** предприятия являются информационные активы, к которым относятся любая информация и данные в цифровой форме (цифровые модели бизнес-процессов, оцифрованные сервисы, цифровой контент, цифровые сервисы, базы данных, веб-ресурсы, программное обеспечение, оцифрованные данные с различных датчиков, данные электронных носителей), информация, обрабатываемая в корпоративных информационных системах и передаваемая по каналам передачи данных.

Информационные риски проявляются в нарушении целостности, надежности и доступности информационных активов (ресурсов). Они

могут быть связаны с надежностью аппаратных компонентов информационной системы и возможностью их выхода из строя, программными сбоями, несоблюдением требований различных стандартов при эксплуатации информационной системы и цифровых сервисов, некомпетентностью и ошибочными действиями персонала предприятия (внутренняя среда), подрядчиков (аутсорсеров) и поставщиков технологий (внешняя среда), а также с несоблюдением требований стандартов на этапах проектирования, производства и эксплуатации системы.

Обеспечение безопасности любой информационной (цифровой) системы (ресурса), как известно, должно удовлетворять ряду требований, основными из которых являются:

конфиденциальность – заключается в том, что компонент системы доступен только тем субъектам (пользователям, программам, процессам), которые обладают соответствующими полномочиями;

целостность – предполагает, что компонент системы может модифицировать только субъект, имеющий на это соответствующие права, и служит гарантией корректности (неизменности, работоспособности) системы в любой момент;

доступность – означает, что субъект, имеющий соответствующие полномочия, может в любой момент получить доступ к необходимому компоненту системы (ресурса).

По своему характеру информационные риски и угрозы могут быть отнесены к одной из групп:

перехват информации – копирование злоумышленником информации или цифровых баз данных, в результате чего злоумышленник получает их полную копию. Современный уровень развития ИКТ предоставляет широкие возможности и инструменты для перехвата данных с использованием разнообразных методов и технических средств;

кража информации – субъект угрозы не только получает соответствующие данные, но и лишает их предприятие, причем объектом кражи может быть не только закрытая (конфиденциальная), но и открытая информация, необходимая для функционирования предприятия;

повреждение или уничтожение данных и информации – субъект угрозы выполняет только задачу нанести ущерб предприятию и нарушить его функционирование;

искажение информации и данных работником вследствие умышленных или неумышленных действий.

**Организационные риски** обусловлены недостаточной эффективностью разработанных правил, регламентирующих деятельность персонала, эксплуатирующего и обслуживающего информационную систему, а также проблемами системы внутреннего контроля.

Зачастую причиной реализации данной формы угрозы становится безответственность и некомпетентность персонала, что проявляется в

нарушении требований по обеспечению информационной безопасности, действующих на предприятии, как по собственной инициативе, так и под влиянием третьих лиц.

Информационные риски включают в себя:

непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих и эксплуатирующих информационную систему. Они наиболее опасны по размеру наносимого ущерба, так как не только представляют угрозу для нормального функционирования информационной системы (неверно введенные данные, приводящая к сбою системы ошибка в программе и т.п.), но и создают уязвимости, которые могут быть использованы киберпреступниками;

кражу и подделку информации – находятся на втором месте по размеру причиняемого ущерба. В результате таких противоправных действий с использованием персональных компьютеров российским организациям ежегодно наносится совокупный ущерб в размере десятков миллиардов рублей;

несанкционированный доступ к информации и несанкционированное изменение данных. К данной категории также относятся риски и угрозы, связанные с утечкой данных, использование их в своих интересах. При этом источником утечки может выступать любой носитель конфиденциальной информации, к которому злоумышленнику удалось получить несанкционированный доступ.

Организационно-управленческие риски обусловлены:

необходимостью построения новой организационной структуры, направленной на повышение эффективности цифровизации предприятия;

отсутствием налаженной горизонтальной и вертикальной интеграции подразделений компании;

неразвитостью цифровой инфраструктуры, что, с одной стороны, уже является значительным риском для экономической безопасности, а с другой – ускоренная цифровизация предприятия может сама по себе вызвать риски из-за усложнения моделей взаимодействия между участниками;

ошибочным представлением руководства предприятия о принципах, целях цифровой трансформации. Цифровая трансформация касается не столько новых технологий, сколько того, как они изменят бизнес-процессы предприятия.

К рискам и угрозам правового характера относятся [100]:

отставание нормативно-правового регулирования экономических отношений от скорости «цифровизации»;

правовая неопределенность ответственности субъектов правоотношений в цифровой экономике;

неопределенность правового статуса трудовых отношений в цифровой среде;

отсутствие правового регулирования деятельности коммерческих организаций по сбору, передаче, хранению, обработке цифровых данных субъекта;

отсутствие правового механизма контроля и надзора за соблюдением установленных требований

В отдельную группу рисков выделяют риски, связанные с использованием технологий цифровой экономики (**технологические риски**):

интернета вещей (IoT). Разнообразные чипы и датчики, встроенные в оборудование и транспортные средства, различные технические устройства, управление которыми осуществляется с помощью интернета и приложений, предоставляют широкие возможности для оптимизации использования ресурсов, рационализации транзакций, автоматизации рутинных операций. В то же время технологии IoT достаточно уязвимы для несанкционированного доступа и кибератак;

распределенного реестра Blockchain. Одной из развивающихся областей применения технологии блокчейн являются блокчейн-платформы и реализуемые через них смарт-контракты. При этом основополагающим принципом блокчейна является неизменность проводимых транзакций: даже если транзакция некорректна, вызвана сбоем, ошибочна или выполнена мошенниками, но при этом подтверждена, ее невозможно исправить или отменить. Это создает ряд уязвимостей в платформе, которые могут привести к ответвлениям («форкам») в экосистеме криптовалют или смарт-контрактов;

ИИ и технологий роботизации и автоматизации, разработанных на его основе. Наряду с новыми возможностями технологии ИИ сопряжены с высокими рисками. Таким образом, использование киберпреступниками ИИ создает угрозы утечки информации, составляющей коммерческую тайну, и т.п.;

импортных компонентов оборудования и новых цифровых технологий. Потенциальная угроза обусловлена возможностью производителя ИКТ встраивать целевые вкладки в выпускаемые компоненты в интересах спецслужб. Если учитывать, что принципиальные схемы и исходные коды программного обеспечения известны только разработчику, то риски, связанные с данной уязвимостью, могут привести к снижению уровня безопасности данных и угрозе цифровой целостности информационной системы;

облачных и распределенных вычислений. Происходят изменения в моделях поведения производителей и потребителей; зависимость компании от надежного функционирования ИКТ возрастает. Распределение ответственности в сфере информационной безопасности между пользователями предприятия, организацией – владельцем облачной платформы и интернет-провайдером объективно влечет за собой

размывание границ ответственности, снижение уровня контроля и управления средствами защиты, а также увеличивает правовую неопределенность;

сети Интернет (стабильность доступа).

Обеспокоенность ученых вызывает ряд факторов, связанных с дефицитом навыков инновационного мышления у людей, формирующих стратегию развития общества и экономики. Это порождает серьезные проблемы на всех уровнях социально-экономического управления. А.И. Рудской, А.И. Боровков, П.И. Романов и О.В. Колосова проанализировали возможные риски такого рода, которые были классифицированы в шесть укрупненных групп [58]:

1. Несопряженность скорости технических изменений и эволюции ментальности управленческих кадров.

2. Выход торговли и финансов за пределы национальных юрисдикций.

3. Постоянно растущий уровень киберпреступности и необходимость правового обеспечения функционирования мирового цифрового пространства.

4. Социальные последствия широкой цифровизации производства, связанные с высвобождением занятых и сокращением рабочих мест.

5. Риски депрофессионализации и необходимость создания устойчивой системы постоянного переобучения и получения новых знаний.

6. Риски и достоинства экономики совместного пользования.

7. Антропологический переход, состоящий в разделении человечества даже не на новые касты, а на виды.

Представленные риски и угрозы безопасности предприятия в условиях цифровой экономики подчеркивают необходимость совершенствования системы электронной безопасности. При этом особенности процесса обеспечения электронной безопасности в условиях цифрового развития заключаются в разработке и использовании инструментов выявления и оценки рисков и индикаторов уровня экономической безопасности, обеспечивающих подсистемы, в том числе информационной, технологической, кадровой, инвестиционной, нормативно-правовой составляющих.

Таким образом, цифровизация обеспечивает ряд преимуществ, но в то же время несет в себе угрозу экономической безопасности на разных уровнях управления. Поэтому дальнейшие цифровые преобразования должны осуществляться с учетом всех возможных рисков.

Если рассматривать методологию оценки рисков бизнеса с позиции его экономической безопасности, то можно отметить, что, несмотря на многочисленные описанные научным сообществом варианты решений проблемы оценки рисков, отсутствует, на наш взгляд, четкий алгоритм

проведения сравнительного анализа и учета внутренних и внешних рисков. При этом процедура определения рисков основана на анализе ретроспективных данных либо на рейтинговой оценке, которая не дает результата в стоимостном выражении. Несовершенство предлагаемых методов и методик оценки экономической безопасности на микроуровне проявляется в части установления логической взаимосвязи между объективными и субъективными факторами, влияющими на оценку экономической безопасности на уровне предприятия, научными подходами, положенными в основу этих методов, и целями их практического применения.

Все перечисленное обуславливает необходимость формирования новых подходов к выявлению и оценке ключевых угроз экономической безопасности бизнеса; понимания процессов, связанных с изменениями социальных, политических и экономических отношений; обоснования системы факторов и показателей экономической безопасности; разработки алгоритма идентификации ключевых факторов и создания принципиально новой методики диагностики угроз экономической безопасности хозяйствующих субъектов с учетом новых возможностей использования цифровых технологий и резкого увеличения объема информации.

#### **2.4. Методика оценки экономической безопасности хозяйствующих субъектов в условиях цифровизации**

Цифровизация позволяет не только обеспечить информационно-эмпирическую базу исследования и повысить достоверность полученных результатов, но и использовать новые дополнительные функциональные возможности для хранения, раскрытия и анализа информации о состоянии рынка и отдельных его сегментов.

С одной стороны, в результате цифровизации резко сокращаются входные барьеры на рынок, а также затраты на хранение, реализацию и транспортировку товаров и услуг, но, с другой стороны, она порождает серьезные проблемы, связанные с защитой информации, регулированием конкуренции, охраной интеллектуальной собственности и конфиденциальности потребителей [83]. Существующие программы с элементами ИИ позволяют оперативно отслеживать изменение рыночных цен, предоставляют возможности контроля действий конкурентов и выявления признаков отклонения от договоренностей, а также помогают выбрать наиболее прибыльную ценовую стратегию, в том числе путем сговора.

В условиях цифровизации значительно расширились возможности анализа безопасности бизнеса в аспекте взаимодействия с поставщиками и торговыми партнерами. Немаловажная причина расширения возможностей проверки контрагентов связана с тем, что добросовестному



налогоплательщику нечего скрывать. Такая ситуация представляет опасность для организаций, уклоняющихся от уплаты налогов, имеющих критическую задолженность по обязательным платежам и находящихся на грани банкротства. При рассмотрении дел в суде налоговые органы исходят из того, что организация сама должна проявлять осмотрительность при выборе контрагентов, проверяя информацию о налоговых правонарушениях, совершенных поставщиком.

Таким образом, в настоящий момент массив общедоступных данных значительно расширился, что позволяет осуществлять мониторинг, который уже не строится на режиме добровольного обмена данными. Следовательно, эта информация может быть использована для корректного анализа бизнес-партнеров по полному и верифицированному составу компаний в интересующем независимого исследователя сегменте рынка.

Однако, поскольку такие сведения представлены в формате, работа с которым требует профессиональной подготовки в области информационных технологий и навыков программирования, возникают трудности для руководителей компаний и аналитиков. В результате на рынке информационных услуг появился целый ряд компаний, предоставляющих услуги по хранению и приведению данных сведений в удобную для анализа форму.

Цифровизация порождает также ряд проблем методологического характера как на макро-, так и на микроуровне (в частности, в сфере учета и измерения прогресса цифровой экономики в рамках статистики ВВП) [129]. Например, возникает проблема неадекватного измерения эффекта от внедрения цифровых моделей взаимодействия в ВВП, поскольку при снижении цены ИКТ создается добавленная стоимость, обеспечивающая возрастающую полезность, которая не имеет экономической ценности.

Система распределенных регистров и некоторые методы ИИ становятся основными сквозными цифровыми технологиями на микроуровне, используемыми бизнесом для обеспечения корпоративного стратегического целеполагания [73]. При этом на корректность и адекватность оценки безопасности, благонадежности контрагентов и идентификации рисков компании оказывают большое влияние достоверность и качество используемой информации.

Современные методики мониторинга уровня экономической безопасности предприятия основаны на методах и приемах анализа и оценки рисков, конкурентоспособности, финансового состояния, платежеспособности и финансовой устойчивости или эффективности использования ресурсов. Анализ факторов риска, способных создавать социально-экономические ситуации критического характера, и оценка возможных экономических потерь в случае нарушения экономической и финансовой безопасности являются важнейшей составляющей мето-

дологии мониторинга уровня экономической безопасности компании, включающего в себя:

1) оценку состояния экономической безопасности в виде системы сложных факторов (функциональных составляющих, или детерминант экономической безопасности), характеризующих различные ее аспекты;

2) вычисление единого интегрального показателя, оценивающего экономическую безопасность предприятия в целом.

В первом случае единственный обобщенный показатель экономической безопасности отсутствует, результаты оценки представлены по каждой составляющей в виде системы показателей в разрезе выбранных детерминант. Сюда можно отнести, в частности, методики [20, 33, 42, 71].

Для интерпретации результатов активно применяется графический метод, который позволяет выполнить визуальную комплексную оценку разнородных факторов, определяющих состояние и тенденции развития предприятия (например, в статье [20]). Графическое представление результатов оценки основано на использовании лепестковых диаграмм в полярной системе координат. Для этого строится многоугольник или окружность, разделенные на секторы в зависимости от выбранного количества индикаторов, затем сравниваются площади фигур в нормальном, кризисном (пороговом) и фактическом состоянии, возможно также сравнение в динамике или межхозяйственное сравнение.

Вторая группа методик использует интегральный показатель для оценки уровня экономической безопасности предприятия, вычисление которого осуществляется с помощью разнообразных алгоритмов.

Интегральные оценки уровня экономической безопасности предприятия определяются, как правило, одним из трех основных способов:

1) использованием аддитивных моделей или путем расчета средневзвешенной суммы компонентов [20, 27, 29, 32, 44, 45, 50];

2) построением стохастических регрессионных моделей [54];

3) применением мультипликативных моделей или расчетом средней геометрической величины совокупных оценок по отдельным составляющим [26, 68].

При использовании первого способа уровень экономической безопасности предприятия определяется как простая или взвешенная сумма величины оценок критериев по разным составляющим с учетом весовых коэффициентов, характеризующих значимость каждой детерминанты. Однако определение весовых коэффициентов экспертным методом делает оценку субъективной. При этом в ситуации, когда некоторые индикаторы безопасности выходят за свои предельные границы, а другие остаются в рамках допустимых значений, теряется важная информация, позволяющая выработать действенные меры реагирования.

Второй, менее распространенный способ определения интегрального показателя связан с использованием математических методов, в том числе стохастического моделирования (интегральный показатель экономической безопасности представляет собой аналитическое выражение стохастической зависимости между исследуемыми индикаторами) либо многомерных функций. В ходе корреляционно-регрессионного анализа определяются уравнения регрессии, отражающие зависимость между интегральным показателем и отдельными факторами.

В случае использования третьего способа величина интегрального показателя рассчитывается как произведение отдельных составляющих (детерминант микроуровня в системе экономической безопасности) или как средняя геометрическая стандартизированных значений показателя для каждой характеристики.

В целях обеспечения экономической безопасности хотя и не снимается задача рационального использования ресурсов, исключительно важной становится выработка стратегии долгосрочного выживания, обеспечивающей адаптацию предприятия к изменчивой и не всегда дружелюбной рыночной среде.

Выбор показателей для измерения экономической безопасности определяется отраслевой спецификой, размером предприятия, формой собственности, структурой активов и условиями функционирования рынка. Исходя из субъективного толкования сущности понятия экономической безопасности предприятия, исследователи предлагают различные методические подходы к оценке уровня его защищенности, при этом каждый из авторов опирается на свои методы и критерии.

Наиболее распространенной в научных источниках является следующая группировка подходов к оценке уровня экономической безопасности предприятия:

- 1) индикаторный подход;
- 2) ресурсно-функциональный подход;
- 3) подход, основанный на оценке экономических рисков;
- 4) комплексный подход.

Индикаторный подход предполагает оценку экономической безопасности предприятия на основе сравнения фактических результатов финансово-хозяйственной деятельности предприятия с индикаторами, для которых установлены пороговые значения (табл. 10).

При этом совокупность показателей (индикаторов), определяющих экономическую безопасность, подразделяется на разные группы. Выбор индикаторов оценки уровня экономической безопасности предприятия и способа их группировки зависит от отраслевой специфики, значимости угроз и субъективных предпочтений авторов. Разные авторы при выборе индикаторов оценки уровня экономической безопасности предприятия и

способа их группировки делают упор на разные аспекты обеспечения экономической безопасности.

Таблица 10

Методики, использующие индикаторный подход  
к оценке экономической безопасности предприятия

Авторы методики	Способ группировки индикаторов	Подход к определению интегрального показателя	Специфические особенности
М.А. Бендиков [20]	1. Индикаторы производства. 2. Финансовые. 3. Социальные	Графическое представление интегральных показателей	Характеристики состояния экономической безопасности: а) нормальное; б) предкризисное; в) кризисное; г) критическое
О.В. Говорина [27]	1. Характеристика производственной активности. 2. Характеристика финансового состояния. 3. Характеристика социального развития. 4. Характеристика рыночных показателей	Интегральная оценка экономической безопасности рассчитывается как средняя арифметическая взвешенная, весовые коэффициенты определяются экспертным путем	Показатели измеряются в баллах от 1 до 10 на основе экспертных оценок
О.Н. Овечкина [45]	Показатели: 1) ликвидности; 2) финансовой устойчивости; 3) деловой активности; 4) эффективности деятельности	Интегральный показатель рассчитывается как сумма отклонений фактических величин показателей-индикаторов от их пороговых значений	Оценка производится на основе финансовых индикаторов в аспекте финансовой безопасности предприятия

Нужно отметить, что в настоящий момент отсутствует надежная методическая база определения индикаторов, учитывающих специфику деятельности конкретного предприятия (размер, отраслевые особенности, форму собственности, материально-техническую оснащенность, структуру капитала).

Сравнительный анализ методик мониторинга и оценки экономической безопасности предприятия в рамках ресурсно-функционального подхода приведен в табл. 11.

Таблица 11

**Методики, в которых индикаторы сгруппированы  
в соответствии с ресурсно-функциональным подходом  
к оценке экономической безопасности предприятия**

Авторы методики	Функциональные составляющие	Подход к определению интегрального показателя	Специфические особенности
В.В. Григорьева, В.В. Шумейко [29]	<ol style="list-style-type: none"> <li>1. Финансовая.</li> <li>2. Основные средства.</li> <li>3. Оборотные средства.</li> <li>4. Кадровый потенциал.</li> </ol>	Интегральный показатель определяется как сумма рейтинговых оценок показателей и может принимать значения от 20 до 100	<p>Состояние экономической безопасности:</p> <ol style="list-style-type: none"> <li>1) абсолютное;</li> <li>2) нормальное;</li> <li>3) неустойчивое;</li> <li>4) предкритическое;</li> <li>5) критическое</li> </ol>
И.Н. Ермакова, Н.Б. Михеева, Д.С. Хандогина [32]	<ol style="list-style-type: none"> <li>1. Финансовая.</li> <li>2. Производственно-сбытовая.</li> <li>3. Техничко-технологическая.</li> <li>4. Кадровая</li> </ol>	Сводный интегральный коэффициент экономической безопасности предприятия выступает как среднее арифметическое по всем составляющим	По каждой составляющей вычисляется итоговая средневзвешенная оценка, в качестве весов выступают корректирующие коэффициенты
А.И. Примакин, Л.В. Большакова [54]	<ol style="list-style-type: none"> <li>1. Техничко-технологическая.</li> <li>2. Финансовая.</li> <li>3. Ресурсная.</li> <li>4. Интеллектуально-кадровая.</li> <li>5. Информационная.</li> <li>6. Социальная.</li> <li>7. Политико-правовая.</li> <li>8. Экологическая.</li> <li>9. Силовая</li> </ol>	На основании значений факторов строится уравнение множественной линейной регрессии, в котором линейные коэффициенты регрессии представляют собой оценку каждого фактора. Интегральные оценки рассчитываются как средневзвешенные арифметические	Факторы оцениваются по 5-балльной шкале от 0 до 5. Выбор факторов и весового коэффициента для каждого фактора производится с помощью экспертных оценок. Весовые коэффициенты для каждой из составляющих представляют собой неотрицательные числа, сумма которых равна единице
Н.Н. Яркина, А.Н. Вершинина [71]	<ol style="list-style-type: none"> <li>1. Финансовая.</li> <li>2. Техничко-технологическая.</li> <li>3. Кадровая и интеллектуальная.</li> <li>4. Конкурентоспособность (оценивается графическим методом)</li> </ol>	Итоговый интегральный показатель не определяется	Выбор индикаторов для оценки и пороговых значений связан с учетом специфики металлургического предприятия

В зависимости от целей исследования и научных интересов в отдельных методиках делается упор на разные аспекты обеспечения

экономической безопасности, виды ресурсов и функциональные составляющие.

Разделение между индикаторным и ресурсно-функциональным подходами достаточно условно. По своей сути ресурсно-функциональный подход является одним из способов группировки показателей при использовании индикаторного подхода. Разница между ними заключается в способе группировки индикаторов. Если для группировки индикаторов применяются виды корпоративных ресурсов (материальные и нематериальные ресурсы, оборотный капитал, трудовые ресурсы и т.д.) или функциональные составляющие экономической безопасности, то подход можно отнести к ресурсно-функциональному.

Ресурсно-функциональный подход охватывает различные функциональные области деятельности предприятия и основывается на предположении, что наиболее эффективное использование корпоративных ресурсов позволяет предотвратить опасности за счет укрепления внутреннего потенциала и создания условий для устойчивого развития. Критерием оценки здесь выступает уровень эффективности использования ресурсов по всем функциональным составляющим экономической безопасности (финансовой, технико-технологической, интеллектуальной, кадровой, нормативно-правовой, экологической, информационной, силовой и т.д.), то есть рациональное использование ресурсов рассматривается как основа для предотвращения угроз экономической безопасности. Оценка уровня экономической безопасности представляется в виде системы функциональных составляющих, каждая из функциональных групп сама по себе также является системой показателей.

Подход на основе оценки экономических рисков (табл. 12) предполагает идентификацию и анализ внешних и внутренних факторов, угрожающих безопасности предприятия, на основе методов количественной и качественной оценки конкретных рисков. В результате для различных угроз и негативных факторов рассчитывается вероятный ущерб, который сравнивается с величиной прибыли, дохода или имущества. В некоторых методиках в качестве критерия экономической безопасности может рассматриваться прибыль, а уровень безопасности оценивается в соответствии с возможностями предприятия нейтрализовать выявленные риски.

Комплексный подход (табл. 13) включает в себя как элементы индикаторного, ресурсно-функционального, рискованного подходов, так и применение различных математико-статистических методов. Методики, предлагаемые авторами в рамках комплексного подхода, оценивают не только внутренний потенциал предприятия, но и факторы внешней среды, отраслевые, региональные, экзогенные и эндогенные риски.

Таблица 12

Методики, оценивающие экономическую безопасность предприятия  
на основе теории экономических рисков

Авторы методики	Источники риска как детерминанты экономической безопасности	Подход к определению интегрального показателя	Специфические особенности
Л.А. Запорожцева, А.В. Агибалов [33]	1. Персонал и уровень управления. 2. Уровень финансовой безопасности, инвестиционные и кредитные риски. 3. Благонадежность контрагентов и деловая репутация	Количественного интегрального показателя нет. Оценивается уровень каждой составляющей по бинарной шкале (высокий – низкий) и дается характеристика типа экономической безопасности в целом	Определяется степень риска по каждой детерминанте и тип стратегической экономической безопасности (высокий, средний или низкий)
В.В. Масленников, А.А. Трохов [42]	Угрозы экономической безопасности определяются с учетом специфики сферы деятельности и значимости риска в соответствии с вероятностью наступления ущерба и его величиной	Интегральный показатель экономической безопасности не вычисляется	Предлагают использовать методы идентификации и управления рисками и строить карту рисков для диагностики угроз экономической безопасности компании
К.В. Мокроусова [44]	1. Финансовое состояние. 2. Рыночное положение. 3. Корпоративное управление. 4. Финансовые результаты деятельности	Интегральный показатель инвестиционной привлекательности определяется по формуле арифметической средневзвешенной. Весовые коэффициенты представляют параметры регрессионной модели и рассматриваются как критерии риска	Проводится сравнительный анализ экономической безопасности ряда предприятий в аспекте их инвестиционной привлекательности
А.В. Шохнех [68]	1. Зависимость предприятия от заемных средств. 2. Структура источников средств	Интегральная оценка рассчитывается с помощью мультипликативной двухфакторной модели	Экспресс-оценка финансовой безопасности. Метод недостаточен для полноценной диагностики угроз экономической безопасности

Таблица 13

Методики комплексного подхода  
к оценке экономической безопасности предприятия

Авторы	Составляющие	Подход к определению	Специфические
--------	--------------	----------------------	---------------

методики	экономической безопасности	лению интегрального показателя	особенности
М.М. Гайфуллина, Е.В. Костомарова [25]	1. Микроуровень. 2. Макроуровень	Комплексный показатель экономической безопасности и детерминанты микроуровня и макроуровней определяются как среднее арифметическое	Выделяются следующие состояния экономической безопасности: а) стабильное; б) предкризисное; в) кризисное; г) критическое. Методика рассчитана на оценку уровня экономической безопасности нефтяной компании
М.Т. Гильфанов [26]	1. Микроуровень. 2. Мезоуровень. 3. Макроуровень	Интегральный показатель экономической безопасности предприятия представлен как произведение усредненных характеристик имеющихся ресурсов на корректирующие коэффициенты, полученные с помощью экспертной оценки на мезо- и макроуровне	На микроуровне используется система индикаторов, а на макро- и мезоуровне – экспертная оценка. На мезо- и макроуровне оцениваются риски в соответствии с рисковым подходом. В зависимости от силы и характера воздействия предложены различные значения корректирующих коэффициентов на мезо- и макроуровне
И.М. Подмолодина, В.П. Воронин, Е.М. Коновалова [50]	1. Оценка эффективности деятельности и использования ресурсов. 2. Оценка пропорциональности экономического роста (устойчивости развития)	Итоговый интегральный показатель экономической безопасности предприятия рассчитывается по формуле арифметической средневзвешенной	Оценка эффективности производственно-хозяйственной деятельности производится с помощью матрицы, включающей темпы роста прибыли, выручки, издержек и объема используемых ресурсов. Отдельно оценивается уровень финансовой устойчивости предприятия и финансовых рисков

В условиях отсутствия стандартных правил проведения оценки экономической безопасности предприятия существующие методики оценки экономической безопасности на микроуровне имеют свои преимущества и недостатки (табл. 14).

*Таблица 14*

Преимущества и недостатки существующих подходов к оценке уровня экономической безопасности предприятия

Подходы	Преимущества	Недостатки
---------	--------------	------------



к оценке экономической безопасности предприятия		
Индикаторный	Простота использования (как правило, не возникают сложности в расчетах и обосновании выводов)	Концентрация на отдельных факторах экономической безопасности; отсутствие четкого научного обоснования объективности включения тех или иных индикаторов; субъективность в определении пороговых значений экономической безопасности предприятия
Ресурсно-функциональный	Возможность учета отраслевой специфики или каждой функциональной составляющей	Отсутствие определенности с набором функциональных составляющих экономической безопасности предприятия; недостаточность оценки экономических рисков; ориентация, как правило, на ретроспективные показатели, в результате чего сложно прогнозировать состояния системы в будущем
На основе оценки рисков	Оценка конкретных рисков, угрожающих экономической безопасности предприятия	Наличие трудностей формализованного описания динамических свойств предприятия с точки зрения достижения и поддержания состояния безопасности во взаимосвязи с действиями дестабилизирующих факторов; отсутствие оценки имеющегося потенциала для развития
Комплексный	Обоснованность выводов об общем уровне экономической безопасности предприятия с учетом разных аспектов деятельности предприятия	Сложности с обоснованием способа расчета интегрального показателя; трудности при определении граничных значений индикаторов экономической безопасности хозяйствующего субъекта; субъективность выводов вследствие использования экспертных оценок; сложность в получении информации для расчета выбранных качественных показателей оценки

От качества идентификации угроз и рисков, правильного выбора критериев и методов измерения, а также от наличия достаточного потенциала, позволяющего противостоять угрозам или нивелировать их, зависят степень адекватности оценки экономической безопасности предприятия и комплекс необходимых мер по предупреждению опасностей, соответствующих масштабу и характеру угроз.

Выбор метода оценки экономической безопасности в каждом конкретном случае осуществляется с учетом цели и задач оценки,

специфики деятельности предприятия, наличия необходимой информации и других объективных факторов. Перечень показателей экономической безопасности определяется каждым предприятием самостоятельно в зависимости от его специфики, применяемых подходов к управлению, роли в отрасли. Эффективность определения параметров пороговых значений индикаторов напрямую зависит от достоверности и качества используемой информации.

Стоит отметить, что практически отсутствует четкое обоснование того, что методы оценки уровня экономической безопасности имеют преимущества по сравнению с апробированными, общепризнанными методами финансово-экономического анализа деятельности предприятия. По нашему мнению, применение описанных методов позволяет выявить исходные причины, негативно влияющие на обеспечение экономической безопасности. При этом несовершенство существующей методологии оценки рисков и угроз экономической безопасности проявляется в сложности одновременной оценки, сопоставления и взаимосвязи внутренних и внешних рисков, высоком уровне неопределенности, который значительно усложняет прогнозирование на основе ретроспективных данных, высокой субъективности рейтинговой экспертной оценки, отсутствии четкого представления о формате и единицах измерения конечных результатов диагностики экономической безопасности компании.

На основании критического анализа существующих методик диагностики состояния экономической безопасности компании можно выделить следующие основные проблемы методологического характера в области диагностики экономической безопасности предприятия:

- высокий уровень неопределенности, снижающий достоверность оценок, основанных на ретроспективных данных;

- субъективность и противоречивость экспертных оценок;

- трудности учета качественных факторов, связанных с уровнем профессионализма высшего менеджмента, структурой собственности, степенью добросовестности поведения на рынке, соблюдением законодательства и прозрачности финансовых потоков и т.д.;

- сложности учета рисков во взаимоотношениях с контрагентами, деловыми партнерами, клиентами и покупателями;

- необходимость оценки деловой репутации, периода деятельности компании, стадии жизненного цикла и истории ее развития;

- противоречивость статистических данных, представленных на сайтах Росстата, налоговой службы, Банка России и различных ведомств.

Для оценки экономической безопасности часто применяют методологию стратегического анализа. Стратегическое планирование – часть общей системы управления экономической безопасностью предприятия, одна из его функциональных подсистем, способствующая

реализации управленческих решений в долгосрочной перспективе. Разработка стратегии обеспечения экономической безопасности предприятия связана с формированием стратегических целей, обеспечивающих рост и защиту экономических интересов организации от различных угроз путем формирования долгосрочных направлений развития.

В условиях конкуренции, изменчивости условий внешней среды необходимы как постоянная корректировка рыночной стратегии, так и значительные усилия по формированию эффективной стратегии экономической безопасности. В нестабильной рыночной среде предприятия (независимо от сферы деятельности) сталкиваются с необходимостью поиска принципиально новых подходов к обеспечению собственной экономической безопасности. При этом исключительно важна выработка стратегии долгосрочного развития, обеспечивающей адаптацию фирмы к рыночной среде. Однако на практике редко наблюдается полная или хотя бы частичная реализация данного механизма управления компанией, что связано с конфликтом интересов различных социальных, экономических и административных субъектов.

Стратегии управления экономической безопасностью предприятия (в зависимости от имеющихся возможностей и ресурсов) могут быть направлены на реализацию планов роста или развития при условии компенсации или нивелирования деструктивных влияний и угроз либо адаптацию и приспособление к угрозам с целью сохранения устойчивости предприятия. Помимо имеющегося внутреннего потенциала, возможностей и ресурсов предприятия, при выборе стратегии экономической безопасности большое значение имеют условия внешней деловой среды, сложившиеся формы взаимодействия хозяйствующих субъектов, степень их кооперации и формы интеграции.

Так, Л.М. Ширко [67, с. 3290], опираясь на сбалансированную систему показателей Р. Каплана, Д. Нортон, проводит оценку экономической безопасности с позиции разработки стратегии развития предприятия. С учетом вышесказанного система показателей экономической безопасности может быть представлена блоками показателей (табл. 15).

**Формирование сбалансированной системы показателей  
экономической безопасности**

Проекция (блок показателей)	Содержание	Возможные целевые установки
«Финансы»	Финансовое состояние предприятия, его финансовая устойчивость и платежеспособность	Обеспечение финансовой устойчивости предприятия. Повышение платежеспособности. Повышение доходности. Обеспечение сохранности денежных средств
«Клиенты»	Конкурентоспособность и обеспечение безопасности предприятия с точки зрения рынка и клиентов	Обеспечение безопасности при работе с контрагентами. Расширение рынков сбыта. Увеличение доли предприятия на рынке и повышение конкурентоспособности
«Внутренние бизнес-процессы»	Внутренняя устойчивость и эффективность функционирования бизнес-процессов	Оптимизация и повышение эффективности бизнес-процессов. Обеспечение безопасности инвестиционной деятельности и воспроизводства основного капитала. Обеспечение сохранности имущества. Контроль за состоянием материально-производственных запасов. Защита интересов предприятия в судах общей юрисдикции. Защита интересов предприятия в рамках процедур контроля (надзора). Эффективность участия в системе государственных закупок
«Кадры»	Качество и квалификация кадрового состава, развитие человеческого капитала, психологический климат в коллективе, соблюдение трудовой дисциплины	Предупреждение правонарушений и недобросовестного поведения. Реализация эффективной кадровой политики. Развитие компетенций и мотивации персонала

Выбор стратегии развития предприятия обуславливается его интересами, ресурсами, условиями внешней среды, степенью ее воздействия на компанию, уровнем чувствительности фирмы к изменению условий среды, институциональными условиями, моделями взаимодействия с внешней средой, природно-географическими условиями и т.д.

При разработке стратегии экономической безопасности часто используют модифицированный инструментарий стратегического маркетинга (матрицу Ансоффа, матрицу БКГ, матрицу МакКинзи, матрицу General Electric и др.), а также SWOT-анализ для выбора стратегии развития компании в зависимости от состояния экономической безопасности предприятия.

Под стратегией обеспечения экономической безопасности Р.В. Белозерцев и В.Н. Белозерцев понимают «систему методов и инструментов реализации управленческих решений, которые позволяют обеспечить приемлемый уровень безопасности функционирования предприятия, высокий производственно-экономический потенциал и реализацию целей по устойчивому развитию в долгосрочной перспективе» [19, с. 6]. На основе результатов SWOT-анализа и количественной оценки степени влияния внешних и внутренних факторов авторы предлагают характеризовать состояние экономической безопасности и осуществлять выбор стратегии ее обеспечения в зависимости от интенсивности воздействия позитивных и негативных факторов.

Стандартное базовое представление позитивных и негативных факторов стратегического планирования, принятое при использовании SWOT-анализа, предполагает оценку влияния факторов внутренней и внешней среды в зависимости от их воздействия на достижение поставленных стратегических целей (рис. 6).

Источник	Влияние	
	Способствует достижению цели (+)	Препятствует достижению цели (-)
Внешняя среда	Strengths (S) Сильные стороны	Weaknesses (W) Слабые стороны
Внутренняя среда	Opportunities (O) Возможности	Threats (T) Угрозы

Рис. 6. Визуальное стандартное базовое представление факторов внешней и внутренней среды при использовании SWOT-анализа

На основе стандартной SWOT-матрицы Р.В. Белозерцев и В.Н. Белозерцев [19] предложили собственную классификацию состояний экономической безопасности предприятия (рис. 7). Они выделяют четыре состояния экономической безопасности в зависимости от степени влияния на результаты деятельности компании и источника угроз.

Внутренняя среда	Внешняя среда	
	Преимущественное влияние негативных факторов (-)	Преимущественное влияние позитивных факторов (+)
Преимущественное влияние позитивных факторов (+)	<b>А.</b> Низкий уровень экономической безопасности, обусловленный негативным воздействием факторов внешней среды	<b>В.</b> Высокий уровень экономической безопасности предприятия
Преимущественное влияние негативных факторов (-)	<b>С.</b> Критическое состояние экономической безопасности предприятия	<b>Д.</b> Низкий уровень экономической безопасности, обусловленный негативным воздействием факторов внутренней среды

Рис. 7. Классификация состояний экономической безопасности предприятия в зависимости от степени влияния внешней и внутренней среды (составлено авторами на основе статьи [19])

По нашему мнению, при наличии количественных данных мониторинга позитивных и негативных факторов данную классификацию состояний экономической безопасности можно использовать при выборе стратегии развития предприятия в конкурентной рыночной среде для выработки механизмов обеспечения экономической безопасности на микроуровне с учетом новых возможностей цифровой экономики.

Современные информационные системы расширяют поисковые возможности и функционал работы со списками юридических, индивидуальных предпринимателей или арбитражных дел, увеличивают информационное поле для мониторинга и оценки факторов и условий деловой среды, определяющих конкурентные позиции работающих на рынке компаний, позволяют рассчитать статистические характеристики выборки компаний в зависимости от разных условий и сравнить компании по различным параметрам: размеру, видам деятельности, финансовому положению и рисковому факторам. Таким образом, благодаря использованию новых информационных технологий и распределенных реестров обеспечивается сбор, обработка и хранение больших объемов данных, расширяются аналитические возможности мониторинга уровня экономической безопасности компании.

На рынке информационных услуг сегодня существует целый спектр информационных и аналитических систем, которые не только

предоставляют услуги по раскрытию финансовой информации, но и предлагают систематизированную информацию для принятия управленческих решений, направленных на снижение рисков и повышение экономической безопасности компании. Собирая воедино данные с сайтов налоговой службы, кредитного бюро, нотариальной палаты, Росреестра, Росстата, арбитражных судов и других информационных ресурсов, систематизируя их и приводя к удобному для восприятия пользователями формату, они превращают информацию в товар.

Современные системы раскрытия информации предоставляют возможности по оценке конкурентоспособности, внутреннего потенциала и внешнего риска компании за счет сравнения результатов хозяйственной и финансовой деятельности компании с аналогичными показателями других предприятий, сопоставимых по численности и обороту в рамках региона или отрасли (вида экономической деятельности).

На основании сформированной базы данных можно выполнить сравнительную оценку величины потенциала и уровня риска. Для сравнительного анализа уровня экономической безопасности компании можно использовать показатели относительных отклонений от эталонного или среднего значения по отрасли или региону. Расчет относительных отклонений позволяет сравнить показатели, представленные в разных единицах измерения. В данном случае эталонное значение можно принять за нулевую отметку. Лучшее значение по сравнению с ним будет представлять собой положительную оценку, а худшее – отрицательную.

Перечень количественных показателей, которые можно получить, используя информационные ресурсы раскрытия информации, достаточно обширен: от данных финансовой и бухгалтерской отчетности, размера оборота, численности персонала до сведений о размерах уплаченных налогов и штрафов, санкций, требований по искам, взаимоотношений с дебиторами и кредиторами и т.д.

На основе выборки данных из информационных систем раскрытия информации можно также оценить как условия внешней среды, так и потенциал развития предприятия.

Если исходить из предлагаемого нами концептуального подхода к определению сущности безопасности экономической системы, то ключевым условием обеспечения экономической безопасности предприятия является наличие комплексного внутреннего потенциала, превосходящего совокупное влияние внешних негативных факторов и достаточного для того, чтобы минимизировать риск и использовать ресурсы для адаптации к негативным воздействиям деловой среды.

Представляется, что предложенный в статье [15] методологический подход, основанный на использовании ABC-матрицы, можно применять для выявления угроз безопасности развития предприятия и выработки управляющих воздействий, направленных на укрепление его потенциала. В этом случае следует не только производить оценку рисков, опасностей и угроз (обозначим риски в каждой клетке матрицы как **Risk** [Источник, Фактор]), но и анализировать преимущества и возможности для развития, предоставляемые имеющимся потенциалом (для последнего будем использовать обозначение **Pot** [Источник, Фактор]). Тогда матрица принимает вид, показанный на рис. 8.

<b>Факторы</b> <b>Factors</b>					
<b>Ис-</b> <b>точ-</b> <b>ники</b> <b>угроз</b> <b>Sources</b> <b>of Threats</b>	<b>Управление</b> <b>Menegment</b> <b>(Meng)</b>	<b>Финансы</b> <b>Finance</b> <b>(Fin)</b>	<b>Трудовые</b> <b>ресурсы</b> <b>Labor</b> <b>(Lab)</b>	<b>Материально-</b> <b>техническая</b> <b>база</b> <b>Technique</b> <b>(Tech)</b>	<b>Итого</b> <b>по источ-</b> <b>никам</b> <b>угроз</b>
<b>Региональная</b> <b>деловая среда</b> <b>(External</b> <b>Business</b> <b>Environment)</b>	<b>Risk</b> <sub>[Ext, Meng]</sub> <b>Pot</b> <sub>[Ext, Meng]</sub>	<b>Risk</b> <sub>[Ext, Fin]</sub> <b>Pot</b> <sub>[Ext, Fin]</sub>	<b>Risk</b> <sub>[Ext, Lab]</sub> <b>Pot</b> <sub>[Ext, Lab]</sub>	<b>Risk</b> <sub>[Ext, Tech]</sub> <b>Pot</b> <sub>[Ext, Tech]</sub>	<b>Risk</b> <sub><math>\Sigma</math>Ext</sub> <b>Pot</b> <sub><math>\Sigma</math>Ext</sub>
<b>Рынок</b> <b>(Market)</b>	<b>Risk</b> <sub>[Markt, Meng]</sub> <b>Pot</b> <sub>[Markt, Meng]</sub>	<b>Risk</b> <sub>[Markt, Fin]</sub> <b>Pot</b> <sub>[Markt, Fin]</sub>	<b>Risk</b> <sub>[Markt, Lab]</sub> <b>Pot</b> <sub>[Markt, Lab]</sub>	<b>Risk</b> <sub>[Markt, Tech]</sub> <b>Pot</b> <sub>[Markt, Tech]</sub>	<b>Risk</b> <sub><math>\Sigma</math>Markt</sub> <b>Pot</b> <sub><math>\Sigma</math>Markt</sub>
<b>Внутренняя</b> <b>среда пред-</b> <b>приятия</b> <b>(Internal</b> <b>Business</b> <b>Environment)</b>	<b>Risk</b> <sub>[Int, Meng]</sub> <b>Pot</b> <sub>[Int, Meng]</sub>	<b>Risk</b> <sub>[Int, Fin]</sub> <b>Pot</b> <sub>[Int, Fin]</sub>	<b>Risk</b> <sub>[Int, Lab]</sub> <b>Pot</b> <sub>[Int, Lab]</sub>	<b>Risk</b> <sub>[Int, Tech]</sub> <b>Pot</b> <sub>[Int, Tech]</sub>	<b>Risk</b> <sub><math>\Sigma</math>Int</sub> <b>Pot</b> <sub><math>\Sigma</math>Int</sub>
<b>Итого по</b> <b>группам</b> <b>факторов</b>	<b>Risk</b> <sub><math>\Sigma</math> Meng</sub> <b>Pot</b> <sub><math>\Sigma</math> Meng</sub>	<b>Risk</b> <sub><math>\Sigma</math>Fin</sub> <b>Pot</b> <sub><math>\Sigma</math>Fin</sub>	<b>Risk</b> <sub><math>\Sigma</math>Lab</sub> <b>Pot</b> <sub><math>\Sigma</math>Lab</sub>	<b>Risk</b> <sub><math>\Sigma</math>Tech</sub> <b>Pot</b> <sub><math>\Sigma</math>Tech</sub>	<b>Risk</b> <sub><math>\Sigma</math></sub> <b>Pot</b> <sub><math>\Sigma</math></sub>

Рис. 8. Факторы безопасного развития предприятия:  
матрица оценки возможностей и угроз [24]



При условии приведения итоговых оценок величины потенциала и риска в каждой клетке матрицы к единой системе оценок, например в координатах от  $-1$  до  $1$ , можно сравнить величину потенциала и риска. В качестве порогового значения, соответствующего нулевой координате, можно использовать усредненное значение показателя по предприятиям того же вида деятельности (отраслевой разрез) или с учетом тенденций развития самого предприятия (динамический разрез).

Если величина потенциала превосходит величину риска:

$$(\mathbf{Pot}_{[\text{Источник, Фактор}]} > \mathbf{Risk}_{[\text{Источник, Фактор}]})$$

то данный фактор на соответствующем уровне деловой среды будет являться возможностью для развития.

Напротив, в случае, когда величина потенциала меньше, чем уровень риска:

$$\mathbf{Pot}_{[\text{Источник, Фактор}]} < \mathbf{Risk}_{[\text{Источник, Фактор}]})$$

возникает угроза для развития хозяйствующего субъекта.

Подобное представление возможностей и угроз не только позволяет количественно оценить их, но и дает направления для выработки комплекса адресных управляющих решений, нацеленных на повышение потенциала развития и устранение или нейтрализацию угроз и рисков.

Применяя метод многокритериального сравнительного анализа потенциала развития и угроз внешней среды, основанный на использовании данных информационных систем раскрытия информации, можно привести оценки потенциала развития и рисков внешней среды к единой размерности. Это дает возможность сопоставить их и построить координатную плоскость в прямоугольной декартовой системе координат, где горизонтальная ось будет представлять собой оценки уровня внешних рисков, а вертикальная – имеющегося внутреннего потенциала.

По нашему мнению, экономическая безопасность хозяйствующего субъекта обеспечивается только при условии соответствия внутренних характеристик его потенциала и ресурсов особенностям внешнего окружения и специфике взаимодействия в пространственной деловой среде. Только в этом случае предприятие сможет противостоять внутренним угрозам и использовать имеющиеся ресурсы для адаптации к внешним рискам, обеспечивая достаточную степень устойчивости и сбалансированности финансовых потоков, чтобы предотвратить риск ущерба, связанного с утратой рыночных позиций и кадрового, имущественного или иного потенциала. В связи с этим в процессе оценки экономической безопасности необходимо наряду с наличием, достаточностью и эффективностью использования внутреннего потенциала учитывать специфику внешней среды, степень зависимости от внешних факторов, надежность взаимоотношений с деловыми партнерами,

клиентами и покупателями, а также риски в рамках взаимоотношений с контрагентами.

Таким образом, уровень экономической безопасности предприятия оценивается во взаимосвязи текущего и прогнозируемого состояния его потенциала и факторов риска деловой среды: в случае существенного превышения совокупного влияния рисков над потенциалом возникают угрозы, которые могут препятствовать функционированию и развитию предприятия.

Учитывая потребности теории и практики в создании приемлемой для научного анализа и бизнес-сообществ концепции оценки экономической безопасности на микроуровне, мы предложили новый метод диагностики угроз развитию предприятия, который позволяет оценивать не только внутренний потенциал и риски компании, но и условия деловой среды, а также степень ее безопасности для предпринимательской деятельности. Данный способ оценки позволяет выявить как возможности, так и угрозы, которые возникают не только на микроуровне, но и в рамках деловой среды на мезоуровне. В этой связи предложенный метод может служить методологической основой для разработки конкретных мер по обеспечению экономической безопасности бизнеса. Полученные результаты открывают возможности их широкого практического применения и могут быть использованы при формировании направлений и выработке конкретных мер по защите от вероятных угроз и снижению рисков.

Таким образом, с одной стороны, современные информационные технологии обеспечивают информационно-эмпирическую базу исследования, а с другой – использование современных информационных технологий и методик работы с базами данных, а также программных средств обработки экономической информации позволяет реализовать на практике предложенную методику и повысить достоверность полученных результатов. Решение задач в этой сфере должно происходить путем объединения усилий всех ветвей власти, бизнеса и общественности. В то же время развитие цифровой экономики в нашей стране требует осознанного внедрения цифровизации бизнес-процессов отечественными предприятиями, что требует дополнительных научных исследований. Более подробно данный вопрос будет рассмотрен в следующем разделе.

## **РАЗДЕЛ 3. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВА И ЕЕ ВЛИЯНИЕ НА БИЗНЕС**

### **3.1. Контрольно-надзорная деятельность государства в условиях цифровой трансформации**

В условиях цифровизации значительно возросли эффективность государственной надзорной и регуляторной деятельности, собираемость налогов и возможности выявления признаков недобросовестного поведения. Использование специализированных информационных систем и систем ИИ позволяет отслеживать финансовые и товарные потоки, пресекать уклонение от уплаты налогов и попытки мошенничества [30, 110].

Современные информационные технологии приводят к существенной трансформации модели взаимодействия государства с бизнесом и населением, предоставляют новые возможности ситуационного управления, основанного на обеспечении многоуровневого полнофункционального управления проектами с использованием ИИ, но в то же время порождают новые проблемы, риски и угрозы.

С ростом прозрачности финансовых потоков и упрощением контроля над ними требуется усиление защиты персональных данных и сведений, имеющих коммерческую ценность, что увеличивает издержки, направленные на предупреждение утечки информации [59]. Кроме того, как отмечает А.А. Пороховский [53, с. 60], цифровая трансформация усиливает взаимозависимость всех экономических субъектов на разных уровнях управления и требует применения новых форм защиты информации для обеспечения информационной безопасности государства.

Значительное послабление режима налоговой тайны, происшедшее в последнее время, привело к существенному расширению спектра информации о финансово-хозяйственной деятельности компаний, не защищенных режимом. Сюда теперь относятся не только общедоступные сведения об организации (в том числе содержащиеся в ЕГРЮЛ: дата создания, адрес и ИНН, Ф.И.О. руководителя и пр.), но и сведения о налоговых нарушениях и мерах ответственности за них и т.д.

Перечень общедоступных сведений о компании существенно расширился за счет информации о размерах недоимки и задолженности с раскрытием конкретных сумм; о среднесписочной численности работников; об уплаченных страховых взносах и налогах (по каждому налогу и сбору); о суммах доходов и расходов по данным бухгалтерской (финансовой) отчетности и прочих сведений. Все эти данные сегодня публикуются в интернете без согласия участников рынка и размещены на

сайте Федеральной налоговой службы. Порядок и сроки размещения данных утверждает сама налоговая служба.

До 2019 года набор общедоступных данных был значительно меньше, причем он касался только некоторых категорий юридических лиц, которые обязаны были публиковать бухгалтерскую отчетность, а также юридических лиц, готовых разместить ее на добровольной основе. При этом стоит отметить, что до 2019 года полученная органами статистики бухгалтерская отчетность организации, даже не подлежащая обязательному опубликованию, фактически тоже находилась в открытом доступе и могла быть предоставлена по дополнительному запросу любому желающему.

Сегодня на первый план выдвигаются проблемы государственного регулирования, в том числе в экономической сфере. Ключевыми регуляторами становятся федеральные контрольно-надзорные органы, в задачу которых входит, с одной стороны, защита интересов государства и общества в целом, а с другой – реализация национальных приоритетов, напрямую связанных с устойчивым развитием экономики. В то же время должностным лицам и органам государственной власти важно руководствоваться как соображениями экономической целесообразности, так и требованием безопасности людей и чувством социальной ответственности. В этой связи отчетливо проявляются новые требования к государственным регуляторам и надзорным органам.

В рамках внедрения новой парадигмы взаимодействия государства с бизнесом существенно меняются условия деловой среды. Контрольно-надзорные органы выступают в качестве регуляторов бизнес-процессов, активно используя современные информационные бесконтактные технологии, роботизацию и новые принципы комплаенса при взаимодействии с поднадзорными субъектами. С государственной точки зрения новые технологии повышают эффективность надзорной и регуляторной деятельности, позволяют в режиме реального времени осуществлять мониторинг транзакций и выявлять признаки недобросовестного поведения и мошенничества, но, в восприятии бизнеса, внедрение новых форм взаимодействия связано с дополнительными затратами и необходимостью повышения уровня квалификации наемных работников.

Функции контроля и надзора, осуществляемые государством, остаются одной из самых болевых точек соприкосновения интересов государства и бизнеса. С одной стороны, происходят реформирование государственного контроля в целях снижения административной нагрузки на бизнес и процесс реализации ряда законодательных инициатив Президента и Правительства Российской Федерации. С другой стороны, представители бизнеса отмечают усиление контрольно-надзорных функций государства.

Следует отметить, что модификация обязательных требований в рамках системы государственного контроля и реализации механизма «регуляторной гильотины» завершилась принятием Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» от 31 июля 2020 года № 248-ФЗ, который вступил в силу в 2021 году.

Внедрение любых законодательных преобразований влечет за собой риски, связанные с их применением и толкованием в конкретных ситуациях на практике. В рамках применения новых механизмов регулирования в условиях сложной геополитической ситуации, санкционного давления, нестабильной эпидемиологической обстановки формируется принципиально иная практика взаимоотношений контрольных органов, населения и бизнес-сообщества, что приводит к необходимости непрерывного мониторинга и корректировки данного процесса на начальном этапе применения новых законодательных норм.

Реализация требований федерального закона № 248-ФЗ направлена на достижение общественно значимых результатов, связанных с минимизацией риска причинения вреда (ущерба) охраняемым законом ценностям, а также должна способствовать улучшению инвестиционного климата и условий ведения бизнеса в Российской Федерации.

Серьезные изменения порядка осуществления государственного контроля (надзора) в Российской Федерации обуславливают необходимость комплексной оценки позиций бизнеса. Кроме того, актуальность и значимость исследования возрастают в связи с изменениями в практике контрольно-надзорной деятельности из-за пандемии COVID-19, в том числе в контексте широкого применения дистанционных форм проверок и ускорения процессов цифровизации контрольно-надзорной и разрешительной деятельности.

Несмотря на усилия государственных структур, направленные на формирование благоприятных условий для функционирования и развития бизнеса, введение процедур оценки регулирующего воздействия на бизнес, разработку законодательных и нормативных актов, связанных с применением так называемой «регуляторной гильотины», предприниматели и инвесторы указывают на проблемы с внедрением новых механизмов государственного контроля (надзора) и риск-ориентированного подхода.

По инициативе Уполномоченного по защите прав предпринимателей в Тверской области А.В. Стамплевского на протяжении последних лет (с 2016 по 2022 годы) проводятся социологические исследования, посвященные анализу влияния государственного и муниципального контроля (надзора) на бизнес на территории Тверской области и изменению административной нагрузки на бизнес в рамках проводимой реформы контрольно-надзорной деятельности государства. Реформа

контрольно-надзорной деятельности направлена на снижение уровня административной нагрузки на бизнес.

Итоги опроса, оценивающего административную нагрузку на бизнес в 2022 году, сопоставляются с аналогичными исследованиями, которые проводились в 2017–2019 годах и (по отдельным вопросам) в 2016 году.

В исследованиях ежегодно принимали участие свыше 300 респондентов, среди которых были представители малого, среднего и крупного бизнеса Тверской области, в том числе хозяйствующие субъекты различных видов экономической деятельности и организационно-правовых форм. Подавляющее большинство опрошенных относилось к субъектам малого и среднего бизнеса. Наибольшую часть респондентов составили предприятия, существующие на рынке более 5–10 лет (более половины от общего числа опрошенных); вновь созданные предприятия, существующие менее одного года, составили менее 10 %. Представляется, что богатый опыт ведения хозяйственной деятельности, которым обладает большинство респондентов, позволит им объективно оценить результаты реформирования контрольно-надзорных мероприятий (КНМ) и их влияние на работу предприятия.

Выявление мнения проходило путем анонимного анкетирования участников, при этом оговаривалось, что все данные будут использоваться только в обобщенном виде.

Распределение респондентов по видам экономической деятельности примерно соответствует отраслевой структуре малых и средних предприятий Тверской области, исходя из чего можно предположить, что полученные результаты отражают восприятие реформы контрольно-надзорной деятельности предпринимательским сообществом региона. Наиболее распространенными организационно-правовыми формами в бизнес-сообществе являются индивидуальные предприниматели и общества с ограниченной ответственностью.

Степень участия респондентов в КНМ в Тверской области в 2016–2022 г. представлена в табл. 16.

*Таблица 16*

Распределение респондентов по количеству КНМ  
в рассматриваемый период (в процентах к числу опрошенных)

Варианты ответа	Год				
	2016	2017	2018	2019	2022
КНМ не проводились	31,70	35,1	60,8	57,9	70,6
КНМ проводились	68,30	64,9	39,2	42,1	29,4
В том числе					
от 1 до 3		42,5	19,1	19,4	11,1
от 4 до 6		8,4	5,3	5,5	1,2
от 7 до 10		3,3	1,6	0,0	0,6
свыше 10		4,3	2,2	1,3	0,9
Не указали число проверок		6,4	11,0	15,9	15,7

Об отсутствии КНМ в 2022 году заявили 70,6 % респондентов. Динамика удельного веса участников опроса, проходивших проверки, свидетельствует о снижении интенсивности КНМ по отношению к одной компании на территории Тверской области за указанный период (рис. 9).

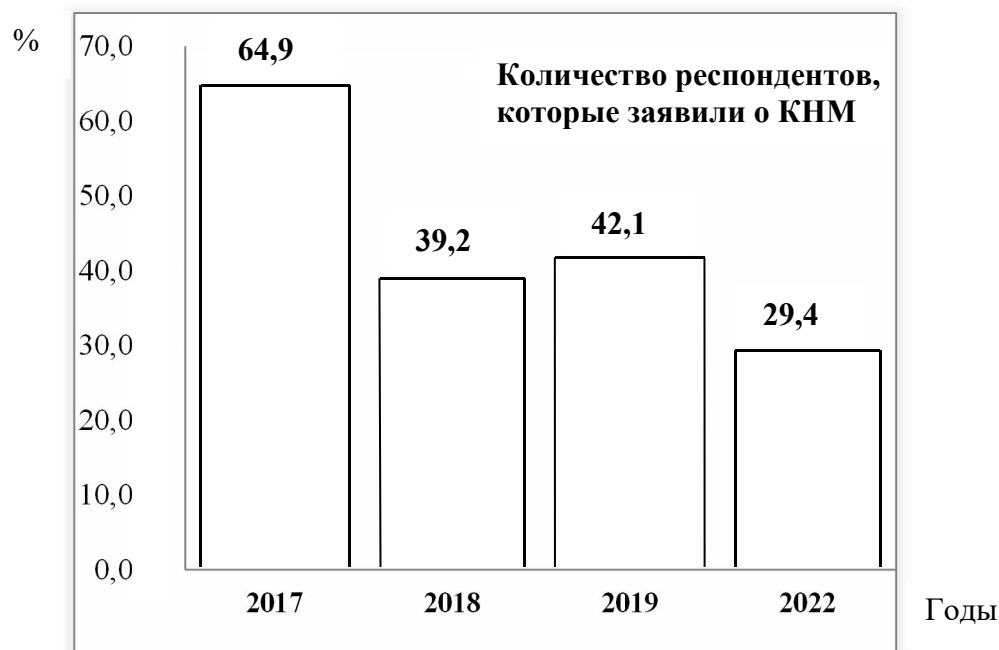


Рис. 9. Удельный вес респондентов, заявивших о проведении КНМ (в процентах от общего количества респондентов)

Ответы респондентов, в отношении компаний которых в 2022 году проводились мероприятия контрольно-надзорных органов, по их конкретным видам представлены в табл. 17. Почти треть респондентов (31,7 %) заявили о документарной проверке, примерно четверть (24,7 %) – об инспекционном визите. Выездная проверка проводилась в отношении 22,8 % опрошенных.

Таблица 17

Распределение ответов по видам КНМ в 2022 году (в процентах от количества респондентов, указавших на проведение КНМ)

№	Варианты ответа	Удельный вес
1	Документарная проверка	31,7
3	Инспекционный визит	24,8
2	Выездная проверка	22,8
4	Выборочный контроль	12,9
5	Рейдовый осмотр	12,9
6	Контрольная закупка	5,0
7	Мониторинговая закупка	4,0

Распределение КНМ в период с 2016 по 2022 год по уровню проводивших их контрольно-надзорных органов представлено в табл. 18.

Таблица 18

Распределение полученных ответов о количестве КНМ, проведенных контрольно-надзорными органами различного уровня (в процентах от общего числа КНМ)

Уровень	Год				
	2022	2019	2018	2017	2016
Федеральный	84,0	74,1	72,8	71,0	63,87
Региональный	5,3	14,3	17,5	19,8	24,52
Муниципальный	10,7	11,6	9,8	9,1	11,61

Как показано на рис. 10, в последние годы наблюдается тенденция к увеличению доли КНМ, проводимых федеральными органами, в общем числе КНМ и снижению удельного веса проверок, проводимых региональными органами.

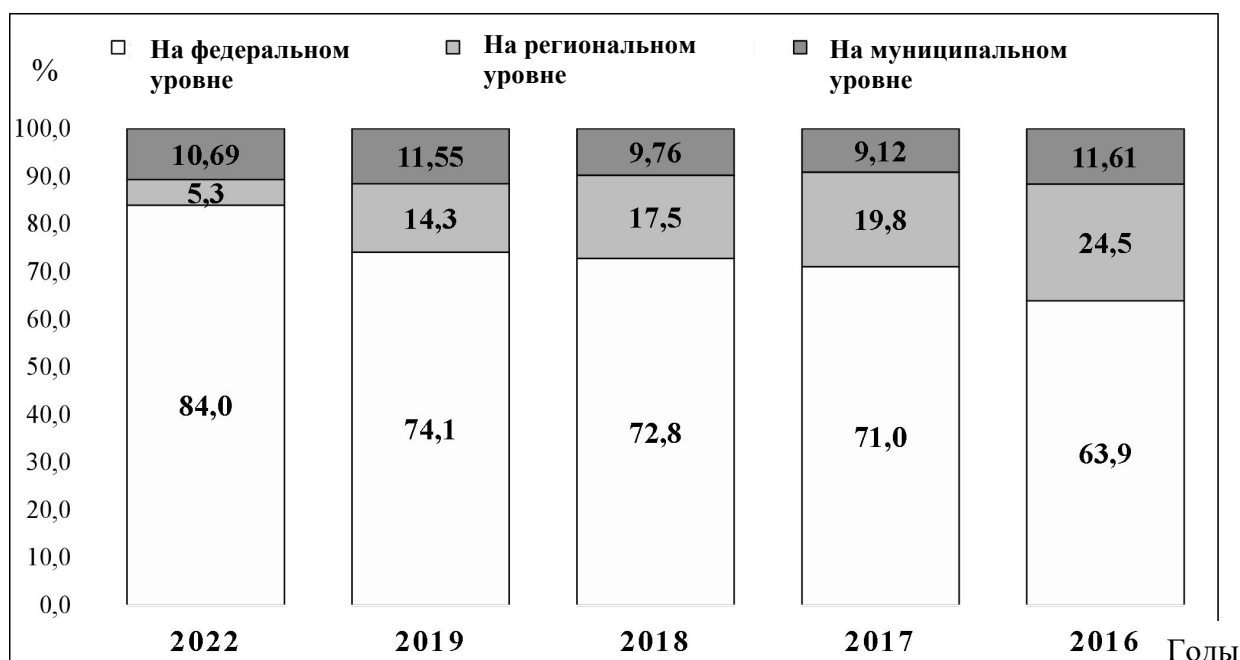


Рис. 10. Удельный вес КНМ, проводившихся органами различного уровня в рассматриваемый период (в процентах от общего количества КНМ)

В целом стоит отметить, что в период с 2016 по 2022 годы в ходе реализации реформы контрольно-надзорной деятельности наблюдалось снижение интенсивности КНМ по отношению к одной компании на территории Тверской области, что видно по увеличению удельного веса опрошенных, указавших на отсутствие КНМ.



Реализация мероприятий реформы контрольно-надзорной деятельности в России начала приносить результаты, заключающиеся в уменьшении числа проверок и активизации взаимодействия контрольно-надзорных органов с предпринимательскими структурами, особенно в рамках взаимодействия с федеральными контролирующими органами.

Таким образом, при сокращении общего числа КНМ в последние годы наблюдается тенденция к уменьшению удельного веса проверок, проводимых на региональном уровне, и увеличению доли проверок, проводимых федеральными органами, в общем числе проверок, что косвенно свидетельствует об усилении централизации в контрольно-надзорной деятельности. Несмотря на существенное уменьшение удельного веса предпринимателей, проходивших проверки, заметного снижения административного давления на бизнес его представители не ощущают.

### **3.2. Взаимодействие бизнеса с контрольно-надзорными органами в контексте цифровизации**

С 1 июля 2021 года вступили в силу основные положения Федерального закона от 31 июля 2020 года № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (далее – Федеральный закон от 31 июля 2020 года № 248-ФЗ, Закон о госконтроле). В связи с проведенной реформой контрольно-надзорной деятельности изменен перечень видов государственного контроля (надзора). Федеральный закон от 31 июля 2020 года № 248-ФЗ, как и Федеральный закон от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (действующий с особенностями применения до 31 декабря 2024 года включительно), не регулирует налоговые, валютные, таможенные проверки, контроль закупок по Федеральным законам № 44-ФЗ и № 223-ФЗ, финансовый контроль.

В ходе анкетирования на протяжении всего периода проведения исследований респонденты также оценивали и количество КНМ, проводимых Федеральной налоговой службой, прокуратурой и полицией, их влияние на работу предприятия.

Как видно из табл. 19, проверки, проводимые вышеназванными органами, в совокупности составили около половины всех КНМ на федеральном уровне.

*На федеральном уровне* в 2022 году наибольшее число проверок пришлось на Роспотребнадзор (20,0 % от общего количества проверок на

федеральном уровне). Второе место заняла ФНС России (19,1 %), на третьем месте – прокуратура (16,4 %).

Таблица 19

Ответы об основных контрольно-надзорных органах, проводивших в 2016–2022 годах проверки на федеральном уровне (в процентах от общего количества КНМ на федеральном уровне)

Федеральные органы контроля (надзора)	Год				
	2022	2019	2018	2017	2016
Роспотребнадзор	20,0	22,6	21,2	19,6	16,6
ФНС России*	19,1	13,4	19,6	18,9	17,8
Прокуратура*	16,4	12,9	16,8	14,3	9,6
Полиция*	10,9	7,5	10,1	8,7	9,3
МЧС России	8,2	15,1	10,1	7,5	8,2
Россельхознадзор	6,4	5,9	3,4	6,4	7,4
Ростехнадзор	5,5	10,2	6,7	7,9	9,9
Роструд	4,5	3,2	1,7	4,5	5,9
Ространснадзор	3,6	2,2	1,7	2,3	3,8

\* Не в рамках Закона о госконтроле.

Доля проверок, проводимых Роспотребнадзором, в общем числе проверок на федеральном уровне увеличилась с 16,6 % в 2016 году до 20,0 % в 2020 году. Это отчасти связано с теми сферами экономической деятельности, которые преобладают в исследуемых предприятиях, поскольку большая часть опрошенных представителей малого и среднего бизнеса занимаются оптовой и розничной торговлей и оказанием разного рода потребительских услуг. Кроме того, на Роспотребнадзор возложен контроль за соблюдением государственных санитарно-эпидемиологических правил и гигиенических нормативов, а также мероприятия по организации и осуществлению федерального государственного санитарно-эпидемиологического надзора и федерального государственного надзора в области защиты прав потребителей и благополучия человека. Это объясняет увеличение частоты проведения КНМ в условиях распространения пандемии коронавируса.

На региональном уровне (табл. 20) очень незначительная часть респондентов, проходивших проверки, смогла оценить деятельность региональных контрольных органов, большинство опрошенных отказались оценивать их влияние на бизнес. По всей видимости, перечисленными региональными органами КНМ не проводились либо практически не повлияли на работу предприятий. Более половины КНМ (57,1 %) на региональном уровне, по мнению участников исследования, пришлось на Министерство Тверской области по обеспечению контрольных функций.

На муниципальном уровне (табл. 21) респондентами чаще всего указывались контрольно-надзорные органы в сфере торговли и услуг (50,0 % проверок), ЖКХ (35,7 %). В динамике на муниципальном уровне заметно увеличение удельного веса проверок в сферах торговли и услуг, ЖКХ, дорожного хозяйства и благоустройства.

Таблица 20

Ответы респондентов о контрольно-надзорных органах, проводивших проверку на региональном уровне в 2022 году (в процентах от общего количества КНМ на региональном уровне)

Варианты ответа	Удельный вес
Министерство природных ресурсов и экологии	2,0
Министерство Тверской области по обеспечению контрольных функций	4,0
Министерство транспорта	0,0
Главное управление «Государственная жилищная инспекция» Тверской области	1,0
Региональная энергетическая комиссия	0,0
Главное управление по государственной охране объектов культурного наследия	0,0

Таблица 21

Распределение ответов респондентов, проходивших проверку на муниципальном уровне, по сферам деятельности (в процентах от общего количества КНМ на муниципальном уровне)

Сфера деятельности	Год				
	2022	2019	2018	2017	2016
Торговля и услуги	50,0	55,6	37,5	50,0	39,6
ЖКХ, дорожное хозяйство и благоустройство	35,7	25,9	29,2	11,8	10,3
Строительство и архитектура	7,1	7,4	8,3	14,7	21,1
Земельно-имущественные отношения	7,1	11,1	12,5	20,6	14,2
Транспорт	0,0	0,0	12,5	2,9	14,8

Большинство опрошенных указывают, что на текущей деятельности работа контрольно-надзорных органов не отразилась или отразилась незначительно. При этом многие респонденты, особенно на региональном уровне, отказались оценить влияние контрольно-надзорных органов на работу компании.

Респондентам было также предложено оценить взаимодействие с сотрудниками контрольно-надзорных органов в ходе проведения КНМ и их профессионализм.

В 2022 году большая часть респондентов (67,4 %) затруднились ответить или не ответили на вопрос о внесении сведений о проверке в единый реестр проверок (68,5; 75,2 и 73,3 % в 2019, 2018 и 2017 годах соответственно) (табл. 22). Можно предположить, что предприниматели Тверской области недостаточно информированы о данном требовании к результатам проведения КНМ либо не интересуются этим вопросом.

Таблица 22

Ответы на вопрос о внесении органом контроля (надзора) сведений о проверке в единый реестр проверок в рассматриваемый период (в процентах от количества респондентов, указавших на проведение КНМ)

Варианты ответа	Год			
	2017	2018	2019	2022
Да	18,7	16,0	23,1	23,8
Нет	8,0	8,8	8,5	8,9
Затрудняюсь ответить	62,9	72,0	63,1	62,4
Нет ответа	10,4	3,2	5,4	5,0

На вопрос: «Возникали ли в ходе проведения КНМ конфликтные ситуации с участием проверяющей стороны?» 84,2 % респондентов в 2022 году ответили отрицательно. Однако 9,9 % опрошенных заявили о конфликтах с сотрудниками контрольно-надзорных органов.

Большинство участников анкетирования (83,2 % в 2022 году; 74,6, 85,6 и 75,3 % в 2019, 2018 и 2017 годах соответственно) указали, что фактические действия органов при проведении КНМ в основном соответствуют целям, задачам и предмету проверки, указанному в распоряжении (приказе), на основании которого такая проверка проводилась. При этом доля отрицательных ответов на вопрос о соответствии фактических действий контрольно-надзорных органов при проведении КНМ целям, задачам, предмету проверки, указанным в распоряжении или приказе о проведении проверки (7,7; 8,8; 13,1 и 7,9 % в 2017, 2018, 2019 и 2022 годах соответственно), означает, что часть респондентов допускают возможность несоблюдения требований к целям, задачам и предмету проверки либо убеждены в незаконных действиях сотрудников контрольно-надзорных органов в ходе проведения проверки.

Более половины респондентов, опрошенных в 2022 и 2019 годах (55,4 и 53,8 % соответственно), затруднились или не стали отвечать на вопрос: «Всегда ли органом государственного контроля (надзора), органом муниципального контроля использовались проверочные листы?». По-видимому, это свидетельствует о том, что они недостаточно хорошо знакомы с принятым порядком осуществления проверок, основными положениями Закона о государственном контроле (надзоре), Постанов-

лением Правительства РФ от 27 октября 2021 года № 1844, утверждающим требования по разработке и применению форм проверочных листов (чек-листов) при плановой проверке и случаи их обязательного применения, а также с другими нормативно-правовыми актами, определяющими требования к контрольно-надзорным органам.

Кроме того, по сравнению с 2019 годом увеличилось количество предпринимателей, заявивших о том, что органом государственного контроля (надзора), органом муниципального контроля не использовались проверочные листы (с 11,5 % в 2019 году до 14,9 % в 2022 году).

Таким образом, оценивая итоги взаимодействия бизнеса с контрольно-надзорными органами, необходимо отметить, что, по мнению респондентов, наибольшее количество проверок в 2022 году провели Роспотребнадзор (федеральный уровень), Министерство Тверской области по обеспечению контрольных функций (региональный уровень) и контрольно-надзорные органы в сферах торговли и ЖКХ (муниципальный уровень).

В перечень видов государственного контроля (надзора) в соответствии с Федеральным законом от 31.07.2020 № 248-ФЗ не включены налоговые, валютные, таможенные проверки, контроль закупок по Законам № 44-ФЗ и № 223-ФЗ, финансовый контроль. Однако несмотря на это, на протяжении всего периода проведения исследований, по заявлению респондентов, проверки, проводимые Федеральной налоговой службой, прокуратурой и полицией, в совокупности составляют около половины всех КНМ на федеральном уровне. При этом большинство респондентов отметили, что на текущей деятельности работа контрольно-надзорных органов не отразилась либо отразилась в незначительной степени. По мнению основной части участников опроса, фактические действия органов при проведении КНМ в целом соответствуют целям, задачам и предмету проверки, указанным в распоряжении (приказе), на основании которого такая проверка проводилась. На вопрос о возникновении конфликтных ситуаций с участием проверяющей стороны в ходе проведения КНМ большинство респондентов ответили отрицательно.

Отмечая очевидные положительные результаты реализации реформы контрольно-надзорной деятельности, связанные с уменьшением интенсивности КНМ по отношению к одной компании на территории Тверской области, стоит сказать, что осведомленность предпринимателей о своих правах и ограничениях проведения отдельных КНМ в 2022 году остается достаточно невысокой. Более половины респондентов, опрошенных в 2019 и 2022 годах, затруднились или не смогли ответить на вопрос, использовались ли органом государственного или муниципального контроля (надзора) проверочные листы. Кроме того, обращает на себя внимание тот факт, что более чем две трети респондентов затруднились или не стали отвечать на вопрос о внесении сведений о проверке в единый

реестр проверок. Можно предположить, что предприниматели Тверской области недостаточно информированы о требованиях к результатам проведения КНМ либо не интересуются этим вопросом.

### **3.3. Оценка влияния реформы контрольно-надзорной деятельности на бизнес**

Помимо закрепления риск-ориентированного подхода, изменения перечня и порядка проведения КНМ, новые нормативно-правовые акты, регулирующие вопросы контроля и надзора, предусматривают возможность применения альтернативных инструментов государственного регулирования экономической деятельности, процедуры профилактики нарушений и иные меры по предупреждению рисков. Риск-ориентированный подход предполагает уменьшение количества государственных проверок в тех сферах, где риск нарушений меньше. Таким образом, его применение должно быть направлено на снижение административной нагрузки на добросовестные предприятия.

Распределение ответов на вопрос о выявленных нарушениях представлено в табл. 23.

*Таблица 23*

Ответы о выявленных нарушениях в рассматриваемый период  
(в процентах от количества респондентов,  
указавших на проведение КНМ)

Варианты ответа	Год				
	2016	2017	2018	2019	2022
Нарушения выявлены по итогам каждой проверки	12,9	11,9	16,8	13,1	7,9
Нарушения выявлены по итогам некоторых проверок	24,3	43,3	47,2	36,9	31,7
Нарушения не выявлены	34,3	33,0	28,0	40,8	49,5
Не стали отвечать на вопрос	28,5	11,9	8,0	9,2	10,9

Примерно у половины участников исследования (49,5 %) в 2022 году не были выявлены нарушения, тогда как у 39,6 % опрошенных нарушения выявлены. В динамике заметно увеличение удельного веса респондентов, у которых при проведении КНМ нарушений не выявляется. Большинство участников исследования заявили, что ими полностью или частично устранены выявленные нарушения. Две трети опрошенных (67,5 %) считают, что все выявленные нарушения по большей части обоснованы, а примерно 20 % – что нарушения не обоснованы или обоснована меньшая их часть. При этом 8,9 % участников опроса, указавших на проведение КНМ в 2022 году, утверждают, что контрольно-надзорные органы запрашивали дополнительные документы (обязательное предоставление

которых не предусмотрено законом). В то же время более половины респондентов (55,4 %) в 2022 году не смогли ответить на поставленный вопрос. Можно предположить, что это связано с недостаточным знанием нормативно-правовых актов в сфере контрольно-надзорной деятельности.

Оценивая проблемы, нарушения или злоупотребления со стороны должностных лиц, почти три четверти опрошенных отметили, что не сталкивались с такими явлениями в ходе проверок (табл. 24).

В динамике растет удельный вес опрошенных, которые заявили об отсутствии нарушений или злоупотреблений со стороны должностных лиц при проведении КНМ, что свидетельствует о положительных итогах реформирования контрольно-надзорной деятельности.

*Таблица 24*

Мнение респондентов о проблемах, нарушениях или злоупотреблениях со стороны должностных лиц при проведении КНМ в рассматриваемый период (в процентах от количества респондентов, указавших на проведение КНМ)

Варианты ответа	Год			
	2017	2018	2019	2022
Да, сталкивались с проблемами, нарушениями или злоупотреблениями	25,8	32,0	24,6	17,8
Нет, с нарушениями и злоупотреблениями не сталкивались	64,5	61,6	67,7	73,3
Нет ответа	9,7	6,4	7,7	8,9

Участникам исследования было предложено указать, какие виды административных наказаний применялись к их компаниям. Согласно данным табл. 25, удельный вес респондентов, указавших на применение таких административных наказаний, уменьшился с 61,2; 52,2; 27,3 и 23,3 % соответственно в 2016, 2017, 2018, 2019 годах до 19,8 % в 2022 году.

*Таблица 25*

Удельный вес респондентов, указавших на применение административных наказаний по отношению к их компании (в процентах от общего количества участников)

Варианты ответа	Год				
	2016	2017	2018	2019	2022
Не указали на применение административных наказаний	38,8	47,8	72,7	76,7	80,2
Административные наказания применялись	61,2	52,2	27,3	23,3	19,8

Самым распространенным видом административных наказаний является штраф. Более половины респондентов, по отношению к предприятиям которых в 2016–2022 годах применялись административные наказания, указали, что это были наказания в виде административных штрафов (рис. 11). Предупреждение применялось реже.

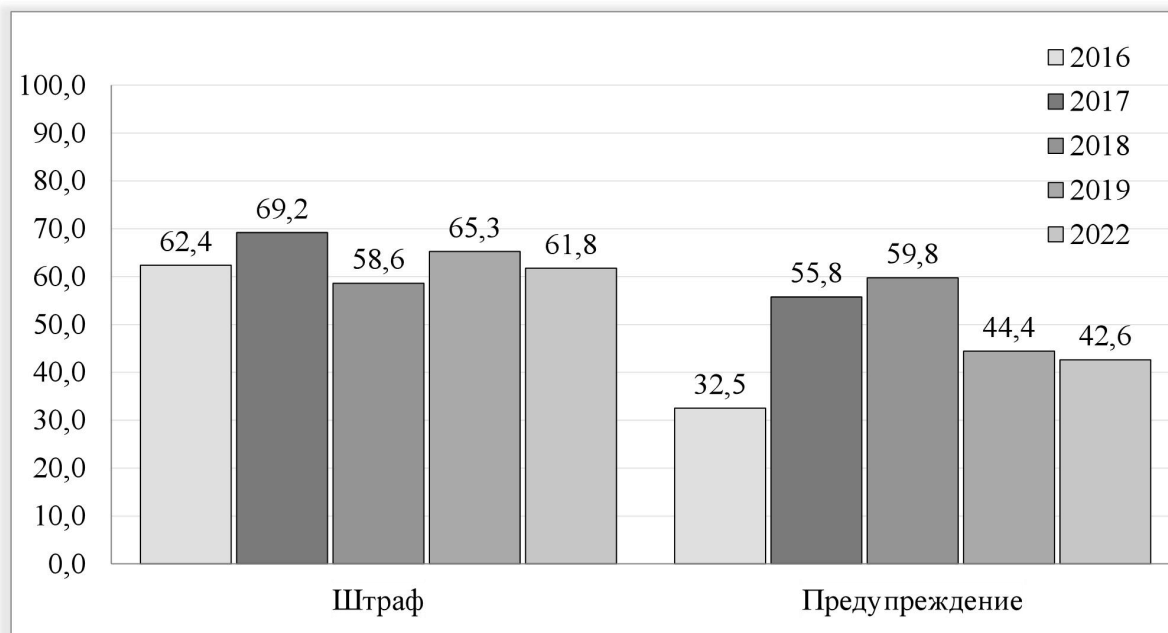


Рис. 11. Ответы респондентов о наиболее распространенных видах административных наказаний в рассматриваемый период (в процентах от числа респондентов, заявивших о применении административных наказаний по отношению к их компаниям)

Например, в 2022 году были оштрафованы 61,8 % респондентов, указавших на применение административных наказаний, тогда как предупреждение вынесено в отношении 42,6 %. Такие виды административных наказаний, как конфискация орудия совершения или предмета совершения правонарушения, лишение специального права (лицензии), дисквалификация должностных лиц или административное выдворение за пределы РФ иностранного гражданина или гражданина без гражданства, применялись достаточно редко.

Оценивая изменение административных наказаний за 2022 год, 58,8 % респондентов заявили, что не ощущают перемен (табл. 26). В восприятии представителей бизнеса административная нагрузка на бизнес за прошедший год существенно не изменилась.

Возможность опротестовать выбранное по результатам проверки наказание опирается на восприятие предпринимателем обоснованности его назначения. Сравнительно небольшое число респондентов, заявивших о применении по отношению к их компании административных наказаний,



пытались обжаловать решение органов контроля и надзора (22,6 %), при этом остальные 77,4 % респондентов, к которым применялись административные наказания, не стали это делать.

Таблица 26

Результаты анкетирования по вопросу  
об изменении административной нагрузки на бизнес  
(в процентах от количества респондентов, ответивших на вопрос)

Варианты ответа	Год					
	2016	2016	2017	2018	2019	2022
Ужесточилась значительно	45,26	68,00	45,3	44,6	47,1	11,6
Ужесточилась незначительно	13,10	19,68	24,7	28,4	28,6	12,0
Не изменилась	8,20	12,32	22,1	21,6	20,0	58,8
Смягчилась незначительно	0	0,00	3,7	5,4	0,0	13,3
Смягчилась значительно	0	0,00	4,2	0,0	4,3	4,3

Тем не менее в относительном выражении доля респондентов, предпринимавших попытки обжаловать решение контрольно-надзорных органов, в 2022 году увеличилась до 22,6 % с 14,8; 14,3 и 14,2 % в 2019, 2018 и 2017 годах соответственно (табл. 27).

Таблица 27

Результаты анкетирования по вопросу о попытках оспаривать  
выявленные нарушения и наложенные по итогам проверок штрафы  
(в процентах от количества респондентов, ответивших на вопрос)

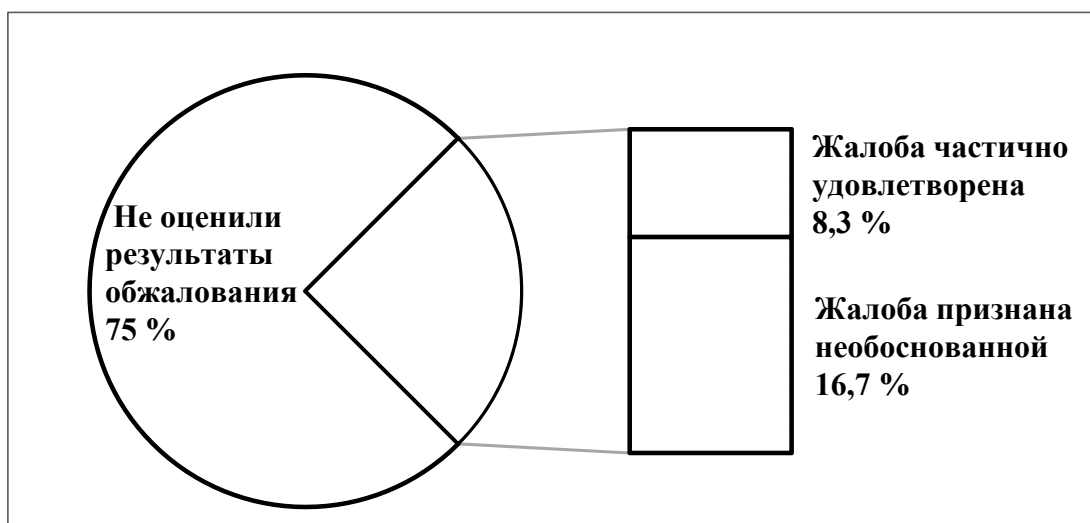
Варианты ответа	Год			
	2017	2018	2019	2022
Да, и добились признания своей правоты	9,3	8,0	11,3	9,4
Да, но нам не удалось доказать свою правоту	4,9	6,3	3,5	13,2
Нет, так как выявленные нарушения и штрафы справедливы	22,4	29,5	21,7	17,0
Нет, так как вышестоящие органы являются заинтересованной стороной	5,3	5,4	6,1	1,9
Нет, из опасения более пристрастного отношения	10,2	10,7	17,4	26,4
Нет (другие причины)	48,0	40,2	40,0	32,1

Увеличение доли респондентов, пытавшихся обжаловать решение контрольно-надзорных органов, связано прежде всего с уменьшением общего числа выявленных нарушений, при этом в абсолютном выражении число представителей бизнеса, готовых вступить в противостояние с государственными органами контроля и надзора, осталось на уровне 2019 года.

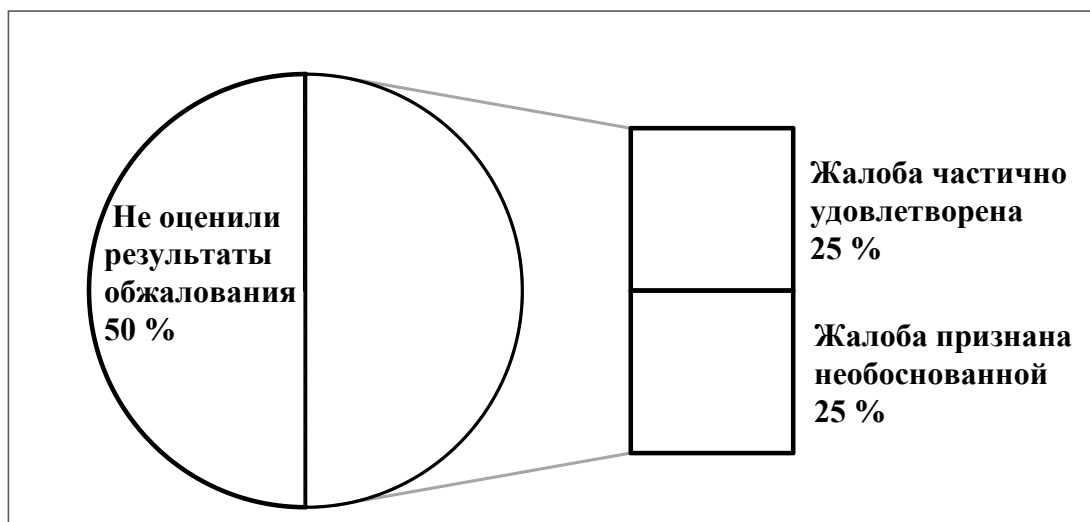
Нежелание участников исследования оспаривать наложенные контрольно-надзорными органами штрафы может свидетельствовать как о

сложности процедуры обжалования, отсутствии у предпринимателей юридических знаний, необходимости дополнительных затрат, длительных сроках рассмотрения дел, так и об отсутствии веры в положительный исход таких действий.

Значительная часть респондентов не раскрыли результаты своих попыток обжаловать решение контрольно-надзорных органов. Три четверти (75 %) и половина респондентов (50 %), заявивших о попытках обжаловать административные наказания в досудебном и судебном порядке соответственно, отказались ответить на вопрос о полученных результатах (рис. 12).



а



б

Рис. 12. Распределение ответов относительно результатов обжалования решений органов государственного контроля (надзора), муниципального контроля в отношении их компаний в 2022 году:

а – в досудебном порядке; б – в суде (в процентах)

Необходимо отметить, что по результатам анкетирования в 2022 году отрицательные результаты обжалования решений контрольно-надзорных органов в досудебном порядке (см. рис. 12а) превалируют над положительными (8,3 % от предпринявших попытки обжаловать административное наказание заявили, что их жалоба была удовлетворена частично, а в 16,7 % случаев жалоба признана необоснованной). При обращении в суд (см. рис. 12б) в одной половине случаев жалоба была удовлетворена частично, а в другой – признана необоснованной.

Таким образом, можно выделить следующие ключевые моменты влияния реформы на бизнес, на которые указали респонденты:

1. Оценивая влияние реформы контрольно-надзорной деятельности на бизнес в целом, следует отметить, что примерно у половины респондентов в 2022 году нарушения не выявлены. В динамике заметно, что удельный вес респондентов, у которых не выявлены нарушения в ходе проведения КНМ, увеличивается. Подавляющее большинство участников опроса полностью или частично устраняют выявленные нарушения и считают выявленные нарушения обоснованными.

2. В динамике растет удельный вес респондентов, которые заявили об отсутствии нарушений или злоупотреблений со стороны должностных лиц при проведении КНМ, что свидетельствует о положительных итогах реформы контрольно-надзорной деятельности.

3. Самым распространенным видом административных наказаний является штраф. Более половины респондентов, к которым применялись административные наказания, утверждают, что в 2016–2022 годах в отношении их компаний применялись наказания в виде административных штрафов. Удельный вес штрафов в общем числе административных наказаний в динамике практически не изменяется (он остается на уровне примерно 60 % от общего числа случаев), но количество респондентов, заявляющих о применении к их компании административных наказаний, сокращается. Предупреждение применяется реже, чем штраф.

4. Сравнительно небольшое число респондентов, заявивших о применении по отношению к их компании административных наказаний, предпринимали попытки обжаловать решение органов контроля и надзора. Большинство респондентов, заявивших о попытках обжаловать административные наказания в досудебном и судебном порядке, отказались ответить на вопрос о полученных результатах. Тем не менее предпринимателям, уверенным в необоснованности решений контрольно-надзорных органов, имеет смысл использовать процедуру их обжалования в досудебном или судебном порядке.

### 3.4. Мнение бизнеса о результатах реформирования и цифровой трансформации контрольно-надзорной деятельности государства

Результаты опросов показывают, что осведомленность предпринимателей о своих правах и ограничениях проведения отдельных КНМ остается невысокой. Недостаточная информированность выявлена по целому ряду вопросов реформирования контрольно-надзорной деятельности. Так, несмотря на то, что более двух третей респондентов (68,8 %) заявили о своей осведомленности об ограничении проведения отдельных КНМ в 2022 году, большинство из них (57,7 %) не смогли ответить на вопрос, распространяются ли данные ограничения на их предприятие или вид деятельности.

Включенный в анкету вопрос о знании предпринимателем категории риска (класса опасности), присвоенной компании, выявил, что порядка трех четвертей участников опроса не в курсе происходящих изменений в контрольно-надзорной деятельности и не знают категорию риска своего предприятия (рис. 13). Мнение респондентов, знающих свою категорию риска, о согласии с присвоенной категорией риска (классе опасности) представлено в табл. 28.



Рис. 13. Осведомленность респондентов о категории риска (классе опасности), присвоенной их предприятию в рассматриваемый период (в процентах от общего количества опрошенных)

Таблица 28

Распределение мнений респондентов относительно их согласия с категорией риска (классе опасности), присвоенной их предприятию (в процентах от количества опрошенных, знающих свою категорию риска)

Варианты ответа	Год			
	2017	2018	2019	2022
Да	78,8	81,4	73,9	87,2
Нет, категория риска (класс опасности) слишком высокая	7,6	8,1	17,4	12,8
Затрудняюсь или нет ответа	13,6	10,5	8,7	0,0

Большинство респондентов, которым известна своя категория риска, согласны с присвоенным им классом опасности – 87,2 % в 2022 (73,9; 81,4 и 78,8 % в 2019, 2018 и 2017 годах соответственно), при этом 12,8 % в 2022 году (17,4; 8,1 и 7,6 % в 2019, 2018 и 2017 годах соответственно) считают, что высокая категория риска присвоена их компании необоснованно.

Возможности получения информационно-справочной поддержки, предоставляемые органами власти, используются относительно небольшим числом респондентов. Только 28,6 % респондентов в 2022 году (31,1; 29,2 и 33,4 % в 2019, 2018 и 2017 годах соответственно) известно о публичных консультациях, регулярно проводимых органами государственного контроля (надзора) по результатам своей деятельности (табл. 29).

Таблица 29

Ответы респондентов на вопрос об осведомленности о регулярных публичных консультациях, проводимых органами государственного контроля (надзора) (в процентах от общего количества респондентов)

Варианты ответа	Год			
	2017	2018	2019	2022
Знаю	33,4	29,2	31,1	28,6
Не знаю или затрудняюсь ответить	60,2	66,1	65,0	66,2
Нет ответа	6,4	4,7	3,9	5,2

Большинство респондентов (84,8 и 83,8 % в 2022 и 2019 годах соответственно) не участвовали в публичных обсуждениях результатов правоприменительной практики, проводимых органами государственного контроля (надзора) (рис. 14).

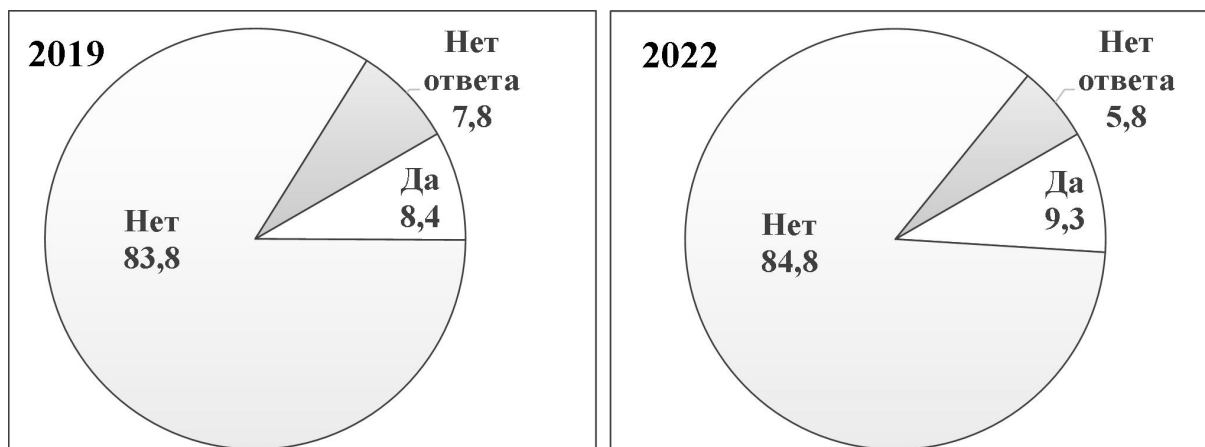


Рис. 14. Распределение ответов на вопрос об участии респондентов в публичных обсуждениях результатов правоприменительной практики, проводимых органами государственного контроля (надзора) (в процентах от общего количества опрошенных)

Низкая осведомленность представителей бизнеса наблюдается и в отношении возможностей прохождения самообследования с использованием чек-листов по видам государственного контроля (надзора) перед проведением КНМ. О такой возможности информированы менее 20 % участников исследования, при этом прошли самообследование только 8,7 % опрошенных.

Представители бизнеса также недостаточно информированы о возможности профилактических визитов со стороны органов контроля и надзора. Более двух третей респондентов (69,1 %) заявили, что не видят отличий от проверки. В то же время свыше 6 % участников опроса указали на наличие потребности в проведении профилактического визита (табл. 30).

Таблица 30

Ответы на вопрос о проведении на предприятиях респондентов профилактического визита (в процентах от общего количества опрошенных в 2022 году)

Варианты ответа	Удельный вес
Да, проводился в очной форме	7,0
Да, проводился путем использования видео-конференц-связи	2,0
Нет, хотя обращались с просьбой об этом в уполномоченный орган	0,6
Нет, но существует потребность в его проведении	5,8
Нет, не видим отличия профилактического визита от проверки	69,1
Нет ответа	15,5

Участникам исследования было также предложено оценить эффективность отдельных профилактических мероприятий, проводимых органами государственного контроля (надзора) в рамках реформы контрольно-надзорной деятельности.

По степени полезности информации, эффективности ее доведения и организации респонденты самыми эффективными считают **консультирование** с сотрудниками органов государственного контроля (надзора). В наименьшей степени по эффективности респонденты оценивают **самообследование**. Интегральная средневзвешенная оценка отдельных профилактических мероприятий по всем критериям в совокупности представлена в табл. 31.

*Таблица 31*

Интегральная средневзвешенная оценка эффективности отдельных профилактических мероприятий в 2022 году по всем критериям по пятибалльной шкале (1 – совсем неэффективно, 5 – очень эффективно)

Мероприятие	Баллы
Консультирование	4,13
Обобщение правоприменительной практики	3,63
Профилактический визит	3,72
Самообследование	3,45

Наиболее эффективной мерой в рамках реформы контрольно-надзорной деятельности респонденты считают замену штрафа на предупреждение и мораторий на КНМ (табл. 32).

*Таблица 32*

Оценка респондентами в 2022 году степени эффективности мер, принятых государством в рамках реформы контрольно-надзорной деятельности (в процентах от общего количества опрошенных)

Варианты ответа	Удельный вес
Замена штрафа на предупреждение	44,6
Мораторий на КНМ	41,7
Профилактические мероприятия	22,2
Сокращение обязательных требований	19,5
Штраф со скидкой в 50 %	19,5
Уменьшение размера штрафа для субъектов малого и среднего предпринимательства	18,4
Исключение дублирования ответственности организации и ее руководителя	7,0
Возбуждение дел об административных правонарушениях только после проведения КНМ	5,5
Установление принципов введения обязательных требований и оценка их эффективности	4,4

В рамках реформы контрольно-надзорной деятельности благодаря возможностям цифровизации и применению ИКТ расширяется практика дистанционного контроля со стороны надзорных органов и удаленного взаимодействия в рамках КНМ.

Отказ от личных встреч, помимо профилактики распространения коронавирусной инфекции, способствует снижению коррупционных рисков. Очевидно, что не все виды проверок могут проводиться дистанционно и не все контрольно-надзорные органы могут осуществлять КНМ в удаленном формате. Так, документарные проверки могут быть проведены в удаленном режиме, в то время как проверку продукции, выполнение различных экспертиз и замеров сложно обеспечить в рамках такого формата. Большинство органов контроля уже частично перешли на дистанционное взаимодействие с бизнесом и предлагают различные сервисы и консультации для бизнеса в удаленном формате.

Предпринимателям было предложено оценить по пятибалльной шкале работу электронных сервисов (1 – совсем неэффективно, 5 – очень эффективно). Средневзвешенные оценки электронных сервисов представлены в табл. 33.

Наилучшим образом респонденты оценили портал государственных услуг (сервис подачи жалобы в рамках досудебного порядка обжалования для отдельных видов госконтроля). Средневзвешенная оценка составила 3,68 балла, а самую низкую оценку (3,21) получил «Сервис 360°» Корпорации МСП.

*Таблица 33*

Оценка респондентами эффективности работы электронных сервисов

Электронный сервис	Средневзвешенная оценка по пятибалльной шкале (1 – совсем неэффективно, 5 – очень эффективно)	Удельный вес респондентов, не ответивших на поставленный вопрос, %
Единый реестр КНМ	3,32	75,2
Единый реестр видов контроля	3,31	77,3
Портал государственных услуг (подача жалобы в рамках досудебного порядка обжалования для отдельных видов госконтроля)	3,68	70,3
«Сервис 360°» Корпорации МСП	3,21	80,2



Необходимо отметить, что большинство респондентов не смогли оценить эффективность электронных сервисов. Это, возможно, связано с низкой информированностью предпринимателей о новых возможностях удаленного взаимодействия с надзорными органами, недостаточной осведомленностью о консультировании бизнеса в дистанционном формате и различных сервисах, появившихся в ходе реформы контрольно-надзорной деятельности.

Как видно из табл. 33, «Сервис 360°» Корпорации МСП оценили менее 20 % опрошенных. Это свидетельствует, с одной стороны, о недостаточно активном использовании субъектами предпринимательства интернет-ресурсов, а с другой – о сложностях самостоятельного принятия решения на основе справочной информации и желании избежать ошибок.

Предпринимателям также было предложено выбрать наиболее действенные меры, которые позволят повысить эффективность контрольно-надзорной деятельности. Ответы представлены в табл. 34.

Наиболее значимой мерой по повышению эффективности контрольно-надзорной деятельности в ходе ее реформирования респонденты считают разработку простых и понятных инструкций для бизнеса по процедурам контроля (надзора). Этот ответ отметили около половины опрошенных.

Таблица 34

Оценка респондентами в 2022 году степени эффективности мер, принятых государством в рамках реформы контрольно-надзорной деятельности (в процентах от общего количества респондентов)

Варианты ответа	Удельный вес, %
Разработка простых и понятных инструкций (памяток) по процедурам контроля (надзора)	41,7
Снижение частоты внесения изменений в законодательство	23,3
Отказ от возбуждения дела об административном правонарушении при своевременном исполнении предписания	21,9
Применение мер стимулирования добросовестности контролируемых лиц	17,2
Налаживание системы межведомственного взаимодействия	15,7
Повышение квалификации инспекторов	9,9
Сокращение обязательных требований	8,7
Другое	5,0
Подача жалобы, размещение результата ее рассмотрения через Единый реестр КНМ	2,3

Как показывают результаты исследования, основной проблемой в процессе реализации реформы контрольно-надзорной деятельности является плохая информированность предпринимателей по целому ряду вопросов, касающихся применения риск-ориентированного подхода, прав предпринимателей и возможностей, которые предоставляются бизнесу в рамках проводимой реформы.

Большинство представителей бизнеса не в курсе изменений в контрольно-надзорной деятельности, связанных с применением риск-ориентированного подхода, и не знают категорию риска своего предприятия. Выявлена недостаточная информированность предпринимателей о предоставляемых органами власти возможностях публичного консультирования, получения информационно-справочной поддержки и т.д.

Представляется, что реализация реформы на региональном и муниципальном уровнях требует дальнейшего углубления и тиражирования наиболее успешных практик. Обеспечение синхронности реализации программы в субъектах РФ и повышение качества реализации контрольно-надзорных полномочий осложняется существенной дифференциацией регионов по уровню развития предпринимательской активности и административному климату.

## **РАЗДЕЛ 4. ПОВЫШЕНИЕ УРОВНЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БИЗНЕСА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ**

### **4.1. Государственная политика обеспечения экономической безопасности в условиях цифровизации**

Цифровая трансформация – это проявление качественных, революционных изменений, заключающихся не только в отдельных цифровых преобразованиях, но и в кардинальном изменении структуры экономики, в переносе центров создания добавленной стоимости в сферу построения цифровых ресурсов и цифровых процессов. В результате цифровой трансформации происходит переход к новому технологическому и экономическому укладу, а также создаются новые сектора экономики.

Экономическая безопасность отражает способность институциональной системы защищать интересы хозяйствующих субъектов на основе национальных и международно-правовых норм для обеспечения стабильного ведения бизнеса, экономического роста, снижения эконо-

мических рисков. В современных условиях приоритетная задача обеспечения экономической безопасности состоит в прогнозировании вызовов и угроз, важнейшей из которых является цифровая трансформация.

В предыдущем разделе раскрывается положительное и отрицательное влияние цифровизации экономики на уровень экономической безопасности, а также рассматриваются риски для экономической безопасности государства в условиях цифровизации.

Государственная политика и нормативные акты играют ключевую роль в осуществлении прорывного научно-технологического и социально-экономического развития страны, увеличении численности населения страны, повышении уровня жизни граждан, создании комфортных условий для их проживания, а также условий и возможностей для самореализации и раскрытия таланта каждого человека. В этой связи 7 мая 2018 года Президент РФ подписал Указ № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», содержащий основные направления деятельности Правительства Российской Федерации и прогноз социально-экономического развития Российской Федерации на период до 2024 года. Ключевые направления развития цифровой экономики в России наглядно представлены на рис. 15.



Рис. 15. Ключевые направления развития цифровой экономики в России

21 июля 2020 года Президентом РФ был подписан Указ № 474 «О национальных целях развития Российской Федерации на период до 2030 года». В нем, в частности, определены следующие национальные цели развития РФ:

- сохранение населения, здоровья и благополучия людей;
- обеспечение возможности для самореализации и развития талантов;
- создание комфортной и безопасной среды;
- обеспечение условий для достойного, эффективного труда и успешного предпринимательства;
- цифровая трансформация.

Кроме того, для реализации внутренней и внешней политики Российской Федерации в сфере применения ИКТ, направленных на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов, Указом Президента РФ от 9 мая 2017 года № 203 была утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.

В соответствии с Приказом Минсвязи России № 428 от 1 августа 2018 года цифровизация (цифровое развитие) – процесс организации выполнения в цифровой среде функций и деятельности (бизнес-процессов), ранее выполнявшихся людьми и организациями без использования цифровых продуктов. Цифровизация предполагает внедрение в каждый отдельный аспект деятельности информационных технологий.

Региональные проекты в области цифровой экономики разрабатываются в целях обеспечения показателей и результатов, определенных в соответствующих федеральных проектах национальной программы «Цифровая экономика Российской Федерации», а также в национальных программах (проектах), федеральных и ведомственных проектах, разрабатываемых в соответствии с Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», и являются отдельными структурными элементами государственной программы субъекта Российской Федерации.

Субъекту Российской Федерации следует разработать пять региональных проектов по следующим обязательным направлениям, соответствующим федеральным проектам национальной программы «Цифровая экономика Российской Федерации»:

1) информационная инфраструктура (с учетом федерального проекта «Информационная инфраструктура»);

2) кадры для цифровой экономики (с учетом федерального проекта «Кадры для цифровой экономики»);

3) информационная безопасность (с учетом федерального проекта «Информационная безопасность»);

4) цифровые технологии (с учетом федерального проекта «Цифровые технологии»);

5) цифровое государственное управление (с учетом федерального проекта «Цифровое государственное управление»).

По каждому из указанных направлений предусмотрена разработка отдельного регионального проекта.

Цифровизация приоритетных отраслей экономики и социальной сферы в субъектах Российской Федерации предусматривает мероприятия по цифровизации ряда отраслей: городского хозяйства, здравоохранения, образования, транспортной инфраструктуры, промышленности, сельского хозяйства, строительства, энергетики и иных отраслей экономики, приоритетных для субъекта Российской Федерации.

Мероприятия по цифровизации отрасли здравоохранения в субъектах РФ разрабатываются с учетом федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)» Министерства здравоохранения РФ. Следует предусмотреть мероприятия по созданию и развитию государственных информационных систем в сфере здравоохранения субъектов РФ, соответствующих требованиям Минздрава России, и их подключению к ЕГИСЗ.

Мероприятия по цифровизации отрасли городского хозяйства и внедрению принципов «умного города» в субъектах РФ разрабатываются с учетом ведомственного проекта «Цифровизация отрасли городского хозяйства “Умный город”» Министерства строительства и жилищно-коммунального хозяйства Российской Федерации.

Мероприятия по цифровизации отрасли образования в субъектах РФ разрабатываются с учетом федерального проекта «Цифровая образовательная среда» национального проекта «Образование», ответственным исполнителем которого является Министерство просвещения РФ. В числе таких мероприятий предусмотрено:

внедрение целевой модели цифровой образовательной среды, в том числе обновление в образовательных организациях материально-технической базы (средств вычислительной техники, программного обеспечения и презентационного оборудования и т.д.);

развитие региональных информационных сервисов и ресурсов в сфере образования;

использование информационных сервисов и ресурсов федеральной информационно-сервисной платформы цифровой образовательной среды, в частности цифрового образовательного контента;

внедрение современных цифровых технологий в административно-управленческую деятельность образовательных организаций, планирование занятий и ведение расписания, электронного журнала и дневника, учета движения учащихся, формирование отчетности (аналитика и отчетность на основании больших данных, электронная отчетность, электронный документооборот, облачная бухгалтерия и т.д.);

развитие цифровой среды для взаимодействия (в том числе в формате peer-to-peer), создание платформ для проведения онлайн-занятий,

работы в проектных группах (образовательные коллаборации, практики наставничества, кросс-форматная среда коммуникации, обмен и передача опыта);

внедрение цифровых платформ по развитию компетенций и управлению человеческим капиталом.

Мероприятия по цифровизации отрасли транспорта и логистики в субъектах РФ разрабатываются с учетом мероприятий ведомственного проекта «Цифровой транспорт и логистика» Министерства транспорта РФ.

Мероприятия по цифровизации отрасли промышленности в субъектах РФ разрабатываются с учетом ведомственного проекта «Цифровая промышленность (Промышленность 4.0)» Министерства промышленности и торговли РФ. В числе таких мероприятий предусмотрены:

создание регионального центра компетенций или центра трансфера технологий, обеспечивающего, в частности, консультативную поддержку по вопросам внедрения цифровых технологий для средних и малых промышленных предприятий субъекта РФ;

создание испытательных полигонов, площадок для апробации и тестирования цифровых технологий в промышленности, в том числе на базе промышленных кластеров;

создание системы переподготовки для сотрудников производственных предприятий в целях цифровой трансформации промышленности;

мониторинг реализации проектов по цифровой трансформации предприятий обрабатывающих отраслей промышленности;

интеграция региональных информационных ресурсов в сфере промышленности с Государственной информационной системой промышленности (ГИСП);

государственная поддержка проектов по цифровой трансформации промышленности, в том числе с использованием региональных фондов развития промышленности.

Мероприятия по цифровизации отрасли сельского хозяйства в субъектах РФ разрабатываются с учетом ведомственного проекта «Цифровое сельское хозяйство» Министерства сельского хозяйства РФ.

Мероприятия по цифровизации отрасли строительства в субъектах РФ разрабатываются с учетом ведомственного проекта «Цифровое строительство» Минстроя России. В числе таких мероприятий предусмотрены:

создание системы мониторинга строительства многоквартирных домов на территории субъекта Российской Федерации;

внедрение информационной системы для формирования единой интеграционной среды решения задач бюджетного и инвестиционного

строительства в регионе в целях минимизации сроков и прозрачности исполнения административных процедур строительной отрасли;

формирование единого банка проектной, исполнительной и отчетной документации по объектам капитального строительства на территории субъекта Российской Федерации;

переход к системе управления жизненным циклом объектов капитального строительства, строящихся за счет средств регионального бюджета, путем внедрения технологий информационного моделирования Building Information Modelling (BIM) на базе государственной информационной системы обеспечения градостроительной деятельности Российской Федерации;

внедрение информационной системы планирования, контроля строительства, реконструкции и капитального ремонта, а также последующей эксплуатации объектов, в том числе объектов, строящихся за счет средств бюджетов различного уровня, с переходом на ведение и представление всей первичной исполнительной и отчетной документации исключительно в электронном виде и с использованием технологий информационного моделирования, с учетом результата мероприятий, предусмотренных в рамках федерального проекта «Цифровое государственное управление».

Мероприятия по цифровизации энергетики в субъектах РФ разрабатываются с учетом ведомственного проекта «Цифровая энергетика» Министерства энергетики РФ. В числе таких мероприятий предусмотрено:

содействие реализации пилотных проектов по внедрению отечественных цифровых решений для предприятий топливно-энергетического комплекса;

создание испытательных полигонов, площадок для апробации и тестирования цифровых технологий при участии организаций топливно-энергетического комплекса;

создание системы переподготовки для сотрудников.

На наш взгляд, для обеспечения экономической безопасности и дальнейшего позитивного развития государства в сферах цифровой экономики следует разработать специальную программу развития цифровой экономики, выделив следующие приоритетные направления:

нормативно-правовое регулирование цифровой индустрии, формирование нового подхода к выявлению необходимых и достаточных законодательных ограничений в отрасли;

повышение цифровой грамотности населения страны (в том числе достижение высоких показателей выпуска компетентных специалистов в области ИКТ);

создание конкурентных условий для формирования в регионах крупных, средних и малых предприятий, работающих в сфере цифровых технологий, и вывод ряда этих компаний на международные рынки;

обеспечение населения страны доступом к широкополосному интернету, разработка новых технологий и средств связи (в том числе для формирования технологической базы функционирования системы связи на основе отечественных разработок).

Помимо вышеперечисленных направлений, программа должна предусматривать эффективные меры по обеспечению уровня экономической безопасности страны. В этой связи имеет смысл обратиться к опыту зарубежных стран по развитию цифровой экономики. Более подробно данный вопрос рассмотрен в следующем параграфе.

#### **4.2. Перспективные направления повышения экономической безопасности на основе цифровизации: международный опыт**

Цифровые технологии трансформируют мировую экономику. Как показывает статистика последних лет, многие страны, которым удалось совершить цифровизацию, в полной мере оценили ее положительные последствия для экономики. Тем не менее многим странам еще только предстоит ощутить все преимущества. В то же время они имеют уникальную возможность учитывать опыт ведущих стран при разработке государственной политики в сфере цифровизации, отвечающей их собственным потребностям и местным условиям. Например, таким шансом воспользовались Корея и Сингапур – вчерашние новички, ставшие сегодня лидерами в своем регионе.

В марте 2021 года Европейская комиссия представила концепцию цифровой трансформации Евросоюза на период до 2030 года. В ее основу положены следующие основные составляющие:

1) навыки и умения (число специалистов, занятых в цифровой сфере, должно превысить 20 миллионов человек; базовыми цифровыми навыками должны обладать как минимум 80 % населения ЕС; гендерная конвергенция);

2) безопасность и устойчивость цифровой инфраструктуры (повсеместное распространение 5G, удвоение доли ЕС в мировом объеме выпуска полупроводников, внедрение квантового компьютера);

3) цифровая трансформация бизнеса (долю европейских компаний, использующих облачные технологии, ИИ, большие данные, планируется довести до 75 % и удвоить количество компаний-«единорогов»;



долю малых и средних предприятий, использующих ИКТ, довести до 90 %);

4) цифровизация госуслуг (100%-й переход на электронный формат оказания государственных услуг, электронные медицинские карты).

Анализ опыта зарубежных стран, достигших наиболее заметных результатов на пути цифровизации (таких, например, как Южная Корея, Сингапур и Гонконг, Эстония, Тайвань и Объединенные Арабские Эмираты), позволяет утверждать, что ключевыми факторами их успеха являются следующие [77]:

активизация внедрения цифровых инструментов (электронная коммерция, цифровые платежи, развлечения и т.д.);

привлечение, обучение и создание условий для развития специалистов в области цифровой экономики. Например, Дания занимает лидирующее положение по уровню обеспеченности кадрами для цифровой экономики, однако, по мнению ряда специалистов, ее более жесткая, чем у большинства стран – членов ЕС, миграционная политика может создать проблемы на пути дальнейшей цифровизации;

поддержка малого и среднего бизнеса в IT-секторе;

предоставление скоростного, общедоступного, наземного (например, оптоволоконного) и мобильного широкополосного доступа в интернет;

ориентация на экспорт цифровых товаров, услуг или медиаконтента;

координация взаимодействия между университетами, предприятиями, властью и экспертами в цифровой экономике.

Анализ опыта стран, в которых цифровизация еще не достигла высокого уровня, но при этом отмечаются высокие темпы роста цифровой экономики (таких, например, как Кения, Вьетнам, Бангладеш, Руанда и Аргентина, Индонезия и Индия), показал, что этому в большей степени способствовал ряд факторов [77]:

обеспечение доступности и высокого качества мобильного интернета для большого числа пользователей;

формирование институциональной среды и создание системы правового регулирования цифровой экономики;

привлечение инвестиций в цифровые предприятия, финансирование цифровых исследований и разработок, подготовка кадров и создание рабочих мест для цифровой экономики;

принятие мер по решению проблемы цифрового неравенства (в зависимости от пола, класса, этнической принадлежности и географических границ).

Для стран Африки, Азии, Латинской Америки и Южной Европы, которые находятся в зоне риска, или стран, в которых наблюдается стагнация цифровой экономики (многие из них являются членами Европейского союза, достигли цифровой зрелости, но происходит замедление темпов экономического роста), аналитики рекомендуют [77]:

обеспечить финансовую поддержку текущих инноваций;

расширить меры государственной поддержки для обеспечения доступа пользователей к информационным технологиям и их защиты от кибератак и других угроз;

решить проблему нехватки специалистов для цифровой экономики посредством реформирования иммиграционной политики;

осуществлять поиск новых технологических ниш и создавать благоприятные условия для привлечения инвестиций;

ориентироваться на долгосрочные стратегические инвестиции в создание инфраструктуры цифровой экономики;

создавать и внедрять цифровые продукты и услуги, способствующие повышению производительности труда и увеличению количества рабочих мест;

поддерживать инициативы (особенно в рамках государственно-частного партнерства), направленные на обеспечение равного доступа к ресурсам сети Интернет по разумной цене.

Опишем ряд долгосрочных тенденций наиболее успешных стран, ориентированных на цифровую эволюцию.

### ***1. Больше конфиденциальности данных, меньше протекционизма данных.***

Под протекционизмом данных будем понимать меры государственного регулирования, направленные на ограничение коммерческого использования цифровых данных.

Экономики, ориентированные на безопасный и беспрепятственный способ получения цифрового опыта, воспитывают тем самым активных потребителей, создают клиентоориентированные, эффективные цифровые экосистемы, которые затем самостоятельно генерируют новые данные, являющиеся одним из ключевых факторов конкурентоспособности в условиях цифровой экономики. Такие страны, как Сингапур, Япония, Канада, Нидерланды, наглядно иллюстрируют этот подход, сочетая открытость и доступность данных и их конфиденциальность.

Между тем в ряде стран – Китае, России, Иране, Саудовской Аравии – наблюдается парадокс: несмотря на значительные государственные инвестиции в создание цифровой экосистемы, правительства в то же время препятствуют свободному потоку данных, что приводит к убыткам в виде упущенной выгоды. Растущая популярность

законов о локализации данных (то есть правил, ограничивающих трансграничную передачу данных) в конечном счете делает их менее доступными, что не только препятствует глобальному экономическому росту, но и снижает конкурентоспособность страны.

В новых экономических условиях политикам следует пересмотреть ключевые индикаторы при формировании стратегии социально-экономического развития. В частности, коллективом авторов во главе с деканом факультета глобального бизнеса Школы Флетчера при Университете Тафтса Б. Чакраворти в качестве такого индикатора предложен «новый ВВП» – валовой продукт, характеризующий результат цифровой экономики.

### ***2. Свободный доступ в интернет необходим, но недостаточен.***

Действительно, рост доступности интернета для широких слоев населения дал мощный толчок развитию цифровой экономики. В этом плане Индии удалось достичь впечатляющих результатов: за последние четыре года количество пользователей сети Интернет здесь удвоилось, и к 2023 году страна собирается приплюсовать еще 350 миллионов пользователей глобальной сети.

Мобильные телефоны – это лишь первый шаг к раскрытию преимуществ цифровизации. Так, пандемия коронавируса продемонстрировала, что развитие цифровой экономики зависит как от качества доступа (то есть более надежного широкополосного доступа по сравнению со спорадическими спутниковыми соединениями), так и от качества самих устройств – ноутбуков и планшетов (в сравнении с недорогими мобильными телефонами). Так, когда Индия вынуждена была перейти на дистанционное образование, единственным способом общения обучающихся с педагогами стало приложение WhatsApp, так как большинство из них имели в своем распоряжении лишь мобильный телефон.

Таким образом, странам с менее развитой цифровой экономикой необходимо наряду с улучшением доступа к недорогому мобильному интернету инвестировать в развитие компьютерной техники. Следование данной стратегии позволило добиться цифрового прорыва таким странам, как Кения, Индия и Вьетнам. И, конечно же, Китай – бесспорный мировой лидер (когда речь идет о внедрении мобильных устройств) благодаря сочетанию масштабных инвестиций в инфраструктуру 4G и развитию рынка мобильных устройств (Xiaomi, Oppo, Huawei и Vivo).

### ***3. Компромисс между развитием по вертикали и распределением по горизонтали.***

Как только экономика достигает определенного уровня цифрового развития, она часто сталкивается с выбором: сохранить темп роста или

направить усилия на укрепление существующих институтов, обеспечить справедливое распределение цифровых технологий по классам, полу, этнической принадлежности и географическому положению.

Всемирный экономический форум объявил 2020 год началом Четвертой промышленной революции, следовательно, сейчас мы стоим у истоков новой эпохи. Как известно, наступление Четвертой промышленной революции ускорилось из-за введения мер социального дистанцирования, местных локдаунов и изоляции городов в глобальном масштабе в целях противодействия распространению пандемии COVID-19 [48].

В контексте развития «умных» городов по всему миру ключевым остается вопрос о том, способствуют ли в конечном счете инвестиции в «умные» технологии росту благосостояния горожан и достижению целей устойчивого развития. Несмотря на очевидные различия в национальных подходах к развитию «умных» городов, центральным элементом любой концепции остается приоритизация интересов индивида.

Политика в сфере «умных» городов должна решать следующие задачи [48]:

- 1) содействовать росту качества жизни и оказания услуг;
- 2) способствовать вовлечению заинтересованных сторон в процесс местного управления и всевозможные сети сотрудничества;
- 3) обеспечивать открытый доступ к данным и взаимодействие заинтересованных сторон;
- 4) формировать целостные и соответствующие запросу решения городских проблем.

Китай и Индия способствовали формированию спроса на «умные» города, который затем подхватили другие страны мира. Практическое внедрение концепции «умного» города в крупнейших агломерациях стало возможным благодаря развитию технологий ИИ, в частности технологий глубокого обучения. Крупные компании в странах Азии, Европы и Северной Америки отреагировали на растущий спрос и занялись разработкой соответствующих решений.

Страны Азии рассматривают «умные» городские системы как способ повысить конкурентоспособность городов и создать импульс для развития городской экономики. В основе стратегии Китая лежит широкое использование технологий ИИ. Список приоритетных национальных проектов был представлен в 2013 году, а с 2014 года под патронажем Министерства жилищного строительства и городского развития были реализованы порядка 500 проектов «умных» городов [48].

Пионером среди стран Азии в развитии «умных» городов стала Южная Корея, где в 2009 году был заложен город Сонгдо, для управления которым были внедрены ИКТ. В 2015 году была запущена инициатива «Умный город» (Smart City Initiative – SCI), в рамках которой в 2018 году «умные» системы были внедрены в Пусане и новом административном центре страны – Седжоне. Благодаря высокому уровню внедрения мобильных технологий, пользователями которых являются 95 % населения страны, высокому уровню урбанизации, развитому ИТ-сектору и активному местному самоуправлению, проекты в рамках SCI имели большой успех. Следует также отметить, что правительство страны регулярно пересматривает приоритеты своей работы, чтобы обеспечить надлежащий уровень защищенности данных, сократить цифровой разрыв и минимизировать издержки цифрового развития.

Начиная с 2010 года Япония также активно поддерживает развитие «умных» городских систем в рамках Новой экономической стратегии и специальной инициативы «Город будущего». В 2016 году правительство страны представило стратегию «Инвестиции будущего», в которой построение Общества 5.0 – японской версии концепции Четвертой промышленной революции – рассматривалось как предтеча будущего развития «умных» городов. Возводя «умные» города, Япония фокусируется на развитии здравоохранения, повышении мобильности, укреплении цепочек поставок, совершенствовании городской инфраструктуры и развитии сферы цифровых финансовых технологий в целом [48].

Индия реализует национальную политику в сфере «умных» городских решений с момента запуска в 2014–2015 гг. инициативы «Миссия: умные города». Министерство жилищного строительства и городского развития Индии заявило о намерении создать не менее ста «умных» городов по всей территории страны. Город-государство Сингапур в 2015 году приступил к реализации стратегии «цифрового двойника» – «виртуального Сингапура» (Virtual Singapore), запустив инициативу Infocomm Media 2025 с целью создания собственной платформы для развития технологий, обеспечивающих устойчивое развитие, качественный экономический рост и повышение уровня жизни.

Обобщая опыт азиатских стран, можно сказать, что в их случае ключевыми элементами политики в области «умных» городских решений являются опора на государственные инициативы, стремление к наращиванию конкурентоспособности ведущих городов и оживлению городской экономики [48].

В Северной Америке ведущую роль в развитии «умных» городов играют США. Промышленная экосистема «умных» городов США в основном формируется из частных компаний. В 2009 году правительство США запустило программу поддержки инноваций, а в 2013 году «зеленый свет» получила инициатива Smart America Challenge. В 2015 году США выделили 160 миллионов долларов на проведение фундаментальных исследований и развитие 25 технологий в рамках инициативы Smart City Initiative. Два года спустя Министерство транспорта США запустило программу Smart City Challenge, ориентированную на создание транспортной системы, управляемой при помощи технологий данных и специализированных приложений, в интересах повышения мобильности пассажиров и товаров.

Американская модель развития «умных» городов опирается на инициативы частного сектора, направленные на рост мобильности и экономию энергии, а также широко использует возможности секторов экономики, производящих продукцию с высокой добавленной стоимостью [48].

В контексте политики по развитию «умных» городов все страны ЕС фокусируются на проблемах окружающей среды и транспорта. Так, в 2010 году была запущена программа Europe-2020, ориентированная на создание условий для устойчивого инклюзивного роста экономики; год спустя был дан старт Европейскому инновационному партнерству (Europe Innovation Partnership), приоритетами которого стали «умные» города и сообщества, использующие передовые цифровые, энергетические и транспортные технологии.

Стратегия имплементации плана по развитию «умных» городов и сообществ была представлена в 2013 году на конференции Smart City. В рамках инициативы Horizon 2020 на период с 2014 по 2020 годы на цели развития «умных» городов было выделено порядка 16 миллиардов евро. Евросоюз запустил также программу WiFi4EU, позволяющую органам местного самоуправления получать целевые гранты на сумму до 15 тысяч евро для развития местной цифровой инфраструктуры.

Таким образом, основные характеристики модели развития «умных» городов в странах ЕС в корне отличаются от американской и азиатской моделей; европейский подход основывается на государственно-частном партнерстве, приоритизации проблематики защиты окружающей среды и повышения мобильности, а также на обеспечении открытости данных.

Региональные модели развития «умных» городов существенно отличаются друг от друга, что обусловлено как историческими, культурными, экономическими и политическими факторами, так и особенностями поставленных целей общественного развития. Растущие

экономики Азии, такие как Китай и Индия, стремятся развивать «умные» города в интересах разрешения проблем городских агломераций с применением возможностей цифровых технологий и содействия экономическому росту, в то время как развитые страны региона – Япония, Южная Корея и Сингапур – реализуют программы развития «умных» городов как элемент подготовки к вызовам Четвертой промышленной революции и средство повышения конкурентоспособности своих городов для усиления внутренней и международной миграции; последняя модель развития опирается на широкое участие государства. Американская модель, напротив, предполагает более активное участие частного сектора, заинтересованного в развитии передовых производств в уже существующих современных городах. В Европейском союзе во главу угла ставятся задачи устойчивого развития и углубления партнерства между «умными» городами и сообществами.

Универсальных решений в области цифровой эволюции не существует. Каждая страна уникальна, поэтому детерминанты, обеспечившие успех одной экономики, могут не сработать в другой. Несмотря на это, изучение мирового опыта и конкретных политических решений, которые помогли ряду стран добиться того, что они имеют, – первый шаг для всех, кто заинтересован в обеспечении экономической безопасности своего государства за счет цифровизации.

#### **4.3. Направления повышения экономической безопасности предприятия в условиях цифровой трансформации**

В условиях конкуренции, изменчивости условий внешней среды необходимы как постоянная корректировка рыночной стратегии, так и значительные усилия по формированию эффективной стратегии экономической безопасности. В нестабильной рыночной среде предприятия (независимо от сферы деятельности) сталкиваются с необходимостью поиска принципиально новых подходов к обеспечению собственной экономической безопасности. При этом исключительно важной становится выработка стратегии долгосрочного развития, обеспечивающей адаптацию фирмы к изменчивой и не всегда дружественной рыночной среде. Однако на практике редко наблюдается полная или хотя бы частичная реализация компанией данного механизма управления, что связано с конфликтом интересов различных социальных, экономических и административных субъектов.

Усиливающаяся мировая конкуренция в технологической сфере приводит к сокращению инновационного цикла и устареванию бизнес-моделей. Процесс постоянного творчества и поиска конкурентных преимуществ создает возможности для новых участников и снижает барьеры для передачи технологий или инноваций, но в то же время способствует увеличению предпринимательских рисков и угроз для бизнеса. Это вызывает необходимость обеспечения безопасности и поиска новых экономических механизмов для предотвращения финансовых или социальных кризисов и реагирования на неблагоприятное влияние внешней бизнес-среды. Хозяйствующие субъекты должны быть в состоянии быстро адаптироваться к меняющимся условиям и использовать возможности для производства товаров или предоставления услуг новыми способами.

Цифровая трансформация – процесс перехода к цифровой экономике, реализуемый как экономическими отраслями, так и отдельными предприятиями с целью получения конкурентных преимуществ.

В зависимости от имеющихся возможностей и ресурсов стратегии управления экономической безопасностью предприятия в условиях цифровой трансформации могут быть направлены на реализацию планов роста и развития при условии компенсации или нивелирования деструктивных влияний и угроз либо на адаптацию и приспособление к угрозам с целью сохранения устойчивости предприятия. Помимо имеющегося внутреннего потенциала, возможностей и ресурсов предприятия, при выборе стратегии экономической безопасности большое значение имеют условия внешней деловой среды, сложившиеся в ней формы взаимодействия хозяйствующих субъектов, степень их кооперации и формы интеграции.

Применяя количественные стандартизированные оценки, рассчитанные на основе представленной выше матрицы (см. рис. 8), можно не только оценить уровень экономической безопасности предприятия, но и выбрать стратегию развития и обеспечения экономической безопасности предприятия на основе сравнения стандартизированных оценок риска и потенциала внешней и внутренней среды (рис. 16).

Если величина потенциала превосходит величину риска, то соответствующая среда будет предоставлять возможности для развития (уровень рисков можно считать низким). Когда же величина потенциала меньше, чем уровень риска, в соответствующей среде возникают значительные угрозы для развития хозяйствующего субъекта (высокий уровень риска).





Рис. 16. Координатная плоскость для выбора стратегии развития с учетом состояния экономической безопасности

Можно предложить четыре вида стратегии развития в зависимости от уровня экономической безопасности:

**А. Высокий уровень экономической безопасности предприятия** – предприятие обладает достаточным экономическим потенциалом и конкурентными преимуществами, чтобы обеспечить стабильное функционирование в краткосрочной перспективе и устойчивое развитие в долгосрочной. В этом случае применяется **стратегия роста**, которая состоит в поиске новых направлений эффективного использования возможностей внешней среды и сильных сторон предприятия.

Описанная стратегия может включать в себя различные виды роста и действия:

- 1) концентрированный рост за счет усиления позиции на рынке, совершенствования продукта и расширения рынка сбыта;
- 2) диверсифицированный рост, расширение видов деятельности и видов продукции;
- 3) интегрированный рост, предполагающий расширение фирмы за счет создания новых структур (путем приобретения собственности, расширения изнутри и т.п.);
- 4) реализацию долгосрочных инвестиционных проектов;
- 5) поиск новых рынков сбыта и технико-технологических решений и т.д.

**В. Низкий уровень экономической безопасности, обусловленный негативным воздействием факторов внешней среды** – высокий уровень внешних рисков и значительное негативное воздействие факторов внешней среды не позволяют фирме эффективно использовать

возможности для реализации имеющегося внутреннего потенциала. Обеспечение экономической безопасности предприятия в данных условиях связано с реализацией **стратегии адаптации**, позволяющей компании приспособиться к внешним угрозам (как макросреды, так и непосредственного окружения), используя, в зависимости от степени влияния факторов, различные ресурсы, составляющие экономической безопасности и структурные изменения на самом предприятии. При этом активизируется работа по мониторингу внешнего окружения. Возможные направления реализации стратегии могут быть связаны с удержанием позиций на рынке с помощью маркетинговых инструментов; поиском направлений повышения конкурентоспособности продукции; снижением цен за счет минимизации производственных затрат; повышением эффективности работы с поставщиками сырья и потребителями готовой продукции; проведением необходимых структурных и организационных изменений на предприятии.

**С. Критическое состояние экономической безопасности предприятия** – низкий уровень экономической безопасности предприятия обусловлен комплексным влиянием дестабилизирующих факторов внешней и внутренней среды, ошибками администрации; при этом предприятие не обладает достаточным потенциалом и ресурсами для нейтрализации негативного воздействия угроз внешней среды. В данных условиях компания ориентируется на **стратегию выживания**, связанную с поиском возможностей реагирования на внешние и внутренние угрозы и восполнения ресурсов за счет сокращения производственной деятельности, продажи части имущества, реструктуризации собственности или утраты самостоятельности в процессе интеграции.

Решение проблем обеспечения экономической безопасности в данном случае может включать в себя:

- 1) сокращение и оптимизацию расходов на производственную, маркетинговую деятельность, оплату труда работников, в том числе сокращение кадров;
- 2) прекращение или сокращение отдельных видов деятельности;
- 3) продажу активов или части имущества предприятия;
- 4) отказ от долгосрочных планов развития в пользу получения максимальных доходов в краткосрочной перспективе;
- 5) поиск возможностей горизонтальной интеграции с предприятием-партнером или конкурентом;
- 6) проведение процедуры самоликвидации или ликвидации компании.

Очевидно, что выбор стратегии развития зависит от наличия у предприятия достаточных объемов различных видов ресурсов, чтобы гарантировать решение задач по обеспечению экономической безопасности. Даже в ситуации, когда предприятие может самостоятельно нейтрализовать или устранить выявленные угрозы и опасности со стороны

внешней и внутренней среды, необходимо проведение упреждающих действий по предотвращению вероятных угроз. При этом изменение формы организации производства, кооперации и межотраслевой интеграции, появление новых рисков и угроз экономической безопасности определяют потребность в оценке влияния межхозяйственного и межотраслевого взаимодействия в рамках обоснования механизмов обеспечения экономической безопасности.

**Д. Низкий уровень экономической безопасности, обусловленный негативным воздействием факторов внутренней среды** – неудовлетворительным состоянием производственно-экономического потенциала предприятия, неэффективным использованием ресурсов и низким качеством управления.

Для анализа причин негативного влияния факторов внутренней среды требуются идентификация и оценка внутренних угроз. При этом наиболее целесообразным будет применение **стратегии укрепления потенциала**, сущность которой заключается в поиске внутренних резервов каждого структурного подразделения, разработке соответствующих мероприятий по их реализации и поиске направлений реализации дополнительных возможностей для развития предприятия за счет внешнего окружения, в том числе повышении эффективности управленческих решений; поиске направлений минимизации издержек на всех звеньях производства и резервов для более эффективного использования кадровых, финансовых и материальных ресурсов и интенсификации производственных возможностей предприятия; использовании конкурентных преимуществ для усиления позиций на рынке.

На основании выборки данных из информационных систем раскрытия информации можно оценить такие важные аспекты безопасности условий внешней среды, как уровень конкуренции и концентрации на рынке.

Предложенный ниже авторский инструментарий оценки уровня конкуренции и концентрации в деловой среде, основанный на использовании выборки данных из информационных систем раскрытия информации, позволяет сопоставить уровень конкуренции на конкретных рынках и взаимной зависимости доходности бизнеса основных стейкхолдеров. Он даст возможность оценить уровень концентрации рынка и корреляции средней доходности бизнеса в разрезе различных видов экономической деятельности, выбрать рациональные формы взаимодействия предприятий, повышающие их экономическую безопасность и обеспечивающие конкурентоспособность.

Координатная плоскость, представленная на рис. 17, отражает характер взаимосвязи между корреляцией доходности предприятий выбранного вида деятельности с предприятиями других видов

деятельности и уровнем концентрации рынка. Подобное представление позволяет соотнести стратегические преимущества от кооперации и интеграции в разрезе видов экономической деятельности по общероссийскому классификатору видов экономической деятельности.

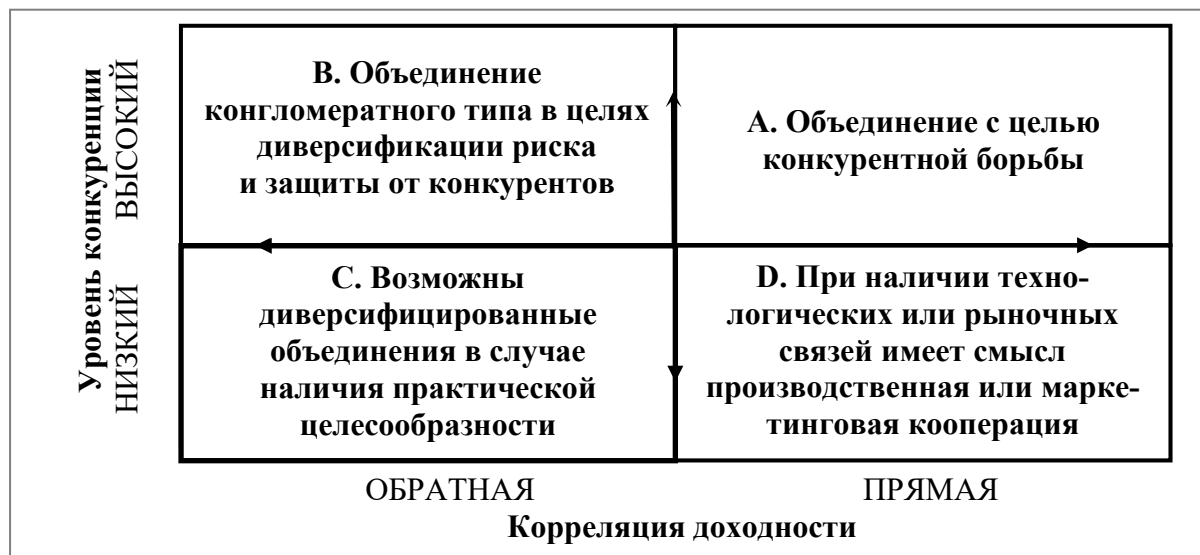


Рис. 17. Координатная плоскость для выбора формы интеграции или кооперативного взаимодействия

Степень зависимости средней доходности бизнеса в разных видах экономической деятельности измеряется с помощью коэффициента корреляции, а для оценки уровня конкуренции в конкретном виде экономической деятельности используется коэффициент концентрации Герфиндаля – Хиршмана (ННІ) в долях единицы. Чтобы привести оценки к единой размерности в диапазоне от  $-1$  до  $1$ , осуществляется пересчет оценок в разных границах измерения в единую шкалу. В итоге строится координатная плоскость в декартовой системе координат, которая позволяет оценить целесообразность применения различных форм интеграции или кооперации для предприятий разных видов экономической деятельности.

Если распределение переменных является нормальным или близким к нормальному, то для оценки уровня зависимости можно использовать коэффициент корреляции (в пределах от  $-1$  до  $1$ ), а для оценки уровня конкуренции – коэффициент концентрации Герфиндаля – Хиршмана (ННІ) в долях единицы. Чтобы привести оценки индекса ННІ к единой размерности в диапазоне от  $-1$  до  $1$ , можно воспользоваться предложенным автором приемом. Он заключается в пересчете оценок в разных границах измерения в единую шкалу за счет определения относительного разброса от стандартного значения, которое соответ-

ствуует нулевому значению и является пограничным между низкими и высокими оценками признака.

В качестве стандартного значения используем значение индекса Герфиндаля – Хиршмана, равное 0,2. Если  $HHI > 0,2$ , рынок будем рассматривать как высококонцентрированный, а при  $HHI < 0,2$  рыночная концентрация будет считаться ниже среднего уровня.

В этом случае формула для пересчета примет вид:

при  $HHI < \overline{HHI}$

$$K_{HHI} = \frac{\overline{HHI} - HHI_i}{\overline{HHI} - \min[HHI_i]};$$

при  $\overline{HHI} > HHI$

$$K_{HHI} = \frac{\overline{HHI} - HHI_i}{\max[HHI_i] - \overline{HHI}},$$

где  $K_{HHI}$  – оценка уровня концентрации рынка в диапазоне от –1 до 1;

$\overline{HHI}$  – пограничное значение индекса концентрации Герфиндаля – Хиршманна, равное 0,2;

$HHI_i$  – значение индекса концентрации Герфиндаля – Хиршмана для  $i$ -го признака:

$\min[HHI_i]$  – минимальное значение индекса из всех наблюдений;

$\max[HHI_i]$  – максимальное значение индекса из всех наблюдений.

В том случае, когда при высокой рыночной концентрации и сильной конкуренции на исследуемых рынках наблюдается прямая зависимость между средним уровнем доходности организаций разных видов экономической деятельности, их объединение может дать дополнительные преимущества в конкурентной борьбе (квадрант А).

В ситуации, при которой в условиях высокой конкуренции корреляция между доходностью организаций отрицательная, преимущества от диверсифицированной интеграции могут быть связаны с диверсификацией риска. Диверсифицированные структуры (конгломераты), объединенные за счет финансовых интеграционных механизмов без каких-либо технологических связей, дадут возможности внутригруппового маневрирования финансовыми ресурсами и снижения уровня транзакционных издержек (квадрант В).

При низком уровне конкуренции в сочетании с обратной корреляцией доходности преимущества от объединений конгломератного типа возможны за счет диверсификации рисков интегрированной структуры, но целесообразность объединений подобного типа оценивается на основе соотнесения издержек и выгод от интеграции в данной ситуации (квадрант С).

В условиях низкоконцентрированных рынков и прямой корреляции между доходностью в разных видах экономической деятельности целесообразность производственной, маркетинговой кооперации или создания сетевых структур зависит от наличия технологических или рыночных связей между предприятиями (квадрант D).

Хотя цифровая трансформация открывает новые возможности для повышения эффективности обеспечения безопасности предприятия, она приводит также и к возникновению новых угроз.

Для устранения данных проблем авторами на основе проведенных исследований был разработан ряд направлений совершенствования системы обеспечения экономической безопасности предприятия:

учет в системе безопасности специфических технологических, финансовых, организационно-управленческих, кадровых факторов деятельности организации;

использование предупредительных мер для прогнозирования угроз, адаптации деятельности предприятия к изменениям во внутренней и внешней среде;

координация деятельности (объединения усилий) службы безопасности и правоохранительных органов с целью снижения уровня угроз и эффективного противодействия существующим угрозам;

расчет экономической целесообразности противодействия вызовам и угрозам;

профессиональный аудит безопасности, направленный на ликвидацию просчетов в обеспечении безопасности;

оценка и реализация цифровых проектов в области обеспечения экономической безопасности (при этом отсутствует уверенность в «правильном» подходе и велика вероятность ошибки);

активизация деятельности «агентов трансформации».

Как отмечают А.И. Рудской, А.И. Боровков, П.И. Романов, О.В. Колосова [58], для России характерны специфические риски цифрового перехода. В частности, к ним относятся:

дефицит актуальных практических знаний и навыков;

проблематичность создания единого образовательного пространства;

цифровое неравенство;

низкая мотивация к получению непрерывного образования;

необходимость коренной перестройки всей системы академического образования.

Важнейшим фактором успешной цифровизации является обеспечение информационной грамотности населения, а также повышение его мотивации к самообразованию, активному использованию систем дистанционного обучения и других способов получения образования, доступных на текущий момент.

Задачу обеспечения рынка труда специалистами в IT-сфере государство намерено решить посредством инициатив, предусмотренных федеральными проектами «Кадры для цифровой экономики» и «Развитие кадрового потенциала IT-отрасли» национальной программы «Цифровая экономика».

По оценкам заместителя председателя Правительства Российской Федерации Д. Чернышенко, дефицит IT-кадров в России на данный момент оценивается в один миллион человек. К 2027 году эта цифра может удвоиться<sup>11</sup>. В 2022 году на реализацию национального проекта «Цифровая экономика» планируется направить 210,7 миллиарда рублей<sup>12</sup>. Динамика бюджетных ассигнований на финансовое обеспечение реализации федерального проекта «Кадры для цифровой экономики» представлена на рис. 18.

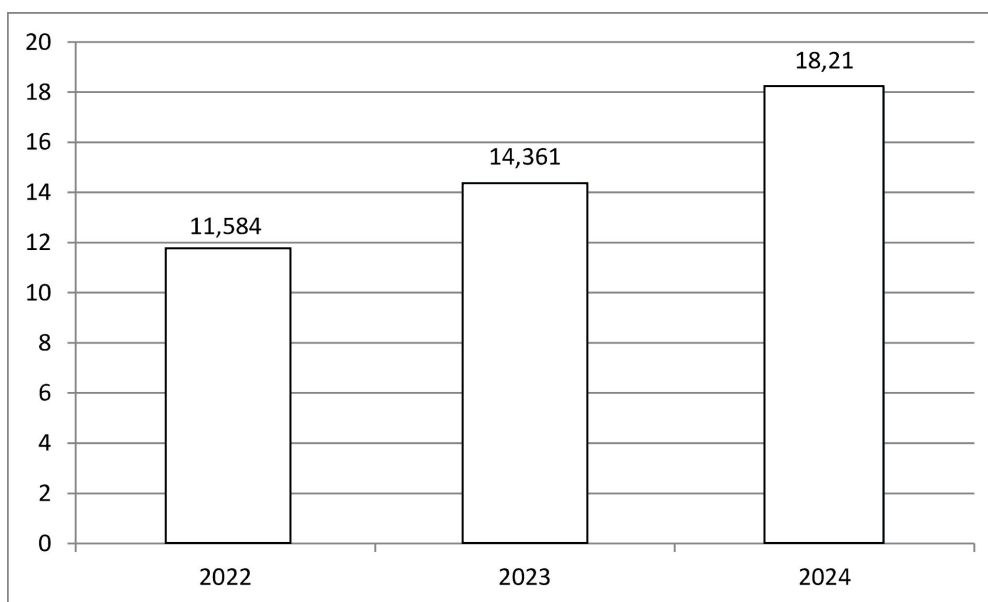


Рис. 18. Динамика бюджетных ассигнований (миллиардов рублей) на финансовое обеспечение реализации федерального проекта «Кадры для цифровой экономики»

Реализация указанных федеральных проектов уже позволила добиться некоторых успехов. Так, по данным Института статистических исследований и экономики знаний НИУ ВШЭ, в 2020 году в профессиях, связанных с ИКТ, было занято 9,2 миллиона человек, что на 6 % больше,

<sup>11</sup> В погоне за кадрами: как Россия готовит специалистов для IT-отрасли. URL: <https://digital.ac.gov.ru/news/5553> (дата обращения: 17.01.2023).

<sup>12</sup> На нацпроект «Цифровая экономика» в 2022 году направят 210,7 млрд рублей. URL: <https://tass.ru/ekonomika> (дата обращения: 17.01.2023).

чем в 2019 году<sup>13</sup>. При этом, по данным экспертов НИУ ВШЭ<sup>14</sup>, доля IT-сектора в российском ВВП составляет менее 1 %. В целом развитию сектора мешают устаревшее профильное образование и дефицит преподавателей для подготовки IT-кадров.

Одной из основных проблем, связанных с подготовкой кадров для цифровой экономики, является повышение качества образования на основе сохранения его фундаментальности и удовлетворения текущих и перспективных потребностей личности, общества и государства. Сегодня качественное образование определяет конкурентоспособность как отдельных вузов, так и национальной системы образования в целом. Чтобы повышать свое качество, система образования должна быстро реагировать на вызовы времени. Решение проблемы качественного образования зависит от своевременного и адекватного реагирования системы образования на потребности общества, изменения внешней среды, общественного строя. Необходимо определить эффективные методы и технологии, соответствующие этим изменениям и потребностям.

Для оценки кадрового потенциала подразделений, ответственных за цифровую среду высших учебных заведений, специалисты НИУ ВШЭ ежемесячно освещают основные проблемы в бюллетене «Мониторинг экономики образования» [36]. Они отмечают, что если в 2017–2020 годах количество IT-специалистов увеличилось на 14,2 %, то в сфере образования наблюдается противоположная тенденция – их численность сократилась на 13,6 %. При этом на их долю приходится всего 2,3 % от общего числа занятых в образовании. Из-за отмечаемого недостатка IT-специалистов на рынке труда вузам приходится бороться с IT-компаниями за высококвалифицированные кадры. Однако из-за ограниченного бюджета вузы оказываются неконкурентоспособны.

Частично справиться с данной проблемой позволяет практика приема на работу в ИКТ-блок собственных выпускников. Кроме того, руководители вузов повышают квалификацию своих работников – либо самостоятельно внутри подразделения, либо направляя работников на курсы, дополнительное обучение.

Существует пространственная неравномерность развития цифровой среды вузов. Так, в Москве обеспеченность вузов ИКТ-специалистами почти на треть выше по сравнению с другими регионами. Таким образом, столичная агломерация более обеспечена работниками этой группы [36]. Имеет значение и статус вуза – ведущие учебные заведения в гораздо большей мере обеспечены кадрами.

---

<sup>13</sup> Информационные технологии: проблемы подготовки кадров. URL: <http://www.vscs.ac.ru/activity/view?id=62593> (дата обращения: 17.01.2023).

<sup>14</sup> Фаляхов Р. Исчезающе мал: что мешает развиваться российскому IT-сектору. URL: <https://www.gazeta.ru/business> (дата обращения: 17.01.2023).



Академический рынок труда традиционно достаточно иерархичен. Наиболее многочисленную возрастную группу среди профессорско-преподавательского состава российских вузов составляют лица в старшем пенсионном возрасте (19,5 %), доля работников в возрасте от 50 до 65 лет – порядка 30 %. С другой стороны, сегодня утверждены новые требования ко всем педагогическим работникам в области владения средствами ИКТ. В этой связи будем объективны: многие представители данной возрастной группы нуждаются в повышении квалификации и переподготовке.

Отчасти именно указанным обстоятельством можно объяснить крайне низкий процент использования в учебном процессе инструментов электронной информационно-образовательной среды вуза. Так, согласно проведенному НИУ ВШЭ опросу представителей 325 российских вузов, большинство респондентов (57,7 % в Москве и 70,6 % в других регионах) согласились с утверждением, что внедрение новых цифровых сервисов встречает сопротивление со стороны преподавателей и студентов. Старший научный сотрудник Центра экономики непрерывного образования РАНХиГС А. Тищенко связал это прежде всего с преклонным возрастом преподавателей. Как правило, они не имеют навыка работы с цифровыми решениями. По мнению 60,1 % опрошенных преподавателей, цифровизация образовательного процесса может привести к вытеснению их коллег – представителей старшего поколения [47].

На наш взгляд, на данный момент в концепции непрерывной, комплексной, многоуровневой и многопрофильной подготовки ИКТ-специалистов недостаточное внимание уделено системе среднего профессионального образования. При этом на производстве, как правило, требуются специалисты не по разработке информационных систем, а по их внедрению, эксплуатации, поддержанию в рабочем состоянии [57].

Подготовка IT-кадров в системе среднего профессионального образования предъявляет особые требования к материально-техническому оснащению колледжей и техникумов. Цифровизация здесь в определенной мере сдерживается финансовыми возможностями. Педагогов, нуждающихся в специализированном программном обеспечении для работы, больше по сравнению с теми, кто имеет к нему доступ. Чаще всего имеются проблемы с научным оборудованием и приборами (их нехватку отметили 11,7 % педагогов, а 13,7 % заявили о плохом состоянии), а также с тренажерами и симуляторами (7,9 и 16,9 % соответственно) [43].

Все названное в очередной раз подтверждает наличие проблемы цифрового неравенства, что особенно ярко проявилось в период ограничений, введенных на фоне пандемии коронавируса. Цифровое неравенство – это ограничение возможностей социальной группы из-за отсутствия у нее доступа к современным средствам коммуникации. По

данным Росстата (исследование проводили среди 60 тысяч домохозяйств), в конце 2020 года доступа к интернету не имели 28,6 % семей, компьютера не было у 38,3 %. Примерно четверть из них (24,6 и 29,8 %) хотели бы приобрести и то и другое, но испытывали нехватку средств. Самый сильный цифровой разрыв характерен для деревень с численностью населения до 200 и до 1 000 человек. Здесь доступ к интернету имеют 48,5 и 49,7 % семей соответственно<sup>15</sup>.

Существуют сложности и с нормативно-правовым обеспечением ИТ-сектора. Так, из более чем 3 000 действующих международных ИТ-стандартов отечественным специалистам доступно не более 5 % – это те, которые переведены на русский язык и приведены к уровню ГОСТ Р. Остальные 95 %, как правило, недоступны специалистам и преподавателям. Постепенно появляются и собственные разработки. Следовательно, требуется интенсифицировать подготовку и пере-подготовку кадров в этой области. В первую очередь нужно готовить соответствующий преподавательский состав<sup>16</sup>.

Необходимо понимать, что подготовка квалифицированных специалистов – задача не одного дня. Нужно не только обучить – важен также опыт работы. К сожалению, в ряде случаев отсутствует понимание того, что выпускник вуза зачастую должен еще несколько лет отработать, чтобы стать квалифицированным специалистом. Решить данную проблему можно только посредством взаимодействия ИТ-компаний и вузов, осуществляемого в виде стажировок и производственных практик для студентов, проведения научных исследований, разработки учебных планов и т.д.

На сегодняшний день российская система подготовки кадров довольно консервативна, недостаточно мобильна и гибка, работает не на рынок труда, что проявляется в следующем:

- 1) текущий перечень специальностей не соответствует вызовам цифровой экономики и процессам информатизации;
- 2) доля направлений подготовки, связанных с ИТ, в общем объеме всех специальностей крайне мала как на федеральном, так и на региональном уровне;
- 3) в подготовке ИТ-специалистов отсутствует системный подход;
- 4) лучшими вузами в сфере подготовки ИТ-кадров, а также вузами, активно сотрудничающими с ИТ-компаниями, являются университеты Москвы и Санкт-Петербурга. Такая локализация свидетельствует о

---

<sup>15</sup> Интернет как роскошь: что такое цифровое неравенство и как его преодолеть. URL: <https://trends.rbc.ru/trends> (дата обращения: 17.01.2023).

<sup>16</sup> Общие вопросы подготовки кадров в области ИТ стандартизации. URL: <https://www.cksit-rspp.ru/products/369/461/> (дата обращения: 17.01.2023).

неравномерном развитии кадрового потенциала в сфере ИТ и высокой концентрации ИТ-специалистов в крупных городах<sup>17</sup>.

Требуется развивать компетенции, которые будут востребованы в следующем десятилетии. Квалификации выпускников устаревают быстрее, чем успевает отреагировать классическая система образования. Для устранения этого разрыва требуется переключение модели образования с проектно-ориентированного обучения на экспериментально-ориентированное; трансфер практических навыков должен обеспечиваться не только за счет стажировок, но и через создание базовых кафедр и распространение специализированных учебных лабораторий.

Использование в образовании информационных технологий, в том числе больших данных, ИИ, разного рода нейротехнологий, приводит к изменению характера получения знаний и предоставления образовательных услуг в целом. Особую значимость в этой связи приобретает формирование единого образовательного пространства, обеспечивающего идентификацию глобальных целей будущего самосохраняющегося общества, сберегающего ресурсы планеты, через ценностно-ориентированное обучение и воспитание. Формирование единого глобального коммуникационного поля и развитие сектора ИКТ способствуют обогащению процесса образования инструментарием интерактивных форм обучения [58].

Программное обеспечение является неотъемлемой составляющей активов хозяйствующего субъекта любой формы собственности, в том числе государственной. В условиях импортозамещения все секторы экономики должны осуществить переход на отечественные цифровые инструменты, причем если частные организации могут сделать это посредством смены поставщика программного продукта, то в отношении государственных объектов необходимо учитывать специфику их функционирования и, в частности, финансирования их деятельности.

Процесс импортозамещения, как следует из самого понятия, представляет собой замену импорта национальными товарами, произведенными внутри страны. С особой остротой эта потребность проявилась в 2014 году на фоне первых санкций, введенных зарубежными партнерами в ответ на действия России по отношению к Украине. Именно тогда Президентом РФ был подписан Федеральный закон № 188-ФЗ от 29 июня 2015 года, в котором, в частности, говорилось о необходимости создания и ведения реестра отечественного программного

---

<sup>17</sup> Информационные технологии: проблемы подготовки кадров. URL: <http://www.vscs.ac.ru/activity/view?id=6259> (дата обращения: 17.01.2023).

обеспечения<sup>18</sup>. В ноябре того же года было утверждено Постановление Правительства РФ № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», которое, в частности, ограничивало возможности госзаказчиков в вопросах закупки программного обеспечения<sup>19</sup>. В частности, был прописан порядок формирования и ведения единого реестра российских и евразийских программ для электронных вычислительных машин и баз данных. На данный момент в нем насчитывается более 12 тысяч продуктов.

Переход федеральных органов исполнительной власти и государственных внебюджетных фондов к использованию отечественного офисного программного обеспечения (в соответствии с Распоряжением Правительства РФ от 26 июля 2016 года № 1588-р) должен был быть завершён к 2018 году, но впоследствии сроки перехода на преимущественное использование отечественного программного обеспечения были перенесены на 2021 год [12].

Согласно целевым показателям, приведенным в паспорте национальной программы (нацпроекта) «Цифровая экономика Российской Федерации», стоимостная доля закупаемого или арендуемого органами власти отечественного программного обеспечения должна расти на 5 % ежегодно и с 2020 года по 2024-й увеличиться с 70 до 90 %. Для государственных корпораций и компаний с госучастием данный показатель должен вырасти с 2020 года по 2024-й с 50 до 70 %.

Тем не менее, по оценке члена правления Ассоциации разработчиков программных продуктов «Отечественный софт» председателя совета директоров компании «АСКОН» А. Голикова, на данный момент доля отечественного софта, используемого в государственных корпорациях и госсекторе, не превышает 30 %<sup>20</sup>. Отчасти это обусловлено и тем фактом, что крупные компании с государственным участием и государственные органы власти сопротивляются данному переходу. В этой связи показательным является судебный процесс между Министерством

---

<sup>18</sup> О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. Российская Федерация. Закон. URL: <http://www.kremlin.ru/acts/bank/39838>. (дата обращения: 17.01.2023).

<sup>19</sup> Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд. Российская Федерация. Постановление. URL: <https://base.garant.ru/71252170/> (дата обращения: 17.01.2023).

<sup>20</sup> Шувалова М. Импортозамещение в сфере ИТ. URL: <https://www.garant.ru/article/1542142/> (дата обращения: 17.01.2023).

строительства и жилищно-коммунального хозяйства Российской Федерации (Минстрой РФ) и ООО «Новые облачные технологии» (российский разработчик офисного программного обеспечения «Мой Офис»)<sup>21</sup>. Так, в сентябре 2016 года был заключен контракт на поставку программного обеспечения Microsoft между Минстроем РФ и ООО «Геокэпитал». ООО «Новые облачные технологии» просило суд признать, что при проведении электронного аукциона Минстрой РФ нарушил Федеральный закон № 44-ФЗ о контрактной системе, а также положения постановления Правительства РФ о запрете на допуск иностранного программного обеспечения при госзакупках. Разбирательство носило прецедентный характер: суд впервые оценивал законность отказа от российского программного обеспечения.

Оставляя за рамками перипетии данного судебного разбирательства, выделим ключевые моменты:

справедливость обоснования невозможности закупки отечественного программного обеспечения требует не только и не столько проведения оценки с формально-юридической, сколько с технической точки зрения;

судебная практика по таким делам отсутствует;

невозможность использования приведенного в реестре отечественного программного обеспечения (в частности, пакета «Мой Офис») связана с тем, что оно работает под операционной системой Linux (что, однако, не в полной мере соответствует действительности);

уже установленные офисные приложения обладают необходимым функционалом, а также полной совместимостью с имеющимся программным обеспечением заказчика.

На наш взгляд, последний довод наиболее наглядно отображает возникшее противоречие между «навязанной сверху» необходимостью перехода на отечественное ПО и естественным нежеланием становиться первопроходцем.

Среди других проблем импортозамещения программного обеспечения на объектах государственного сектора выделим:

отсутствие полноценных отечественных аналогов для некоторых зарубежных решений;

отсутствие комплексных архитектур и решений для замещения сформировавшихся годами экосистем корпоративного программного обеспечения;

обратную совместимость отечественных IT-продуктов с иностранными технологиями;

недостаточное финансирование со стороны государства;

---

<sup>21</sup> Суд объяснил на примере Минстроя, как можно закупать иностранное ПО в обход российских альтернатив. URL: <https://www.tadviser.ru> (дата обращения: 17.01.2023).

дефицит квалифицированных разработчиков программного обеспечения;

консерватизм заказчика;

отсутствие необходимого функционала у отечественного программного обеспечения;

нехватку перспективных российских IT-стартапов, создающих инновационные продукты, а не клонирующих уже имеющиеся решения;

административные барьеры (отсутствие единых стандартов, запутанные алгоритмы получения необходимых сертификатов).

В складывающейся на данный момент ситуации очевидно, что процесс импортозамещения в сфере IT необходимо ускорить.

Во-первых, юридические лица, перечисленные в Федеральном законе от 18 июля 2011 года № 223-ФЗ (за исключением муниципальных), с 31 марта 2022 года не могут закупать иностранное программное обеспечение для использования на принадлежащих им значимых объектах критической информационной инфраструктуры без согласования с уполномоченным Правительством РФ.

Во-вторых, на данный момент ситуация осложняется тем обстоятельством, что уход производителей программных средств с территории России произошел не только в ответ на протекционистские методы регулирования со стороны государства, но и согласно с их волеизъявлением.

Таким образом, несмотря на наличие значительного количества нормативно-правовых актов в области импортозамещения программного обеспечения на объектах государственного сектора, наличие организационных, технических, кадровых, финансовых ограничений сдерживает темпы отказа от иностранного софта<sup>22</sup>.

Ужесточение налогового администрирования и рост собираемости налогов заставляют налогоплательщиков искать новые способы снижения налоговой нагрузки. При этом применяются различные методы снижения налогового бремени – как налоговые льготы, так и пробелы в фискальном законодательстве. Используются и незаконные способы уклонения от налогов и иных обязательных платежей, нарушаются сроки и полнота их уплаты.

Законное уменьшение платежей по налогам в рамках действующего законодательства путем оптимизации осуществляется на основе льгот, которые предоставляет государство, выстраивания налоговых схем и грамотного составления договоров. При этом оптимизация налогообложения не сводится к простой минимизации налоговых платежей; помимо снижения размера налоговых платежей, ее инструментами

---

<sup>22</sup> Шувалова М. Импортозамещение в сфере IT. URL: <https://www.garant.ru/article/1542142/> (дата обращения: 17.01.2023).

являются отсрочка уплаты налогов, уменьшение суммы выплачиваемых в бюджет средств за счет снижения налогооблагаемой прибыли и т.д. Налоговая оптимизация, направленная на минимизацию расходов бизнеса в рамках закона, помогает выживанию предприятий в условиях агрессивной деловой среды и способствует обеспечению их экономической безопасности.

Незаконные схемы налоговой оптимизации связаны с фиктивными сделками и схемами уклонения от уплаты налогов, в том числе с фальсификацией документов и искажением сведений о фактах хозяйственной жизни.

В целях улучшения ситуации актуально формирование комплекса организационных и правовых мер по предупреждению, контролю, пресечению ухода от налогообложения и совершенствованию нормативно-правовой базы до уровня, при котором возможность нахождения законных путей неуплаты налогов будет сведена к минимуму. Важнейшую роль здесь играет повышение степени открытости финансовой информации о деятельности организаций, формирование в обществе налоговой культуры и морали.

Представляется, что система мер в области налогообложения, направленная на повышение защиты бизнеса в условиях цифровизации, предполагает организацию эффективного взаимодействия бизнеса с надзорными органами.

Ключевые проблемы бизнеса и налоговых органов и организационные методы их решения представлены на рис. 19.

Принявшие участие в опросе предприниматели настаивают на необходимости организации эффективного взаимодействия власти, надзорных органов и бизнеса, конструктивного диалога и решения сложившихся проблем.

Среди прочих мер, направленных на организацию эффективного взаимодействия бизнеса и надзорных органов, представители бизнеса предложили ввести дифференцированный риск-ориентированный подход к налогообложению бизнеса. Это может проявляться как в налоговых льготах для предприятий, длительно существующих на рынке, не замеченных в нарушении существующих норм и правил налогового законодательства и являющихся добросовестными налогоплательщиками, так и в дифференцированных налоговых ставках.

Представляется, что введение системы премий и льгот добросовестным налогоплательщикам позволит не только ускорить темпы собираемости налогов, но и повысить уровень доверия между налоговыми органами и налогоплательщиками.



Рис. 19. Методы решения проблем при взаимодействии налоговых органов с хозяйствующими субъектами

Хорошим стимулом для развития компаний может стать льготное налогообложение прироста доходов. Представляется, что подобная мера позволит сократить количество случаев применения налогоплательщиками различных схем уклонения и повысит вероятность применения законодательно разрешенных способов снижения налоговой нагрузки. При этом целесообразно усиление ответственности и контроля за целевым использованием денежных средств, высвобождаемых при применении льготных условий налогообложения (например, применение ускоренной амортизации должно быть возможно только в случае инвестирования накопленных средств амортизационного фонда в закупку нового оборудования, модернизацию производства).

Отметим, что преимущество системы налоговых преференций по сравнению с выдачей единовременных субсидий состоит в том, что финансовые потери бюджетной системы в текущем периоде компенсируются ростом налоговой базы, при этом улучшается предпринимательский климат.



В ближайшее время наша страна, благодаря достигнутому соглашению между Правительством Российской Федерации и Банком России о регулировании цифрового актива, может стать одним из государств, признавшим криптовалюту денежной единицей, платежным средством. В то же время в связи с тем, что на указанный вид валюты не распространяются традиционные финансовые гарантии, необходимо принять пакет законов в области защиты прав потребителей и обеспечения безопасности и надежности финансовой системы. 1 января 2021 года в России вступил в силу Федеральный закон № 259-ФЗ от 31 июля 2020 года «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», регулирующий отношения, связанные с оборотом цифровых финансовых активов [10]. При этом под цифровыми финансовыми активами понимаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов» [10].

Тем не менее в Федеральном законе «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» имеется противоречие: с одной стороны, в нем содержится определение криптовалюты и тем самым она легализуется, с другой – этим законом запрещается использование ее в России в качестве средства платежа.

В соответствии с данным нормативно-правовым актом цифровая валюта понимается как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей и (или) в качестве инвестиций» [10].

Предложенная законодателем трактовка универсальна и применима не только в отношении криптовалюты. В настоящее время на рассмотрении в Государственной Думе РФ находится законопроект № 1065710-7 «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации (в части налогообложения цифровой валюты)» [1], принятый во втором чтении 13 октября 2021 года. Он определяет механизм налогообложения и декларирования цифровых валют. При этом ключевыми являются следующие положения:

цифровая валюта признается в качестве объекта налогообложения<sup>23</sup>; сведения об операциях с цифровыми валютами при годовом обороте более 600 000 рублей подлежат обязательному декларированию;

налоговые органы имеют право истребовать у банков информацию по операциям физических лиц с цифровыми валютами.

В законопроекте описан порядок подачи отчетности об операциях и остатках цифровых валют, оговорены меры наказания за непредоставление в налоговые органы соответствующей информации и неуплату налогов по операциям с цифровыми валютами.

Цифровые финансовые активы регулируются в соответствии с нормами, принятыми в международной практике. Например, в России планируется осуществлять контроль за операциями с цифровыми финансовыми активами не в рамках налоговых проверок, а на основе регулярных запросов банков (так обычно контролируются указанные операции в США).

Конечно, есть и ряд особенностей, характерных для норм отечественного права. Так, например, планируется введение уголовной ответственности в случае, если обладатель криптовалюты не предоставил информацию о владении активами. Министерство финансов РФ предлагает обязать граждан декларировать проведенные в цифровой валюте операции, за исключением граждан, находящихся на территории страны менее 183 дней. В частности, налогообложению подлежат операции с цифровыми валютами, проходящие через счета российских банков и служащие основанием для определения налоговой базы и расчета налоговых обязательств. Как в Налоговом, так и в Гражданском кодексе РФ цифровая валюта в качестве отдельного объекта регулирования по-прежнему не указана.

В Налоговом кодексе предлагается признать цифровую валюту имуществом. При этом вводимое понятие противоречит подходу, реализованному в Федеральном законе № 259-ФЗ от 31 июля 2020 года. В частности, цифровая валюта не рассматривается как вид платежного средства, поэтому ограничивается ее использование в качестве инструмента расчетов<sup>24</sup>.

Необходимость налогообложения операций с цифровыми финансовыми активами напрямую вытекает из Письма Минфина России от 24 августа 2020 года № 03-03-06/1/73953. В частности, в нем говорится,

---

<sup>23</sup> Налогообложение цифровых активов в России: теория и практика. URL: <https://bits.media/nalogooblozhenie-tsifrovyykh-aktivov-teoriya-i-praktika/> (дата обращения: 17.01.2023).

<sup>24</sup> Налогообложение цифровых активов в России: теория и практика. URL: <https://bits.media/nalogooblozhenie-tsifrovyykh-aktivov-teoriya-i-praktika/> (дата обращения: 17.01.2023).

что логика положений главы 25 Налогового кодекса РФ подразумевает налогообложение всех доходов, полученных налогоплательщиком при осуществлении деятельности, за исключением поименованных в статье 251 НК РФ. Поскольку в главе 25 НК РФ отсутствует особый порядок налогообложения доходов, полученных при совершении операций с криптовалютой, указанные доходы налогоплательщика учитываются при определении налоговой базы по налогу на прибыль в общем порядке.

Таким образом, для физических лиц ставка налога назначается в размере 13 % от суммы полученного дохода и 15 % на доход, превышающий пять миллионов рублей в год. Юридические лица уплачивают налог на прибыль организаций по ставке 20 %, при этом уменьшение налогооблагаемой базы на сумму амортизационных отчислений не производится<sup>25</sup>. Довольно проблематичным на данный момент является вопрос о признании расходов, уменьшающих налогооблагаемые доходы по операциям с криптовалютой.

Для признания расходов при формировании налогооблагаемой базы как по налогу на прибыль, так и по налогу на доходы физических лиц необходимо наличие первичных документов на покупку цифровых финансовых активов или их создание.

Как отмечалось выше, проектом федерального закона предусматривается установление налоговой ответственности за неправомерное непредставление (несвоевременное представление) отчетности или представление отчета об операциях (гражданско-правовых сделках) с цифровой валютой и об остатках указанной цифровой валюты, содержащего недостоверные сведения [1]:

неуплата или неполная уплата налогоплательщиком сумм налога в результате невключения в налоговую базу прибыли (доходов) от операций, расчеты по которым осуществлялись с использованием цифровой валюты, влечет взыскание штрафа в размере 40 % от суммы неуплаченного налога в части таких операций;

неправомерное непредставление в установленный срок лицом в налоговый орган сообщения о получении права распоряжаться, в том числе через третьих лиц, цифровой валютой, отчета об операциях с цифровой валютой и об остатках цифровой валюты влечет взыскание штрафа в размере 50 000 рублей;

неправомерное непредставление лицом в налоговый орган отчета об операциях с цифровой валютой и об остатках цифровой валюты или представление отчета об операциях с цифровой валютой и об остатках цифровой валюты, содержащего недостоверные сведения,

---

<sup>25</sup> Налогообложение цифровых активов в России: теория и практика. URL: <https://bits.media/nalogooblozhenie-tsifrovyykh-aktivov-teoriya-i-praktika> (дата обращения: 17.01.2023).

влечет взыскание штрафа в размере 10 % от наибольшей из двух сумм в рублевом эквиваленте – суммы поступления цифровой валюты лицу или суммы списания цифровой валюты лицом, которое вправе распоряжаться (в том числе через третьих лиц) этой цифровой валютой.

В настоящее время обсуждается законопроект «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации», предусматривающий ответственность за уклонение от обязанности декларировать сведения об операциях, связанных с использованием цифровой валюты, а также то, что совершение преступления с использованием цифровой валюты является обстоятельством, отягчающим наказание.

Масштабное распространение цифровых финансовых активов и расширение числа экономических субъектов, использующих их, привело к необходимости законодательного регулирования этих активов как в части отражения в бухгалтерском учете, так и в части признания в качестве объекта налогообложения. Нормативно-правовое обеспечение признания и налогообложения операций с цифровыми финансовыми активами требует детальной и тщательной проработки. Тот факт, что криптовалюта нередко используется для легализации (отмывания) денежных средств, еще раз подтверждает актуальность рассмотренных вопросов.

Таким образом, политика государства выступает основой для обеспечения экономической безопасности бизнеса. Решение проблем, возникающих в ходе цифровой трансформации, как и уменьшение цифрового неравенства, требует разработки комплекса организационных и нормативно-правовых мер, направленных на устранение угроз безопасности и стимулирование цифрового развития бизнеса.

## ЗАКЛЮЧЕНИЕ

В монографии выполнено исследование влияния цифровизации на экономическую безопасность бизнеса и разработаны новые аналитические инструменты идентификации рисков и оценки стратегических преимуществ компании при использовании дополнительных функциональных возможностей цифровой экономики и современных информационных систем.

Наряду с традиционными методами научного анализа, экономической и математической статистики, в работе реализуются методологические приемы, основанные на применении новых аналитических инструментов. Используются возможности фильтрации информации современных баз данных и систем раскрытия информации, поиска подмножества данных и последующей работы с выборками, сформированными на основании заданных условий; приемы графического моделирования в декартовой системе координат позволяют отобразить результаты оценки в наглядном и удобном для восприятия и интерпретации виде.

Авторами доказано, что цифровизация открывает дополнительные функциональные возможности для хранения, раскрытия и анализа информации о состоянии рынка в целом и отдельных его участников. Предложены новые методологические подходы для оценки уровня рисков и стратегического анализа деятельности компании. Авторские методики реализованы с помощью использования поисковых возможностей и функционала работы современных информационных систем.

Предложенный инструментарий позволяет выбрать стратегию повышения экономической безопасности и конкурентоспособности предприятия, идентифицировать риски, внешние и внутренние угрозы, с тем чтобы обосновать комплекс конкретных мер по использованию конкурентных преимуществ в управлении рисками компании.

Анализируя роль цифровизации в обеспечении экономической безопасности, авторы выделили следующие основные направления обеспечения экономической безопасности в условиях развития цифровой экономики:

1. Повышение конкурентоспособности компаний, работающих в сфере информационных технологий и электронной промышленности.

2. Устранение зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, разработки и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе.

3. Инновационное развитие информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны.

Исходя из вышеуказанного, можно сформулировать основные стратегические цели цифровой трансформации в концепции экономической безопасности:

инновационное развитие системы защиты информации, информационных технологий и электронной промышленности;

создание и внедрение информационных технологий, изначально устойчивых к различного рода угрозам;

проведение исследований и опытно-конструкторских работ с целью создания перспективных информационных технологий и средств;

повышение безопасности информационной инфраструктуры и стабильности ее функционирования, разработка механизмов обнаружения и предотвращения информационных угроз, а также ликвидации последствий их проявления;

совершенствование методов и способов производства и безопасного использования продукции, оказание услуг на основе информационных технологий с использованием разработок, отвечающих требованиям безопасности.

Современные информационные технологии, с одной стороны, позволили обеспечить информационно-эмпирическую базу исследования. С другой стороны, использование современных информационных технологий и методик работы с базами данных, а также программных средств обработки экономической информации дает возможность реализовать на практике предложенный авторами инструментарий и повысить достоверность полученных результатов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации (в части налогообложения цифровой валюты): Законопроект № 1065710-7. URL: <https://sozd.duma.gov.ru/bill/1065710-7> (дата обращения: 01.02.2023).

2. О государственной стратегии экономической безопасности Российской Федерации (Основных положениях): указ Президента РФ от 29 апреля 1996 года № 608 // Собрание законодательства РФ. 1996. № 18. Ст. 2117.

3. О государственном регулировании внешнеторговой деятельности: Федер. закон от 13 октября 1995 года № 157-ФЗ (ред. от 10.02.1999) // Собрание законодательства РФ. 1995. № 42. Ст. 3923.

4. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента РФ от 7 мая 2018 года № 204 // Собрание законодательства РФ. 2018. № 20. Ст. 2817.

5. О национальных целях развития Российской Федерации на период до 2030 года: указ Президента Российской Федерации от 21 июля 2020 года № 474 // Собрание законодательства РФ. 2020. № 30. Ст. 4884.

6. О Стратегии научно-технологического развития Российской Федерации: указ Президента РФ от 1 декабря 2016 года № 642 // Собрание законодательства РФ. 2016. № 49. Ст. 6887.

7. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 2 июля 2021 года № 400 // Собрание законодательства РФ. 2021. № 27. Ст. 5351.

8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 года № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

9. О Стратегии экономической безопасности Российской Федерации на период до 2030: указ Президента РФ от 13 мая 2017 года № 208 // Собрание законодательства РФ. 2017. № 20. Ст. 2902.

10. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон от 31 июля 2020 года // Доступ из справ.-правовой системы «КонсультантПлюс». URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_358753/](http://www.consultant.ru/document/cons_doc_LAW_358753/) (дата обращения: 14.01.2023).

11. Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «Цифровая трансформация»: приказ Министерства цифрового развития, связи и

массовых коммуникаций РФ от 18 ноября 2020 года № 600. URL: <https://www.consultant.ru> (дата обращения: 14.01.2023).

12. Об утверждении Основ государственной политики регионального развития Российской Федерации на период до 2025 года: указ Президента РФ от 16 января 2017 года № 13 // Собрание законодательства РФ. 2017. № 4. Ст. 637.

13. Об утверждении разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации»: приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 1 августа 2019 года № 428. URL: <https://www.consultant.ru> (дата обращения: 14.01.2023).

14. Агапова Т.Н. Методика и инструментарий для мониторинга экономической безопасности региона // Вопросы статистики. 2001. № 2. С. 44–48.

15. Александров Г.А., Вякина И.В., Скворцова Г.Г. Комплексный метод анализа инвестиционного климата и несистематической составляющей инвестиционного риска // Экономика в промышленности. 2016. № 3. С. 230–240.

16. Александров Г.А., Вякина И.В., Скворцова Г.Г. Экономическая безопасность и инвестиционная привлекательность предприятий: характер взаимосвязи и проблема оценки // Экономические отношения. 2019. Т. 9. № 3. С. 2269–2284.

17. Афонцев С.А. Проблемы экономической безопасности России в контексте рыночной трансформации // Социально-экономическая трансформация в России: научные доклады Московского общественного научного фонда. 2001. Вып. 131. С. 15–42.

18. Баринаева В.А., Земцов С.П., Царева Ю.В. Предпринимательство и институты: есть ли связь на региональном уровне в России? // Вопросы экономики. 2018. № 6. С. 92–116.

19. Белозерцев Р.В., Белозерцев В.Н. Формирование стратегии обеспечения экономической безопасности предприятия // Экономический вестник ГОУ ВПО ЛНР «ДонГТУ». 2019. № 2. С. 5–12.

20. Бендиков М.А. Экономическая безопасность промышленного предприятия в условиях кризисного развития // Менеджмент в России и за рубежом. 2000. № 2. С. 19–29.

21. Бородушко Е.С. Принципы и методы оценки дисбалансов экономической системы как источника угроз экономической безопасности // Вестник Санкт-Петербургского университета МВД России. 2011. № 1 (49). С. 147–151.

22. Бухт Р., Хикс Р. Определение, концепция и измерение цифровой экономики // Вестник международных организаций. 2018. Т. 13. № 2. С. 143–172.



23. Возжеников А.В. Парадигма национальной безопасности реформирующейся России. 2-е изд., испр. и доп. М.: ЭДАС ПАК, 2000. 358 с.

24. Вякина И.В. Методы оценки экономической безопасности предприятия как инструментарий диагностики угроз развития // Экономический анализ: теория и практика. 2020. Т. 19. № 5. С. 835–859.

25. Гайфуллина М.М., Костомарова Е.В. Методический подход к оценке экономической безопасности нефтяной компании // Наукоеведение: интернет-журнал. 2017. Т. 9. № 2. С. 11.

26. Гильфанов М.Т. Организационно-методический инструментарий оценки детерминантов и обеспечения экономической безопасности предприятия // Социально-экономические явления и процессы. 2013. № 8 (054). С. 19–27.

27. Говорина О.В. Разработка механизма оценки экономической безопасности предприятия в рыночных условиях // Вестник КрасГАУ. 2008. № 3. С. 13–19.

28. Градов А.П., Ильин И.В. Экономическая безопасность страны: принципы анализа состояния и противодействия угрозам // Экономическая наука современной России. 2005. № 3. С. 88–101.

29. Григорьева В.В., Шумейко В.В. Методика оценки уровня экономической безопасности предприятия // European research: сборник статей XIX Международной научно-практической конференции. Пенза: МЦНС «Наука и Просвещение», 2019. С. 163–167.

30. Грунина Д.К. Контрольно-надзорная деятельность как фактор повышения деловой активности налоговых органов // Экономика. Налоги. Право. 2018. Т. 11. № 3. С. 131–139.

31. Дроздова М.И., Осетров Д.А. Цифровизация экономики как одно из условий экономической безопасности // Развитие территорий. 2020. № 2 (20). С. 23–26.

32. Ермакова И.Н., Михеева Н.Б., Хандогина Д.С. Методические подходы к оценке уровня экономической безопасности сельскохозяйственного предприятия // Социально-экономический и гуманитарный журнал Красноярского ГАУ. 2018. № 4. С. 43–54.

33. Запорожцева Л.А., Агибалов А.В. Концепция оценки уровня стратегической экономической безопасности предприятия // Социально-экономические явления и процессы. 2014. Т. 9. № 11. С. 78–85.

34. Игонина Л.Л. Экономическая безопасность России в системе макроэкономических инвестиционных критериев // Национальные интересы: приоритеты и безопасность. 2013. № 2 (191). С. 49–57.

35. Илларионов А.И. Критерии экономической безопасности // Вопросы экономики. 1998. № 10. С. 35–58.

36. Волкова Г.Л., Демьянова А.В., Шматко Н.А. Кадры для цифровой трансформации высшего образования: сотрудники ИКТ-подразделений. Мониторинг экономики образования: информационный бюллетень // Высшая школа экономики (национальный исследовательский университет). Москва: НИУ ВШЭ, 2022. 37 с.

37. Камнева В.В., Гнатышина Е.А. Цифровая экономика, цифровизация и цифровая трансформация // Вопросы студенческой науки. 2020. Вып. № 2 (42). С. 377–381.

38. Каплан Роберт С., Нортон Дейвид П. Сбалансированная система показателей: от стратегии к действию / пер. с англ. М. Павловой. М.: Олимп-Бизнес, 2008. 294 с.

39. Козырь Н.С. Подходы к определению глобальной конкурентоспособности // Национальные интересы: приоритеты и безопасность. 2015. Т. 11. № 26 (311). С. 39–52.

40. Кондратьев К.Я., Лосев К.С. Иллюзии и реальность стратегии устойчивого развития // Вестник Российской академии наук. 2000. Т. 72. № 7. С. 592–601.

41. Куклин А.А., Кривенко Н.В., Кривенцова Л.А. Экономическая безопасность и псевдобезопасность как элементы развития социально-экономической системы // Международный научно-исследовательский журнал. 2019. № 11-1 (89). С. 166–169.

42. Масленников В.В., Трохов А.А. Методические подходы к оценке рисков, определяющих экономическую безопасность компании // Азимут научных исследований: экономика и управление. 2016. Т. 5. № 4 (17). С. 272–274.

43. Романова О.А., Розенфельд Н.Я. Материально-техническая база в профессиональных образовательных организациях. Мониторинг экономики образования: информационный бюллетень // Высшая школа экономики (национальный исследовательский университет). Москва: НИУ ВШЭ, 2021. 44 с.

44. Мокроусова К.В. Идентификация и оценка инвестиционных рисков как задачи системы обеспечения экономической безопасности промышленного предприятия // Экономика. Инновации. Управление качеством. 2017. № 4. С. 4–9.

45. Овечкина О.Н. Понятие и методика оценки финансовой безопасности предприятия // Вопросы экономики и права. 2013. № 3. С. 87–92.

46. Олейников Е.А. Экономическая и национальная безопасность. М.: Экзамен, 2004. 768 с.

47. Волкова Г.Л., Пермякова В.А., Шматко Н.А. Организация цифровой коммуникации между подразделениями, преподавателями и студентами. Мониторинг экономики образования: информационный

бюллетень // Высшая школа экономики (национальный исследовательский университет). М.: НИУ ВШЭ, 2021. 35 с.

48. Пак С. Глобальный мегатренд Четвертой промышленной революции в цифровой экономике: как реализовать на практике потенциал «умных» городов? // Вестник международных организаций. 2022. Т. 17. № 2. С. 135–163.

49. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16). URL: <https://www.consultant.ru> (дата обращения: 14.01.2023).

50. Подмолодина И.М., Воронин В.П., Коновалова Е.М. Подходы к оценке экономической безопасности предприятий // Вестник Воронежского государственного университета инженерных технологий. 2012. № 4 (54). С. 156–161.

51. Поздеев В.Л. О понятии «экономическая безопасность предприятия»: аналитический аспект // Вестник СамГУПС. 2015. Т. 2. № 2 (2). С. 113–116.

52. Попов Е.В., Семячков К.А. Проблемы экономической безопасности цифрового общества в условиях глобализации // Экономика региона. 2018. Т. 14. Вып. 4. С. 1088–1110.

53. Пороховский А.А. Частные и общественные интересы как факторы развития в условиях цифровизации // Экономическое возрождение России. 2019. № 2 (60). С. 55–61.

54. Примакин А.И., Большакова Л.В. Модель оценки уровня экономической безопасности хозяйствующего субъекта // Вестник Санкт-Петербургского университета МВД России. 2012. № 4. С. 139–145.

55. Проценко О.Д., Дудин М.Н. Роль малого предпринимательства в социально-экономическом развитии регионов России // Экономика и социум: современные модели развития: межвузовский сборник научных трудов. 2016. № 12. С. 33–41.

56. Рифкин Дж. Третья промышленная революция: Как горизонтальные взаимодействия меняют энергетику, экономику и мир в целом / пер. с англ. М.: Альпина нон-фикшн, 2014. 409 с.

57. Рудакова Е.Н., Паньшин А.И., Власов А.В. Цифровизация как одна из тенденций развития транспорта и логистики в современных условиях // Путеводитель предпринимателя. 2021. Т. 14. № 1. С. 51–61.

58. Рудской А.И. Пути снижения рисков при построении в России цифровой экономики: Образовательный аспект // Высшее образование в России. 2019. Т. 28. № 2. С. 9–22.

59. Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере // Информационное право. 2016. № 4. С. 13–19.
60. Сенчагов В.К. О сущности и основах стратегии экономической безопасности России // Вопросы экономики. 1995. № 1. С. 98–101.
61. Солодилова Н.З., Гришин К.Е., Маликов Р.И. Конфигурационный подход к исследованию региональной экосистемы предпринимательства // Экономическая политика. 2018. Т. 13. № 5. С. 134–155.
62. Тамбовцев В.Л. Объект экономической безопасности России // Вопросы экономики. 1994. № 12. С. 45–53.
63. Тапскотт Д. Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта / пер. с англ. И. Дубинского; под ред. С. Писарева. Киев: INT Пресс: М.: Релф-бук, 1999. 432 с.
64. Татаркин А.И., Куклин А.А. Изменение парадигмы исследований экономической безопасности региона // Экономика региона. 2012. № 2. С. 25–39.
65. Украинский В.Н. Региональная конкурентоспособность: методологические рефлексии // Вопросы экономики. 2018. № 6. С. 117–132.
66. Ширко Л.М. К вопросу о сущности экономической безопасности предприятия // Экономические отношения. 2020. Т. 10. № 4. С. 1555–1564.
67. Ширко Л.М. Система показателей оценки экономической безопасности предприятия в сфере дорожного хозяйства // Экономика, предпринимательство и право. 2020. Т. 10. № 12. С. 3285–3296.
68. Шохнех А.В. Математические методы оценки экономической безопасности хозяйствующих субъектов // Электронный научный журнал «Управление экономическими системами». 2012. № 6 (42). URL: <http://uecs.ru/uecs42-422012/item/1403-2012-06-14-11-18-32> (дата обращения: 14.01.2023).
69. Экономическая безопасность: учеб. пособие / под. ред. В.А. Богомолова. 2-е изд., перераб. и доп. М.: ЮНИТИ, 2013. 295 с.
70. Экономическая безопасность: учебник для вузов / под общ. ред. Л.П. Гончаренко. 2-е изд., перераб. и доп. М.: Юрайт, 2019. 340 с.
71. Яркина Н.Н., Вершинина А.Н. Формирование системы экономической диагностики металлургического предприятия как фактор обеспечения его экономической безопасности // Молодой ученый. 2017. № 11. С. 300–306.
72. Accelerating the Digital Economy: Four Key. URL: <https://e.huawei.com/kz/eblog/industries/insights/2021/accelerating-digital-economy> (date of access: 14.01.2023).
73. The Distributed Situational Centers System as an Instrument of State and Corporate Strategic Goal-Setting in the Digital Economy / Z.K. Avdeeva [et al.] // IFAC-Papers OnLine. 2020. Vol. 53. Issue 2. P. 17499–17504.

74. Bahl M. *The Work Ahead: The Future of Businesses and Jobs in Asia Pacific's Digital Economy*. Chennai: Cognizant. URL: <https://www.cognizant.com/whitepapers/the-work-ahead-the-future-of-business-and-jobs-in-asia-pacific-s-digital-economy-codex2255.pdf> (date of access: 14.01.2023).
75. Baporikar N. *Fintech Challenges and Outlook in India // Inno-vative Strategies for Implementing Fin Tech in Banking*. 2021. P. 18.
76. Bazzi S., Blattman C. *Economic Shocks and Conflict: Evidence from Commodity Prices // American Economic Journal: Macroeconomics*. 2014. No. 6 (4). P. 1–38.
77. Bhaskar C., Ajay B., Ravi S.C. *Which Economies Showed the Most Digital Progress in 2020?* URL: <https://hbr.org/2020/12/which-economies-showed-the-most-digital-progress-in-2020?ab=hero-subleft-3> (date of access: 14.01.2023).
78. Brynjolfsson E., Collis A. *How Should We Measure the Digital Economy?* URL: <https://hbr.org/2019/11/how-should-we-measure-the-digital-economy> (date of access: 14.01.2023).
79. Brynjolfsson E., Collis A., Eggers F. *Using massive online choice experiments to measure changes in well-being // Proceedings of the National Academy of Sciences*. 2019. Vol. 116. No. 15. P. 7250–7255.
80. *GDP-B: Accounting for the Value of New and Free Goods in the Digital Economy / E. Brynjolfsson [et al.] // NBER Working paper*. No. 25695.
81. *The Role of the Entrepreneur in the Promotion of the Digital Economy: A Multi-Country Case Study Between Brazil and Portugal / M.A. Catussi [et al.] // Handbook of Research on Entrepreneurship and Marketing for Global Reach in the Digital Economy*. 2019. P. 23.
82. Chavula H., Kayiska C., Abebe C.T. *Policy Development Process in Africa // Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements*. 2011. P. 28.
83. Chen Y. *Improving Market Performance in the Digital Economy // China Economic Review*. 2020. Vol. 62. URL: <https://doi.org/10.1016/j.chieco.2020.101482> (date of access: 14.01.2023).
84. Dahlman C., Mealy S., Wermelinger M. *Harnessing the Digital Economy for Developing Countries*. Paris: OECD. URL: <http://www.oecd-ilibrary.org/docserver/download/4adffb24-en.pdf> (date of access: 14.01.2023).
85. Daidj N. *Strategic and Business-IT Alignment Under Digital Transformation: Towards New Insights? // Business Transformations in the Era of Digitalization*. 2019. P. 13.
86. Kesim E. *Development Trends in Economics of Distance Education from the Perspective of New Technologies // Handbook of Research on Emerging Priorities and Trends in Distance Education: Communication, Pedagogy, and Technology*. 2014. P. 14.

87. Digital Economy Definition: 3 Digital Economy Examples. URL: <https://www.masterclass.com/articles/digital-economy> (date of access: 14.01.2023).

88. Digital Middle East: Transforming the Region into a Leading Digital Economy. / T. Elmasry [et al.]. New York: McKinsey & Company. URL: <http://www.mckinsey.com/global-themes/middle-east-and-africa/digital-middle-east-transforming-the-region-into-a-leading-digital-economy> (date of access: 14.01.2023).

89. Fernández-Macías E. Automation, digitization and platforms: Implications for work and employment. URL: <https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/digital-economy> (date of access: 14.01.2023).

90. Fernández-Villacañas M.M.A. The New Concept of Disruptive Logistics: Global Sustainable Logistics 4.0 in a Future Post-New World Economic Order // Handbook of Research on Emerging Business Models and the New World Economic Order. 2022. P. 26.

91. G20 DETF. G20 Digital Economy Development and Cooperation Initiative. URL: <http://www.g20.utoronto.ca/2016/g20-digital-economy-development-and-cooperation.pdf> (date of access: 14.01.2023).

92. Goodwin T. The Battle Is For The Customer Interface. URL: <https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/> (date of access: 14.01.2023).

93. Goodyear S. Smart City Technology and Civic Engagement in Ontario, Canada: Case Examples From Toronto and Barrie // Handbook of Research on the Role of Libraries, Archives, and Museums in Achieving Civic Engagement and Social Justice in Smart Cities. 2022. P. 20.

94. Digital Transformations and the Importance of Business Models for Organizations: Digital Business Models – The Key for Success in Today's Business World Lavinia / A. Gruia [et al.] // Handbook of Research on Digital Transformation Management and Tools. 2022. P. 22.

95. Guerra A.G., Gómez L.S., Rivas C.J. Digital Social Innovation: Fundamentals and Framework of Action // Organizational Transformation and Managing Innovation in the Fourth Industrial Revolution. 2019. P. 28.

96. Hintošová A.B. The Digital Economy in the Context of Foreign Direct Investment Flows // Fostering Innovation and Competitiveness With Fin Tech, Reg Tech, and Sup Tech. 2021. P. 18.

97. Iguehi J.I., Charity O.A., Ose F. Influence of Information and Communication Technologies (ICTs) on the Digital Economy // Handbook of Research on Knowledge and Organization Systems in Library and Information Science. 2021. P. 21.

98. Iuga I.C. The Degree of SMEs Digitalization in the Context of the European Digital United Market // Handbook of Research on IoT, Digital Transformation, and the Future of Global Marketing. 2021. P. 33.

99. Karimov N.G., Parpieva R.A., Khamidova F.A. Digital Transformation of the Economy as a New Challenge to Economic Security // ICFNDS 2021: The 5th International Conference on Future Networks & Distributed Systems. 2021. P. 348–355.
100. Kirishchieva I., Skorev M., Mishchenko O., Grafova T. Risks and threats to economic security in the digital economy // International Symposium “Sustainable Energy and Power Engineering 2021” (SUSE-2021). 2021. Vol. 288. URL: <https://doi.org/10.1051/shsconf/202111001028> (date of access: 14.01.2023).
101. Understanding the Digital Economy / E. Brynjolfsson, B. Kahin (eds). Cambridge: MIT Press. P. 295–324.
102. Knickrehm M., Berthon B., Daugherty P. Digital Disruption: The Growth Multiplier. Dublin: Accenture. URL: [https://www.accenture.com/\\_acnmedia/PDF-4/Accenture-Strategy-Digital-Disruption-Growth-Multiplier.pdf](https://www.accenture.com/_acnmedia/PDF-4/Accenture-Strategy-Digital-Disruption-Growth-Multiplier.pdf) (date of access: 14.01.2023).
103. Korovkin V. Chief Digital Officers and Their Roles, Agendas, and Competencies // Encyclopedia of Organizational Knowledge, Administration, and Technology. 2021. P. 12.
104. Kraiwanit T., Limsaku A. Adoption of Libra as a Digital Currency in Thailand // Handbook of Research on Current Trends in Asian Economics, Business, and Administration. 2022. P. 22.
105. Lane N. Advancing the Digital Economy into the 21st Century // Information Systems Frontiers. 1999. Vol. 1. No. 3. P. 317–320.
106. Lee H. Endress. Sustainable Economic Development. Resources, Environment and Institutions // Scarcity, Security, and Sustainable Development. 2015. Chapter 3. P. 49–66.
107. Lemoine P.A., Hackett P.T., Richardson Michael D. Global Higher Education and VUCA – Volatility, Uncertainty, Complexity, Ambiguity // Handbook of Research on Administration, Policy, and Leadership in Higher Education. 2017. P. 20.
108. Levchaev P.A. The digital economy: problems and prospects. International Journal of Applied And Fundamental Research. 2017. No. 4. URL: <https://www.science-sd.com/472-25370> (date of access: 14.01.2023).
109. Liska R. The Digital Economy Readiness Study: The Czech Republic in the European Context // Managerial Issues in Digital Transformation of Global Modern Corporations. 2021. P. 32–51.
110. Mundula L. Institutional Entrepreneurship, Trust, and Regulatory Capture in the Digital Economy Source // Handbook of Research on Entrepreneurship and Marketing for Global Reach in the Digital Economy. 2019. P. 22.

111. Mamatelashvili O.V., Kulagina Zh.D. Economic Security of Business in The Digital Economy // European proceedings of social and behavioral sciences EPSBS. 2021. P. 878–887.
112. Manolova M. Ethical Risks in the Cross Section of Extended Reality (XR), Geographic Information Systems (GIS), and Artificial Intelligence (AI) // Applied Ethics in a Digital World. 2022. P. 17.
113. The Emerging Digital Economy / L. Margherio [et al.]. Washington, DC: Department of Commerce. URL: [http://www.esa.doc.gov/sites/default/files/emergingdig\\_0.pdf](http://www.esa.doc.gov/sites/default/files/emergingdig_0.pdf) (date of access: 14.01.2023).
114. Mesenbourg T. Measuring the Digital Economy. URL: <http://www.census.gov/estats> (date of access: 14.01.2023).
115. Mkrttchian V. The Internet of Things and Blockchain Technologies Adaptive Trade Systems in the Virtual World: By Creating Virtual Accomplices Worldwide // Multidisciplinary Functions of Blockchain Technology in AI and IoT Applications. 2021. P. 19.
116. Being Digital / eds. N. Negroponte. New York: Alfred A. Knopf, 1995. 243 p.
117. Nordhaus W.D. Schumpeterian profits in the American economy: Theory and measurement // National Bureau of Economic Research. 2004. No. w10433.
118. Approaches to Tackle Smart Cities Challenges in Brunei / F. Nur [et al.] // Handbook of Research on Disruptive Innovation and Digital Transformation in Asia. 2021. P. 19.
119. OUP Digital Economy. Oxford Dictionary. Oxford: Oxford University Press. URL: [https://en.oxforddictionaries.com/definition/digital\\_economy](https://en.oxforddictionaries.com/definition/digital_economy) (date of access: 14.01.2023).
120. Peluso N., Watts M. Violent Environments: Responses. ECSP REPORT, 2003. Vol. 9. P. 93–96.
121. Ritchie B., Brindley C. Risk Management in the Digital Economy // Encyclopedia of Information Science and Technology, Second Edition. 2009. P. 8.
122. Romanelli M. Towards Sustainable Peace by Technology // Marketing Peace for Social Transformation and Global Prosperity. 2019. P. 24.
123. Rouse M. Digital Economy. Newton: Tech target. URL: [http://searchcio.techtarget.com/definition/digital-economy\\_economy](http://searchcio.techtarget.com/definition/digital-economy_economy) (date of access: 14.01.2023).
124. Shankar S.I. Application of Digital Technologies: Integrated Blockchain With Emerging Technologies // Handbook of Research on Supply Chain Resiliency, Efficiency, and Visibility in the Post-Pandemic Era. 2022. P. 28.



125. Strommen-Bakhtiar A. Digital Economy, Business Models, and Cloud Computing // Global Virtual Enterprises in Cloud Computing Environments. 2019. P. 19–44.

126. Tolstoguzov O. International Movement of Highly Skilled Professionals // Migration and Urbanization: Local Solutions for Global Economic Challenges. 2020. P. 22.

127. Tolstykh T.O., Vertakova Y. Professional Training for Structural Economic Transformations Based on Competence Approach in the Digital Age // Handbook of Research on Students' Research Competence in Modern Educational Contexts. 2018. P. 22.

128. Tugui A. Calm Technologies as the Future Goal of Information Technologies // Encyclopedia of Multimedia Technology and Networking, Second Edition. 2009. P. 8.

129. Measuring GDP in the digital economy: Increasing dependence on uncaptured GDP / C. Watanabe [et al.] // Technological Forecasting and Social Change. 2018. Vol. 137. P. 226–240. URL: <https://doi.org/10.1016/j.techfore.2018.07.053> (date of access: 14.01.2023).

130. Yildirim S., Demirtas I., Yildirim D.C. Review of Alternative Economic Approaches to Achieve Sustainable Development: The Rising Digitalization and Degrowth Post COVID-19 // Handbook of Research on Sustainable Development Goals, Climate Change, and Digitalization. 2022. P. 20.

131. Yu P., Chen D., Ahuja A. Smart and Sustainable Economy: How COVID-19 Has Acted as a Catalyst for China's Digital Transformation // AI-Enabled Agile Internet of Things for Sustainable FinTech Ecosystems. 2022. P. 41.

132. Zairis A.G. The Effective Use of Digital Technology by SMEs // Entrepreneurial Development and Innovation in Family Businesses and SMEs. 2020. P. 12.

## ПРИЛОЖЕНИЯ

### Приложение А

#### ОБЗОР ТРАКТОВОК ТЕРМИНА «ЦИФРОВАЯ ЭКОНОМИКА»

№	Понятие	Автор
1	Цифровая экономика – вид бизнеса, преимущественно основанный на электронной коммерции, направленный на производство электронных товаров и электронных услуг	О.В. Толстого [126]
2	Цифровая экономика – это экономика, характеризующаяся растущей взаимосвязанностью людей, организаций и машин посредством интернета и использованием цифровых технологий (например, робототехника и автоматизация производства, новые источники данных, облачные вычисления, аналитика больших данных и ИИ)	Л. Мундула [110]
3	Цифровая экономика – это смена парадигмы, происходящая в экономике на основе расширения использования цифровых технологий	Э. Кесим [86]
4	Цифровая экономика – это экономика, использующая цифровые технологии в процессе осуществления различных видов деятельности	И.Д. Икенве, О.Ф. Осе-Абама [97]
5	Цифровая экономика, или «новая экономика», характеризует текущие преобразования, происходящие в экономике, вследствие использования цифровых технологий	Ю.К. Юга [98]
6	Цифровая экономика представляет собой цифровые транзакции, выполняемые с помощью информационных и телекоммуникационных технологий	Ш.С. Айер [124]
7	Цифровая экономика – это система экономических, социальных и культурных отношений, основанная на использовании цифровых и информационно-коммуникационных технологий	Т.О. Толстых, Ю. Вертакова [127]
8	Цифровая экономика – это термин, используемый для описания современного неизбежного влияния новых технологий на экономику	С. Гудиер [93]
9	Цифровая экономика – это экономика, основанная на цифровых вычислительных технологиях, хотя мы все чаще воспринимаем ее как ведение бизнеса через интернет-торговлю. Цифровую экономику называют также интернет-экономикой, новой экономикой или веб-экономикой	Р. Лиска [109]
10	Цифровая экономика – это экономическая деятельность, ориентированная на цифровые и электронные технологии (в частности, ориентирована на электронный бизнес и торговлю, а также произведенные ими товары и услуги)	В. Мкртчян [115]

Продолжение прил. А

№	Понятие	Автор
11	Цифровая экономика – это экономика, основанная на доступе к сети Интернет и использовании ее ресурсов	П. Лемуан, Т. Хакетт, М.Д. Ричардсон [107]
12	Цифровая экономика – хотя общепризнанный подход к трактовке данного понятия на данный момент отсутствует, согласно существующим исследованиям, она представляет собой экономическую систему, широко использующую ИКТ, электронную коммерцию (бизнес-модель, в которой широко используются ИКТ на входе и выходе) и транзакции с использованием ИКТ в моделях В2В, В2С и С2С	П. Ю, Д. Чен, А. Ахуджа [131]
13	Цифровая экономика – это ситуация, при которой различные виды экономической деятельности используют ИКТ для достижения поставленных целей, что способствует развитию национальной экономики в целом. Другими словами, цифровая экономика – это экономика, основанная на электронных товарах и услугах, производимых электронным бизнесом и реализуемых с помощью электронных средств	Х.К. Чавула, А. Чекол [82]
14	Цифровая экономика – это глобальная сеть экономической деятельности, коммерческих операций и профессиональных взаимодействий, которые обеспечиваются на основе применения ИКТ	М. Манолова [112]
15	Цифровая экономика базируется на разработках в области ИКТ и использует их для ведения бизнеса и осуществления коммерческой деятельности	Б. Ричи, К. Бриндли [121]
16	Цифровая экономика – это экономика, основанная на цифровых вычислительных технологиях	Н.Ф.Н. Сайфулбахри, С.Х.М.А. Лим [118]
17	Цифровая экономика – это модель цифровой трансформации существующей экономической теории и деловой практики	С. Йилдирим, И. Демирташ, Д.Ч. Йилдирим [130]
18	Цифровая экономика – это экономика, основанная на использовании цифровых вычислительных технологий, связанных между собой через интернет, на постоянной основе. Она включает в себя электронный бизнес (например, онлайн-торговлю) и оцифрованные части традиционного бизнеса (например, онлайн- и мобильный банк)	В.В. Коровкин [103]

## Продолжение прил. А

№	Понятие	Автор
19	Цифровая экономика – это экономика, основанная на ИКТ, как средство коммуникации и создания стоимости	А. Герра, Л.С. де Гомес, К.Х. Ривас [95]
20	Цифровая экономика – это экономическая деятельность, коммерческие операции и общение, основанное на ИКТ или обеспечиваемое ими	А. Стреммен-Бахтияр [125]
21	Цифровая экономика предполагает повсеместное использование информационных технологий (аппаратных средств, программного обеспечения, приложений) во всех отраслях экономики, включая внутрихозяйственную деятельность организаций (коммерческих, государственных и некоммерческих), а также внешние транзакции между организациями и отдельными лицами	М. Романелли [122]
22	Цифровая экономика – это экономическая система, в которой в основном используются цифровые технологии	М.А. Фернандес-Вильяканьяс Марин [90]
23	Цифровая экономика – это экономика, основанная на онлайн-деятельности людей, предприятий, цифровых устройств, данных и процессов. Примерами подобных цифровых взаимодействий являются онлайн-платежи, электронная коммерция, онлайн-биржи и другие виды деятельности, основанные на интернете вещей	Т. Крайванит, А. Лимсаку [104]
24	Цифровая экономика представляет собой следствие качественной трансформации широкого круга экономических отношений, основанных на интенсивном использовании ИКТ	А.Б. Хинтошова [96]
25	Цифровая экономика – это экономика, основанная на цифровых технологиях и интернете	А.Г. Заирис [132]
26	Цифровая экономика ознаменовала собой исторический переход к новому подходу к ведению бизнеса на основе новых ИКТ, таких как ИИ, анализ больших данных, облачные вычисления, интернет вещей, машинное обучение	Д. Набыла [85]
27	Цифровая экономика – термин, применимый к любому экономическому процессу, транзакции, взаимодействию, основанным на цифровых технологиях	Н. Бапорикар [75]
28	Цифровая экономика – это сектор экономики, который изучает воздействия новых технологий связи, производства и информации на создание стоимости бизнеса	М. Антонио, К. Пашоалотто, П.Э. де Оливейра, А.Р.К. Луз [81]

## Продолжение прил. А

№	Понятие	Автор
29	Цифровая экономика – это часть экономической продукции, полученная исключительно или в основном с помощью цифровых технологий	А. Груя, Н. Бибу, М. Нэстасе, Д. Дэнэяцэ, Н. Кристаке [94]
30	Цифровая экономика – это объединение экономических субъектов в сеть посредством цифровизации потоков и процессов субъекта, а также создания и обмена цифровыми активами (виртуальными активами) на фоне физического расширения и развития интернета	А. Туги [128]
31	Цифровая экономика – это широкий диапазон видов экономической активности, к которым относится использование оцифрованной информации и знаний в качестве ключевого фактора производства, современных информационных сетей в качестве важной области деятельности, а также эффективное использование ИКТ в качестве важного фактора экономического роста и оптимизации экономической структуры	Определение «Большой двадцатки» [91]
32	Цифровая экономика – это экономика, которая функционирует в основном за счет применения цифровых технологий, в частности безналичных операций через интернет	Оксфордский словарь английского языка [119]
33	Цифровая экономика представляет собой сочетание технологий общего применения и ряда видов экономической и общественной деятельности, осуществляемых пользователями интернета при помощи соответствующих технологий. Цифровая экономика, таким образом, включает в себя физическую инфраструктуру, которую задействуют цифровые технологии (широкополосные проводящие сети, маршрутизаторы), устройства доступа (компьютеры, смартфоны), информационные системы (Google, Salesforce) и обеспечиваемый ими функционал (интернет вещей, анализ больших данных, облачные вычисления)	К. Далман, С. Мили, М. Вермелин- гер [84]
34	Цифровая экономика – это всемирная сеть видов экономической деятельности, которые стали доступными благодаря ИКТ. Иными словами, цифровую экономику можно определить как экономику, основанную на цифровых технологиях	М. Роуз [123]
35	Цифровая экономика представляет собой часть общего объема производства, создаваемую различными «цифровыми» ресурсами. Эти ресурсы включают цифровые навыки, цифровое оборудование (комплектующие, программное обеспечение и средства связи) и промежуточные цифровые товары и услуги, используемые в производстве. Данный подход отражает суть цифровой экономики	М. Никрем, Б. Бертон, П. Догерти [102]

№	Понятие	Автор
36	Автор не дает определение как таковое; вместо этого в работе проводится разграничение между «задействованием» цифровых технологий и «существованием» благодаря им	М. Бахл [74]
37	Авторы не приводят конкретного определения, отмечая, что «цифровая экономика – это меньше, чем концепция, и больше – способ осуществления деятельности», однако выдвигают три атрибута рассматриваемого феномена: создание стоимости на передовых направлениях деловой активности, оптимизация процессов, учитывающих клиентский опыт, и формирование базового потенциала, поддерживающего всю структуру	Т. Элмасри [88]
38	Цифровая экономика – это конвергенция компьютерных и коммуникационных технологий в сети Интернет и возникающий поток информации и технологий, которые стимулируют развитие электронной торговли и масштабные изменения в организационной структуре	Н. Лейн [105]
39	Автор не дает четкого определения; рассматриваются четыре фактора развития цифровой экономики: разрастание сети Интернет, электронная торговля между предприятиями, цифровая доставка товаров и услуг и розничная продажа физических товаров	Л. Маргеро [113]
40	Цифровая экономика – это процесс трансформации всех секторов экономики благодаря цифровизации при помощи компьютерных технологий	Э. Бри-нольфссон, А. Коллис [80]
41	Цифровая экономика включает товары и услуги, развитие, производство, продажа или предоставление которых находится в критической зависимости от цифровых технологий	Р. Клинг, Р. Лэмб [101]
42	Автор указывает на то, что понятие «цифровая экономика» включает в себя три компонента: инфраструктуру электронного бизнеса, которая является частью всей экономической инфраструктуры, используемой для осуществления электронных операций и электронной торговли; электронный бизнес, то есть операции, осуществляемые предприятием при помощи компьютерных сетей; электронную торговлю, под которой подразумевается объем товаров и услуг, реализуемый через компьютерные сети	Т. Мезенбург [114]

МЕТОДИКИ РАСЧЕТА ОБЯЗАТЕЛЬНЫХ ПОКАЗАТЕЛЕЙ  
РЕГИОНАЛЬНЫХ ПРОЕКТОВ

№	Наименование показателя, единица измерения	Методика расчета	Источники
<b>1. Информационная инфраструктура</b>			
1	Доля медицинских организаций государственной и муниципальной систем здравоохранения субъекта РФ (больниц и поликлиник), подключенных к сети Интернет, %	$N = MO1 / MO2 * 100 \%$	Росстат, орган исполнительной власти субъекта РФ в сфере здравоохранения
		MO1 – число объектов медицинских организаций государственной и муниципальной систем здравоохранения субъекта РФ (больниц и поликлиник), подключенных к сети Интернет, в соответствии с утвержденным перечнем, представленным субъектом РФ	
2	Доля фельдшерских и фельдшерско-акушерских пунктов медицинских организаций государственной и муниципальной систем здравоохранения субъекта РФ, подключенных к сети Интернет, %	$N = ФАП1 / ФАП2 * 100 \%$	Росстат, орган исполнительной власти субъекта РФ в сфере здравоохранения
		ФАП1 – число фельдшерских и фельдшерско-акушерских пунктов государственной и муниципальной систем здравоохранения субъекта РФ, подключенных к сети Интернет, в соответствии с утвержденным перечнем, представленным субъектом РФ	
		$N = ФАП1 / ФАП2 * 100 \%$	
		ФАП2 – общее число фельдшерских и фельдшерско-акушерских пунктов государственной и муниципальной систем здравоохранения субъекта РФ, осуществляющих свою деятельность на территории субъекта РФ, в соответствии с утвержденным перечнем	

№	Наименование показателя, единица измерения	Методика расчета	Источники
3	Доля образовательных организаций государственной собственности субъекта Российской Федерации и муниципальной собственности, реализующих образовательные программы общего образования и/или среднего профессионального образования, подключенных к сети Интернет, %	$N = \text{ОО1} / \text{ОО2} * 100 \%$	Росстат, орган исполнительной власти субъекта РФ в сфере образования
		ОО1 – число образовательных организаций государственной собственности субъекта РФ и муниципальной собственности, реализующих образовательные программы общего образования и/или среднего профессионального образования, подключенных к сети Интернет, в соответствии с утвержденным перечнем	
		ОО2 – общее число образовательных организаций государственной собственности субъекта РФ и муниципальной собственности, реализующих образовательные программы общего образования и/или среднего профессионального образования, осуществляющих свою деятельность на территории субъекта РФ	
4	Доля органов власти субъекта Российской Федерации, органов местного самоуправления, подключенных к сети Интернет, %	$N = \text{ОГВ1} / \text{ОГВ2} * 100 \%$	Органы власти субъекта РФ, органы местного самоуправления
		ОГВ1 – число органов власти субъекта РФ, органов местного самоуправления, подключенных к сети Интернет, в соответствии с утвержденным перечнем	
		ОГВ2 – общее число органов власти субъекта РФ, органов местного самоуправления в соответствии с утвержденным перечнем	
<b>2. Кадры для цифровой экономики</b>			
1	Количество выпускников организаций профессионального образования государственной собственности субъекта Российской Федерации и муниципальной собственности с ключевыми компетенциями цифровой экономики, чел.	$N = \text{КВ}$	Росстат
		КВ – численность выпускников организаций профессионального образования, расположенных в субъекте РФ, прошедших независимое оценивание на владение ключевыми компетенциями цифровой экономики	



№	Наименование показателя, единица измерения	Методика расчета	Источники
2	Количество трудоспособных жителей субъекта РФ, прошедших переобучение по компетенциям цифровой экономики в рамках дополнительного образования, чел.	N = КС	Росстат
		КС – количество трудоспособных жителей субъекта РФ, прошедших переобучение по компетенциям цифровой экономики в рамках дополнительного образования, чел.	
<b>3. Информационная безопасность</b>			
1	Средний срок простоя информационных систем органов власти субъекта РФ и органов местного самоуправления в результате компьютерных атак, ч	Разрабатывается в рамках соответствующего мероприятия федерального проекта «Информационная безопасность»	Росстат
2	Количество специалистов, подготовленных по образовательным программам в области информационной безопасности в организациях высшего профессионального образования и организациях среднего профессионального образования, расположенных в субъекте Российской Федерации, чел.	Разрабатывается в рамках соответствующего мероприятия федерального проекта «Информационная безопасность»	Росстат
3	Стоимостная доля закупаемого и (или) арендуемого органами исполнительной власти субъекта Российской Федерации, органами местного самоуправления отечественного программного обеспечения, %	Разрабатывается в рамках соответствующего мероприятия федерального проекта «Информационная безопасность»	Росстат
<b>4. Цифровые технологии</b>			
1	Увеличение затрат на развитие «сквозных» цифровых технологий компаниями, зарегистрированными на территории субъекта Российской Федерации, %	$N = V_n / V_0 * 100 \%$	Данные показатели запланированы к внесению в форму статистической отчетности Росстата
		$V_0$ – объем затрат на развитие «сквозных» цифровых технологий компаниями, зарегистрированными на территории субъекта Российской Федерации, в 2019 году	
		$V_n$ – объем затрат на развитие «сквозных» цифровых технологий компаниями, зарегистрированными на территории субъекта Российской Федерации, в отчетном году	

№	Наименование показателя, единица измерения	Методика расчета	Источники
<b>5. Цифровое государственное управление</b>			
1	Доля взаимодействий граждан и коммерческих организаций с органами власти субъекта РФ и органами местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, осуществляемых в цифровом виде, %	$N = \text{ОБР1} / \text{ОБР2} * 100 \%$ <p>ОБР1 – число обращений и заявлений граждан и коммерческих организаций в органы власти субъекта РФ и местного самоуправления и организации государственной собственности субъекта РФ и муниципальной собственности, направленных в электронной форме через сеть Интернет</p> <p>ОБР2 – общее число обращений и заявлений граждан и коммерческих организаций в органы власти субъекта РФ и местного самоуправления и организации государственной собственности субъекта РФ и муниципальной собственности</p>	Росстат
2	Доля приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, соответствующих целевой модели цифровой трансформации (предоставление без необходимости личного посещения государственных органов и иных организаций, с применением реестровой модели, онлайн (в автоматическом режиме), проактивно), %	$N = \text{ПГС1} / \text{ПГС2} * 100 \%$ <p>ПГС1 – число приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, предоставляемых без необходимости личного посещения государственных органов и иных организаций, с применением реестровой модели, онлайн (в автоматическом режиме), проактивно</p> <p>ПГС2 – общее число приоритетных государственных услуг и сервисов по утвержденному перечню, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности</p>	Орган исполнительной власти субъекта РФ в сфере информационных технологий и связи

№	Наименование показателя, единица измерения	Методика расчета	Источники
3	Доля отказов при предоставлении приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, от числа отказов в 2018 году, %	$N = \text{ОТК1} / \text{ОТК2} * 100 \%$	Орган исполнительной власти субъекта РФ в сфере информационных технологий и связи, Росстат
		ОТК1 – число отказов в предоставлении приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности, в текущем году	
		ОТК2 – число отказов в предоставлении приоритетных государственных услуг и сервисов, оказываемых органами власти субъекта РФ, органами местного самоуправления, организациями государственной собственности субъекта РФ и муниципальной собственности, в 2018 году	
4	Доля внутриведомственного и межведомственного юридически значимого электронного документооборота органов власти субъекта РФ и местного самоуправления и организаций государственной собственности субъекта РФ и муниципальной собственности, %	$N = \text{МВ1} / \text{МВ2} * 100 \%$	Орган исполнительной власти субъекта РФ в сфере информационных технологий и связи, Росстат
		МВ1 – число документов, направленных органами власти субъекта Российской Федерации и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности посредством внутриведомственного и межведомственного юридически значимого электронного документооборота	
		МВ2 – общее число исходящих документов, направленных органами власти субъекта РФ и местного самоуправления и организациями государственной собственности субъекта РФ и муниципальной собственности	

Ирина Владимировна Вякина  
Анна Викторовна Бойкова

**Экономическая безопасность бизнеса  
в условиях цифровизации**

*Монография*

Редактор М.Б. Юдина  
Корректор С.В. Борисов

---

Подписано в печать 21.07.2023

Формат 60×84/16

Физ. печ. л. 10,75

Тираж 50 экз.

Усл. печ. л. 9,998

Заказ № 40

Бумага писчая

Уч.-изд. л. 9,353

С – 40

---

Редакционно-издательский центр  
Тверского государственного технического университета  
170026, г. Тверь, наб. А. Никитина, 22