УДК 33 DOI: 10.14451/1.251.411

Риски цифровой экономики

© 2025 **Волкова Эльвира Сергеевна**
Кандидат экономических наук, доцент кафедры Менеджмент. Санкт-Петербургский филиал Финансового университета при Правительстве РФ, Россия, Санкт-Петербург.
E-mail: ESVolkova@fa.ru

Ключевые слова: цифровые технологии, трансформация, риски, данные, безопасность, развитие.

Совершенствование разработок в области IT становится возможным в результате расширения государством векторов развития цифровой экономики страны. Современные IT-программы по обмену большими массивами информационных данных способствуют принятию взвешенных управленческих решений, выполнению прогнозных расчетов, обработке всевозможной информации, созданию баз данных.
На этом фоне, однако, нередко возникают всевозможные угрозы и риски, связанные с потерей непосредственно бизнеса, со снижением численности рабочих и сокращением штата, а также уровня безопасности.
Сегодня уже активно применяются и внедряются технологии IT в жизнь общества и государства. Технологии меняют сферу массового обслуживания, появляются новые бизнес-модели в различных отраслях, а также создаются рабочие группы, которые рассматривают различные категории рисков.
В этих глобальных технологических изменениях многое зависит от позиции государства. По мнению экспертов, государство рассматривает своей главной задачей возможность создания единой нормативной базы для совершенствования IT-технологий, на основе которой бизнес начнет самостоятельную трансформацию вследствие изменений внешней деловой среды и роста конкуренции. Несмотря на все существующие риски, плюсы заключаются в удобстве и появлении новых возможностей, которых не было раньше.

Характеристика проблем

В объекте управления первый класс проблем вызывается диспропорцией и узкими местами:

- сложность в контроле и невозможность прекращения внедрения новых технологий вследствие их «самоподпитки»;
- отсутствие равных возможностей у регионов для внедрения инновационных технологий;
- необходимость соблюдения при внедрении новых технологий национальных интересов по обеспечению безопасности информации.

Расхождение целей и интересов лежат в основе второго класса проблемных ситуаций:

- не сформулированные окончательно цели и задачи создания именно цифровой экономики;
- существование внешних и внутренних препятствий для реализации инновационных проектов и программ;
- высокая степень рисков, связанных с коррупцией;
- высокий уровень зависимости от «олигархических рисков».

В основе третьего класса проблем в субъекте управления отмечаются нарушения коммуникационных взаимодействий:

- повышение уровня безработицы;
- нередкое отсутствие воображения вследствие развития преимущественного машинного восприятия и мышления у молодежи;
- высокий уровень зависимости от современных гаджетов наряду с зависимостью от IT-технологий в целом.

Характеристика решений

Первый класс проблем возможно преодолеть путем поэтапного планирования внедрения новых разработок с учетом степени технической оснащенности субъектов.

Второй класс проблемных ситуаций можно разрешить с помощью активного координирования по вертикали власти сверху-вниз на всех ее уровнях.

Третий класс проблем минимизируется путем принятия организационных решений для разработки новой Программы по обеспечению национальной безопасности данных [5; 6].

Риски в объекте и угрозы в субъекте управления

Сложность в контроле и невозможность прекращения внедрения новых технологий вследствие их «самоподпитки»:

1. Риск не совершенности управленческой системы научно-технологического сектора развития экономики в условиях современности [4; 9].
2. Риск отсутствия полного контроля за автономными роботомашинными системами, способными к самоорганизации.

Отсутствие равных возможностей у регионов для внедрения инновационных технологий:

1. Риск недостатка собственных ресурсов и технологий у регионов, требуемых для выполнения плановых мероприятий Программы.
2. Риск имеющейся достаточно высокой степени зависимости от импортных поставок в ряде секторов российской экономики.
3. Риск отсутствия возможности внедрения инновационных технологий вследствие низкого уровня технологической грамотности населения.

Необходимость соблюдения при внедрении новых технологий национальных интересов по обеспечению безопасности информации:

1. Риск сохраняющегося кибертерроризма и кибершпионажа, которые осуществляются иностранными террористическими организациями.
2. Риск «кражи личности» после внедрения единого идентификационного документа личности.
3. Риск роста реальных угроз в отношении национальной кибербезопасности.
4. Риск извлечения данных из гигантских объемов информации с помощью применения технологий Big Data.
5. Значительное ограничение суверенитета и повышение его уязвимости.

Не сформулированные окончательные цели и задачи создания именно цифровой экономики:

1. Риск снижения оптимального расходования бюджетных средств, которое ведет к дефициту бюджета.
2. Риск снижения качества технологических инновационных решений в сфере IT.
3. Риски снижения репутации компаний и доверия к ним вследствие роста конкуренции в IT-секторе экономики.

Существование внешних и внутренних препятствий для реализации инновационных проектов и программ:

1. Риск снижения устойчивости со стороны государства в случае изменения нормативно-законодательной базы.
2. Риск внедрения в разнообразные виды деятельности чужих технологических решений IT-сферы, что снижает суверенитет с повышением его уязвимости.
3. Риск недостаточности проверенных методик и нормативных инструментов, позволяющих

стандартизировать и регулировать разработанные технологии.
4. Риск зависимости от ускоренного импорта методик внедрения технологий, применяемых в других государствах.

Высокая степень рисков, связанных с коррупцией:

1. Риск анонимного и безнаказанного пользования материальными благами.
2. Риск уклонения от уплаты налогов.
3. Риск незаконного вывоза капитала.
4. Риск «отмывания» незаконно полученных доходов с использованием криптовалют.

Высокий уровень зависимости от «олигархических рисков»:

1. Риск приобретения конкурентных преимуществ при биржевой торговле на мировых рынках криптовалюты с использованием ИИ.
2. Риск применения современных генно-инженерных технологий для опасных разработок, угрожающих человечеству.
3. Риск создания условий привилегированности для ведения бизнеса за счет перераспределения активов.

Повышение уровня безработицы:

1. Риски, определяющиеся демографическими особенностями.
2. Риск разрастания паники среди населения в результате утраты рабочих мест.
3. Риск, связанный с отсутствием у роботов способности разумно реагировать на непредвиденную обстановку и изменение рабочей среды
4. Риск обеднения человеческого и кадрового потенциала.

Нередкое отсутствие воображения вследствие развития преимущественного машинного восприятия и мышления у молодежи:

1. Риск стандартизированного мышления, неспособности мыслить неординарно.
2. Риск образовательной системы — «отмирание» старых профессий и появление новых.
3. Риск снижения развития технологий в будущем, который может быть вызван отсутствием потенциальных разработчиков.

Высокий уровень зависимости от современных гаджетов наряду с зависимостью от IT-технологий в целом:

1. Риск снижения прецессионного мастерства.
2. Риск информационной перегрузки как следствие обилия информации, в том числе некачественной.
3. Риск возникновения неспособности адекватно планировать и прогнозировать будущее.
4. Риск потери способности глубокого аналитического осмысления и ситуационного мышления.

В матрице выделяется 10 основных рисковых факторов и угроз для субъекта:

- Риск несовершенности управленческой системы научно-технологического сектора развития экономики в условиях современности (∑223).
- Риск недостатка собственных ресурсов и технологий, требуемых для выполнения плановых мероприятий Программы (∑215).
- Риск отсутствия полного контроля за автономными роботомашинными системами, способными к самоорганизации (∑209).
- Риск снижения оптимального расходования бюджетных средств, которое ведет к дефициту бюджета (∑209).
- Риск потери способности глубокого аналитического осмысления и ситуационного мышления (∑203).
- Риск сохраняющегося кибертерроризма и кибершпионажа, осуществляемых иностранными террористическими организациями (∑202).
- Риск «кражи личности» вследствие внедрения единого идентификационного документа личности (∑201).
- Риск имеющейся достаточно высокой степени зависимости от импортных поставок в ряде секторов российской экономики (∑200).
- Риски снижения репутации компаний и доверия к ним вследствие роста конкуренции в IT-секторе экономики (∑199).
- Риск отсутствия возможности внедрения инновационных технологий вследствие низкого

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	∑
1		9	9	3	8	3	6	8	3	7	8	5	8	6	9	6	5	5	8	9	6	7	3	7	5	7	6	8	9	6	9	5	7	6	7	223
2	3		3	2	2	8	8	9	6	9	5	5	8	7	8	8	8	5	5	6	4	4	5	7	6	9	3	6	6	7	6	9	8	8	6	209
3	7	4		6	7	4	7	6	7	6	9	7	9	8	8	8	8	7	7	4	3	2	6	4	9	8	3	3	8	6	4	8	7	7	8	216
4	7	1	7		9	6	6	8	6	4	8	8	6	7	6	8	6	8	6	6	3	3	3	3	7	8	4	5	5	3	5	8	4	7	9	209
5	9	2	9	2		5	6	5	3	5	8	9	8	7	4	7	5	9	6	5	3	1	5	6	7	6	3	6	8	8	8	6	3	6	8	198
6	1	6	3	7	4		9	8	7	9	6	8	9	6	7	9	7	8	7	2	2	1	6	6	8	6	4	5	6	8	6	4	5	5	7	202
7	2	4	4	6	4	9		8	9	8	6	5	6	4	4	9	9	5	5	3	8	7	5	3	6	8	6	6	4	7	5	6	7	5	5	189
8	2	5	3	4	5	9	9		8	9	5	7	4	3	2	7	7	7	5	5	3	5	6	3	3	6	3	8	7	9	7	6	8	6	6	192
9	3	6	2	3	3	9	9	9		9	7	6	7	6	9	7	9	6	3	4	5	6	5	4	5	5	5	5	4	9	9	4	6	4	8	201
10	6	4	1	3	4	8	8	9	9		6	8	6	4	8	8	6	7	1	7	7	3	3	3	6	5	4	6	2	7	7	3	7	5	7	188
11	8	6	7	6	7	7	7	7	4	4		6	5	6	7	9	7	9	2	9	9	4	4	4	5	4	5	5	3	8	8	5	7	6	9	209
12	9	5	8	6	9	6	5	5	5	5	7		6	6	8	5	7	1	6	3	1	6	3	6	6	6	5	7	1	7	7	6	4	9	8	194
13	8	5	8	7	8	8	8	7	3	7	8	5		7	7	6	5	2	4	4	2	3	5	3	8	7	4	9	2	9	9	3	3	7	8	189
14	9	7	9	8	8	8	8	6	7	7	8	4	4		5	7	6	2	5	3	2	5	5	5	3	5	6	1	6	3	1	5	6	7	6	187
15	6	8	6	7	6	8	6	4	5	8	5	2	2	1		5	4	3	6	2	3	4	3	4	5	6	5	2	4	4	2	6	6	8	6	165
16	6	9	8	7	4	7	5	6	8	6	6	1	2	1	4		3	7	5	5	5	4	5	5	7	6	9	2	5	3	2	5	3	6	8	170
17	8	8	9	6	7	9	7	6	9	9	8	2	3	2	3	5		5	2	7	8	4	2	6	4	9	8	3	6	2	3	6	3	3	6	188
18	6	5	6	4	4	9	9	4	9	6	5	5	4	3	5	6	5		3	5	3	5	3	3	3	7	8	5	9	3	3	5	4	5	5	174
19	4	7	4	3	2	7	7	3	9	6	3	5	4	4	5	5	6	7		6	6	4	4	5	5	3	5	8	1	5	6	3	3	6	5	166
20	3	6	6	3	3	8	8	5	9	5	4	3	5	6	6	4	6	7	5		7	4	6	6	5	5	5	5	2	6	6	4	4	5	4	174
21	4	6	5	3	1	8	7	4	5	4	3	5	6	4	8	5	6	3	4	5		6	3	7	7	3	9	6	2	5	3	3	6	6	6	168
22	4	7	2	2	1	7	7	7	6	7	5	5	5	5	9	7	7	1	7	7	3		4	6	6	4	5	5	6	4	5	5	3	8	7	179
23	2	9	1	2	1	8	5	8	3	6	5	6	4	3	7	9	9	2	9	9	2	5		5	4	5	2	9	8	4	2	5	5	3	5	172
24	5	8	2	3	2	9	8	8	7	8	3	8	5	5	7	7	1	6	3	1	3	3	3		5	5	3	6	3	5	3	3	4	5	6	168
25	7	9	5	4	3	6	3	3	3	4	5	9	7	6	6	4	2	4	4	2	4	4	5	5		6	4	5	5	8	7	6	6	5	5	171
26	9	9	5	4	4	3	3	3	4	3	4	7	9	7	8	5	2	5	3	2	5	6	6	5	6		3	4	7	9	8	5	6	6	4	179
27	9	2	3	6	4	6	4	4	1	4	5	7	7	3	9	7	3	6	2	3	5	3	7	8	7	5		6	8	6	7	7	7	8	5	184
28	6	7	6	6	3	5	2	2	1	2	3	6	3	4	7	9	7	5	5	5	7	7	5	5	5	6	6		9	8	7	8	8	9	7	181
29	2	3	3	6	5	4	5	2	4	3	3	4	5	5	6	4	2	1	8	5	8	3	6	5	6	4	3	4		5	5	9	8	7	9	162
30	1	9	4	7	2	5	6	3	3	4	2	3	2	9	8	4	3	2	9	8	8	7	8	3	8	5	5	5	7		6	6	7	7	7	183
31	3	4	9	7	8	7	5	1	4	2	6	4	3	6	3	5	4	3	6	3	3	3	4	5	9	7	6	6	6	4		8	3	8	8	179
32	8	7	7	8	9	7	7	4	6	5	7	4	4	3	3	3	4	4	3	3	3	4	3	4	7	9	7	5	5	6	6		9	9	9	192
33	7	6	8	5	8	7	6	5	8	6	5	6	4	6	4	6	6	4	6	4	4	1	4	5	7	7	3	5	4	6	7	7		7	7	181
34	9	8	9	7	6	6	7	6	6	5	8	6	3	5	2	4	6	2	2	1	2	3	6	7	6	2	3	4	3	7	8	8	9		9	186
35	9	8	9	8	7	4	7	5	6	5	8	6	5	4	5	5	6	3	4	4	3	4	7	8	6	3	3	4	3	9	9	8	9	9		203
∑	192	209	189	171	168	220	210	188	183	187	184	187	178	169	207	213	187	161	166	157	150	141	158	173	202	187	163	179	174	206	196	195	185	218	230	

Рис. 1. Матричная модель рисков и угроз.

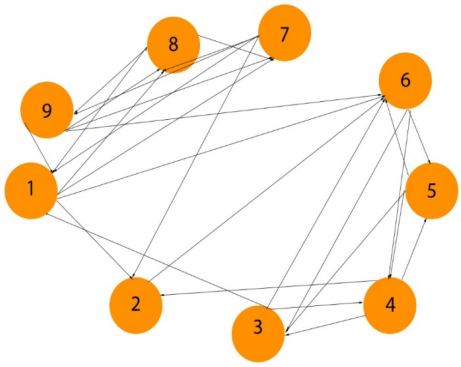

Рис. 2. Взаимосвязи дискретно-ситуационной сети.

уровня технологической грамотности населения (∑198) [5, с. 23].

И 10 рисков для объекта:

- Риск сохраняющегося кибертерроризма и кибершпионажа, осуществляемых иностранными террористическими организациями (∑230).
- Риск потери способности глубокого аналитического осмысления и ситуационного мышления (∑230).
- Риск роста реальных угроз в отношении национальной кибербезопасности (∑220).
- Риск возникновения неспособности адекватно планировать и прогнозировать будущее (∑218).
- Риск недостаточности проверенных методик и нормативных инструментов, позволяющих стандартизировать и регулировать разработанные технологии (∑213).
- Риск отсутствия полного контроля за автономными роботомашинными системами, способными к самоорганизации (∑209) [6, с. 26].
- Риск внедрения в разнообразные виды деятельности чужих технологических решений IT-сферы, что снижает суверенитет с повышением его уязвимости (∑207).
- Риск образовательной системы — «отмирание» старых профессий и появление новых (∑206).
- Риски, определяющиеся демографическими особенностями (∑202).
- Риск извлечения данных из гигантских объемов информации с помощью применения технологий Big Data (∑197).

Представленные результаты исследования рисков позволяют определить следующие положительные эффекты от внедрения цифровой экономики:

- Простота центрального управления;
- Глобальная автоматизация и стандартизация решений;
- Снижение риска влияния бюрократии и коррупции;
- Рост «прозрачности» государственной деятельности;
- Упрощение политической жизни;
- Полное снятие национального вопроса;
- Минимизация влияния человеческого фактора;
- Повышение производительности труда.

В заключение следует отметить, что суверенитет и национальная безопасность России все больше становятся уязвимы в условиях открытой рыночной экономики и санкционной войны со стороны западных недружественных стран.

Таблица 1. Элементы дискретно-ситуационной сети.

Проблемные ситуации (ПС)	1	2	3	4	5	6	7	8	9	Сумма причин
Сложность в контроле и прекращении внедрения новых технологий (1 класс)		3				4	5	3		15
Отсутствие равных возможностей у регионов для внедрения инновационных технологий. (1 класс)						4				4
Необходимость соблюдения при внедрении новых технологий национальных интересов по обеспечению безопасности информации. (1 класс)	5			3		2				10
Риски коррупции и олигархии (2 класс)		4	4		5					13
Отсутствие целей и задач создания цифровой экономики (2 класс)			3	5		5				13
Внешние и внутренние препятствия реализации программ цифровой экономики (2 класс)			3	5	4					12
Рост безработицы из-за роботизации некоторых видов деятельности (3 класс)	3	5						3	4	15
Развитие у молодежи машинного мышления и отсутствие воображения (3 класс)	3						4		5	12
Зависимость от гаджетов и от технологий IT-отрасли (3 класс)	2					3	5	5		15
Сумма следствий	13	12	10	13	9	18	14	11	9	109

В период глобального развития инновационных технологий в качестве противодействия санкционным мерам должно выступать развитие собственных информационных технологий, поскольку использование западных технологий и одновременная защита суверенитета России невозможны [7].

Цифровая трансформация становится очередным этапом в эволюции, на котором разрабатываются и внедряются новые технологии, позволяющие улучшить привычные процессы в деятельности, от которых в большинстве своем бизнес и общество получают дополнительные выигрыши.

Рост благополучия общества вследствие применения новых технологий не оспаривается теми, кто готов к трансформированию своей деятельности, кто способен оценить достоинства новых технологий, несмотря на всевозможные риски их внедрения [2].

Библиографический список

1. Актуализация особенностей разработки системы стратегического управления экономикой России / А. Е. Карлик [и др.] // Международная конференция по мягким вычислениям и измерениям. — 2017. — Т. 2. — С. 303—306.
2. *Волкова Э. С.* Механизм управления стратегическим позиционированием современного предприятия // Экономические науки. — 2025. — № 242. — С. 622—627. — DOI: 10.14451/1.242.622.
3. *Волкова Э. С.* Системный подход к рискозащищенной технологии стратегического управления на основе когнитивного моделирования : Сборник научных трудов XXV Международной научной и учебно-практической конференции. В 3-х частях, Санкт-Петербург, 13–14 октября 2021 года. Часть 1 // Системный анализ в проектировании и управлении. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2021. — С. 338—341. — DOI: 10.18720/SPBPU/2/id21-76.
4. *Волкова Э. С.* Стратегическое планирование деятельности предприятий электроэнергетики. — СПб. : Скифия-принт, 2022. — 108 с. — ISBN 978-5-98620-579-3.
5. *Гаджиев М. М.*, *Яковлева Е. А.* Диагностика проблемных ситуаций в социально-экономических системах: сетевые формы взаимодействия // Управление экономическими системами: электронный научный журнал. — 2018. — 3 (109). — С. 2—3.
6. *Гаджиев М. М.*, *Яковлева Е. А.* Функциональная диагностика деятельности предприятий на основе теории адаптивного управления и анализа проблемных ситуаций в условиях информационно-сетевой экономики // Управление экономическими системами: электронный научный журнал. — 2018. — 3 (109). — С. 2—6.
7. Методическое обеспечение системы стратегического планирования / Б. Л. Кукор [и др.]. — М. : Русайнс, 2025. — 156 с. — ISBN 978-5-466-08785-7.
8. Модели выявления приоритетов для инновационных компаний / В. Н. Волкова [и др.] // Международная конференция по мягким вычислениям и измерениям. — 2016. — Т. 2, № 4—7. — С. 279—282.
9. Рискоориентированная технология информационного обеспечения в условиях цифровой экономики: управление рисками в электроэнергетике / М. Б. Игнатьев [и др.] // Экономические науки. — 2018. — 4 (161). — С. 21.
10. *Яковлева Е. А.*, *Козловская Э. А.* Инновационное развитие экономики (концепция импортозамещения) // Вестник Финансового университета. — 2016. — Т. 20, 6 (96). — С. 54—62.