

*Петров Александр Николаевич,
з.д.н., науки, д.э.н., профессор, первый проректор СПбГЭУ, заведующий
специализированной кафедрой ПАО «Газпром»
Россия, Санкт-Петербург*

*Сулейманкадиева Алжанат Эльдеркадиевна,
д.э.н., профессор специализированной кафедры ПАО «Газпром»,
руководитель академического отделения института магистратуры
Санкт-Петербургского государственного экономического университета
Россия, Санкт-Петербург*

Управление корпоративными рисками в условиях цифровой экономики

Corporate risk management under the conditions of digital economy

Аннотация: В статье исследуются специфика цифровой экономики и анализируются наиболее вероятные риски, связанные с переходом на цифровые технологии. В статье делается упор на корпоративный уровень рисков, рассматриваются как риски, связанные с мошенничеством и коррупцией, доступом коррупционеров к информационной системе управления, так и риски, связанные со сбоями в самой информационно-коммуникационной системе и вероятностью потери объективных данных. Авторами уделяется большое внимание процессу и механизму управления корпоративными рисками, в связи с чем предлагается универсальная модель управления корпоративными рисками, включающая как этапы цикла управления (выявления рисков, анализа и реагирования на риски), так и методы/инструменты и заинтересованные стороны в управлении (в том числе в перераспределении) рисками

Ключевые слова: цифровизация экономики, корпоративные риски, модель управления рисками

Abstract: The article explores the specifics of the digital economy and analyzes the most likely risks associated with the transition to digital technology. The article focuses on the corporate level of risks, considers both the risks associated with fraud and corruption, the access of corrupt officials to the management information system, and the risks associated with failures in the information and communication system itself and the likelihood of losing objective data. The authors pay great attention to the process and mechanism of corporate risk management, in connection with which a universal model of corporate risk management is proposed, including both the stages of the management cycle (identifying risks, analyzing and responding to risks), as well as methods / tools and stakeholders in management (in including redistribution) of risks

Keywords: digitalization of the economy, corporate risks, risk management model

Введение. Специфика цифровизации экономики. Спецификой современной экономики является ее всеобщая цифровизация и ее инновационный характер развития, которые совместными усилиями ведут глобальное общество к сингулярности. *Цифровую (инновационную) экономику* можно определить как форму хозяйствования, где важнейшим фактором производства являются цифровые данные, в котором систематизация и обработка большого объема информации и анализ полученных результатов дают возможность повысить конкурентные преимущества любой современной компании. Сегодня наступили такие времена, когда любой менеджер, сидя за кухонным столом» может найти и делового партнера, и стратегического клиента, и поставщика, и даже конкурента, который сможет помочь определиться с приоритетными направлениями развития бизнеса. В условиях современной экономики происходят необратимые трансформационные процессы, которые существенно меняют основные корпоративные и управленческие функции компаний, а тем самым, образ жизни, культуру, систему ценностей, компетентностную и ментальную модель лиц, принимающих управленческие решения. Эти процессы можно обосновать появлением таких информационно-управленческих технологий, как: 1) концепция процессного управления компанией (*BPMS*) [1], в которой бизнес-процессы выступают в роли особых ресурсов компании, способных чутко реагировать даже на слабые сигналы внешней среды и быстро адаптироваться к ним. Основным инструментом управления в данной концепции выступает технологическое программное обеспечение поддержки *BPMS* на основе различных языков программирования, таких как: *BPMN*, *EPC*, *IDEFO* и программных систем таких, как: *BPEL*, *YAWL* и др.; 2) современные сервисы (например, *Azure Stream Analytics*), позволяющие обрабатывать потоки данных в режиме близкого к реальному времени и мгновенного получения результатов и реагирования на них; 3) технология распределенного реестра (*DLT*), которая представляет собой децентрализованную электронную систему БД, распределенную между несколькими сетевыми узлами или устройствами. Эта система дает возможность записывать и хранить информацию в сети без единого контролирующего органа [7]; 4) *кибербезопасность*, которую можно понимать как некий набор политик, концепций, инструментов, мер и/или руководств, подходов (методов), для обеспечения безопасности, процесса управления рисками, обучения, а также распространения лучших практик, обеспечения гарантий и т.д. [2]. Актуальность существования этой системы обоснована необходимостью обеспечения как компьютерной и информационной безопасности компаний, так и создания гарантий безопасности жизни людей.

Можно сказать, что, с одной стороны, все эти инновационные явления и процессы, протекающие в современной цифровой (инновационной) экономике, в корне меняют смысл и образ жизни современного человека, систему ценностей современного общества и культуру его в целом; с другой, – видим, что изменения протекают с такой скоростью, что многие

футурологи однозначно предсказывают скорое наступление эпохи сингулярности, в которой будет выжить и человеку, и компаниям без стратегии управления рисками достаточно сложно.

В этой связи многие компании видят источником выживания создание сетевых корпоративных структур, в которых каждая компания, вступающая в сеть, преследует собственные интересы [4]. При этом интересами участников сети могут быть: а) получение доступа к ресурсным источникам, в том числе к информационному ресурсу; б) поиск и удержание своего статуса на рынке товаров и услуг; в) поддержание бренда компании и повышение интеллектуального потенциала участника сети и всей сети, в целом; г) возможность перераспределения корпоративных рисков между участниками сетевой структуры. Таким образом, можно отметить, что выбирая путь вступления в сеть, каждая компания-участник сетевой структуры получает ряд преимуществ.

Следует отметить, что управление рисками (в том числе корпоративными рисками) представляет собой одновременно и процесс, и достаточно сложный механизм формирования модели управления ими, распределения непредсказуемых корпоративных рисков между участниками сетевой структуры, в которую все чаще вступают компании, чтобы обеспечить свою жизнеспособность.

Выше сказанное позволяет сформулировать цель данной работы, которая заключается в формировании общего механизма управления корпоративными рисками с сетевой структуре в условиях цифровизации экономики.

Макро- и микроэкономические (корпоративные) риски в условиях цифровой экономики

В условиях цифровой экономики роль и значение управления рисками (как общими, так и корпоративными) приобретают особую актуальность. Связано это с тем, что наряду с существующими видами рисков появляются новые, не известные ранее. Кроме того, те риски, которые имели место в обществе и в компаниях ранее, приобретают новое содержание в условиях цифровой экономики.

Так, для современного общества (и компаний в том числе) в условиях цифровой экономики характерны следующие виды общих и корпоративных рисков, которые классифицируются по уровневому подходу (табл.1).

Таблица 1 – Виды макро- и микроэкономических (корпоративных) рисков в зависимости от уровня управления¹

№	Уровень и вид риска	Содержание
1	<i>Риски макроэкономического уровня</i>	
1.1	Технологический	Вызван разбалансировкой развития реального сектора экономики и темпов развития цифровой экономики. Это связано с тем, что одни отрасли и сектора реальной

¹ Таблица составлена авторами на основе анализа работ [3, с. 22-29; 5, с. 184-272; 6]

		экономики развиваются ускоренными темпами, а другие развиваются медленнее, следовательно, несоответствие темпов развития разных секторов и отраслей экономики как уровню и требованиям цифровой экономики, та и друг другу ведет к тому, что внутри социально-экономической системы возникает конфликтная ситуация, экономика не может развиваться инновационным путем и не может обеспечить синхронный переход всех ее секторов и отраслей к цифровой экономике
1.2	Социальный	Свидетельствует о формировании атмосферы социальной напряженности, которая связана с ростом безработицы, вызванной следующими явлениями, как: а) потеря работы и необходимость переобучения немолодых (возрастных) людей новым менее квалифицированным и малооплачиваемым специальностям; б) неблагоприятный прогноз положения высококвалифицированных специалистов, которые окажутся до последнего момента задействованными в процессе перехода к цифровым технологиям организации производства и после перехода будут не востребованными на новых должностях, так как они уже будут заняты; в) увеличение коэффициента Джинни, связанное с усилением неравенства доходов населения, следовательно, усугубление социально-экономического неравенства в обществе; г) ухудшение физического состояния и психологические расстройства, вызванные изменением характера и содержания труда современных работников, увеличением количества времени, которое работник проводит за компьютером, в виртуальном мире, увеличением общей нагрузки на организм человека и ухудшением его общего физического и психологического состояния; д) усиление конкуренции за рабочее место и появление микрокультуры, которая не поддерживает общепринятую в обществе систему ценностей и норм поведения
1.3	Риск снижения профессионального мастерства специалистов	Связан с тем, что переход к цифровой экономике сопряжен многократными сменами профессий работником, так как квалификация специалиста быстро теряет свою актуальность. Одни профессии сменяются другими, и эта ситуация, в конечном счете, потребует непрерывного обучения, переквалификации или повышения квалификации работников. Эта ситуация ведет к росту затрат времени и ресурсов
1.4	Риск запаздывания образовательной системы	Связан с несоответствием системы образования требованиям новой цифровой экономики. Если скорость отмирания профессии составляет 7-10 лет, а подготовка специалиста по новой профессии занимает в среднем 4 года, следовательно, преподаватели должны обучаться с гораздо большей скоростью, то есть непрерывно должны повышать квалификацию и/или проходить переподготовку
1.5	Риск техногенного характера	Связан с загрязнением экологии, болезнями и авариями, вызванными сбоями в информационно-технических системах (в том числе системах цифровой обработки)

		данных)
1.6	Риск информационно-технического воздействия со стороны зарубежных стран (страновой риск)	Допускает воздействие на информационную и техническую инфраструктуру экономики России со стороны зарубежных государств в политических, социально-экономических, военных и биотехнологических целях
2	<i>Риски микроэкономического (корпоративного) уровня</i>	
2.1	Риск мошенничества с цифровыми данными	Выражен в том, что с приходом цифровой экономики: а) участились мошенничества, которые связаны с безналичными (нематериальными) деньгами на банковских счетах; б) появились преступления в сфере недвижимости, с помощью цифровой подписи, а также связанные с юридическим сопровождением сделок в виртуальном мире; в) появилось такое явление, как киберпреступность, которая связана не только с информационной безопасностью компании или личности, но и военного и промышленного комплекса в целом; г) увеличились преступления, связанные с нарушением конституционных прав и свобод человека, касающихся неприкосновенности его частной жизни, личной и семейной тайны при обработке персональных данных с использованием ИТ
2.2	Риск развития коррупции в цифровой экономике	Создает условия недоверия и напряжения лиц, принимающих управленческие и финансовые решения в виртуальном мире, так как существует опасность получения коррупционерами доступа к паролям, никам и кодам, с помощью которых совершаются финансовые (инвестиционные) сделки и принимаются управленческие решения. Таким образом существует опасность того, что коррупционер может пользоваться материальными благами, не раскрывая своей личности, анонимно. Кроме того, для того, чтобы выявить и наказать его удастся только благодаря организации непрерывного наблюдения за его действия и идентификации совершенных им расходов со счета
2.3	Риск сопротивления внедрению цифровой экономики	Связан с тем, что если сотрудники компании или подразделения не способствуют активному внедрению информационных технологий, не повышают свою квалификацию в соответствии с требованиями новой экономики или сопротивляются этому процессу, то неминуема участь банкротства компании и потери работы работниками
2.4	Риск сбоев в информационной системе	Существует на начальном этапе формирования цифровой экономики, так как именно на данном этапе наиболее вероятны сбои в информационно-коммуникационных системах и ИТ любого уровня управления

Условия современной экономики таковы, что цифровая экономика наступает вопреки интересам человечества и темпы ее наступления также не зависят от его желаний. Цифровизация общества происходит по экспоненциальному закону. И эти изменения приходится учитывать и

приспосабливаться к ним. Несомненно, для своевременного реагирования и безболезненной адаптации к изменениям цифровой экономики целесообразно своевременно принять к учету возможные виды рисков и подготовиться к ним.

Несмотря на существование большого количества рисков в условиях всеобщей цифровизации, в соответствии с целью данной работы отметим, что существует общий механизм управления корпоративными рисками. Эта модель достаточно популярно описана в работе [5], в которой все риски распределяются по уровневому подходу внутри сетевой компании (рис. 1). В этой модели выделяются еще и заинтересованные стороны распределения уровней корпоративных рисков.

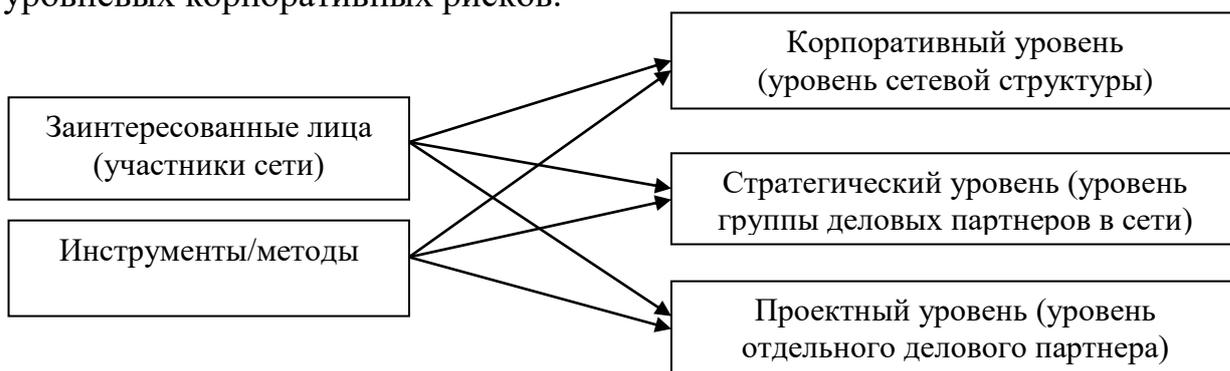


Рисунок 1 – Механизм управления корпоративными рисками

На рис. 1 очевидно, что в сетевой структуре участвует большое количество заинтересованных лиц (кроме доминантной компании сети) в перераспределении корпоративных рисков. Следовательно, инструменты/методы, которыми они будут руководствоваться в управлении рисками на соответствующем уровне будут разными.

Цикл управления корпоративными рисками сети независимо от типа сетевой структуры и уровня корпоративного риска включает в себя процесс непрерывного выявления и анализа (оценки) рисков и реагирования на них. Модель управления корпоративными рисками сетевой структуры выглядит следующим образом (рис. 2).

Эта модель управления корпоративными рисками сетевой структуры является универсальной для рисков сети любого уровня управления. В ней продемонстрированы и механизм оценки, и место заинтересованных сторон распределения и управления рисков, а также показана взаимосвязь цикла управления, включающего в себя три основных этапа (выявление рисков, анализ (оценка рисков) и реагирование на них). Следует отметить, что процесс управления рисками является непрерывным и постоянным в деятельности компании (сетевой структуры) независимо от типа структуры управления.

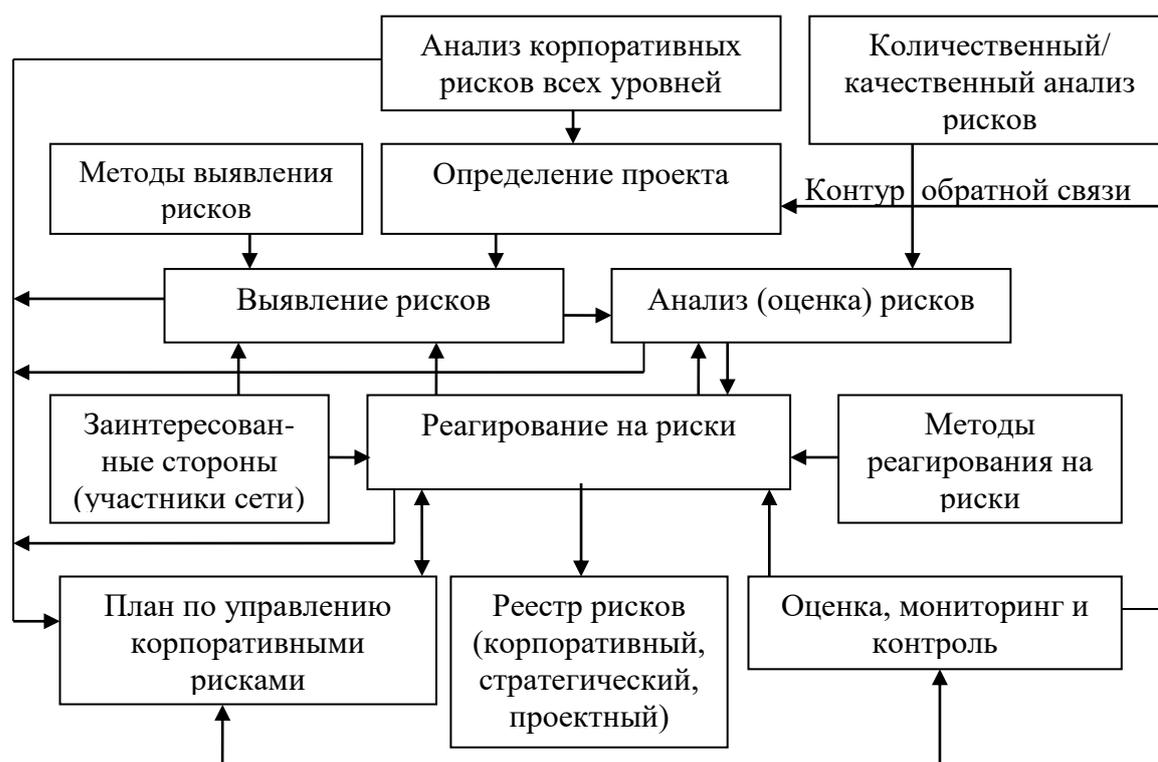


Рисунок 2 – Модель управления корпоративными рисками всех уровней

Заключение. Специфика развития цифровой экономики в современном обществе вносит свои коррективы в естественный ход развития цивилизации, которая заключается, прежде всего, в том, что с ней сопряжены новые виды рисков (как макроэкономические, так и корпоративные). В этой связи нами был проведен анализ типов рисков, связанных именно с цифровизацией экономики и их влиянием на корпоративный уровень. Выделены такие типы рисков корпоративного уровня, как: риск мошенничества с цифровыми данными, риск развития коррупции в цифровой экономике, риск сопротивления внедрению цифровой экономики и риск сбоев в информационно системе. В таблице приведены лишь часть наиболее возможных типов рисков, хотя в реальной жизни возможны и другие их разновидности.

Авторами данной работы предложена наиболее универсальная схема модели управления рисками, которая: а) является объективной для любого уровня управления корпоративными рисками; б) включает в себя и процесс цикла управления, и механизм управления ими с отдельными элементами и участниками (заинтересованными сторонами) в перераспределении рисков между участниками сетевой структуры; в) позволяет обеспечить координацию и непрерывность процесса мониторинга и управления рисками из единого центра (доминирующей компании) сетевой структуры.

Библиографический список:

1. BPM (управленческая концепция) [Электронный ресурс]// <https://ru.wikipedia.org/wiki/> (Дата обращения 09.05.2020).

2. Зачем нам нужна кибербезопасность? [Электронный ресурс]// <https://mega-obzor-ru.turbopages.org/s/mega-obzor.ru/chto-takoe-kiberbezopasnost.html> (Дата обращения 09.05.2020)
3. Зверева Т. В. Экономические риски цифровой экономики// Риски цифровой экономики Проблемы анализа риска, том 14, 2017, № 6. С. 22-29
4. Сулейманкадиева А.Э., Хорева Л.В. Сетевой менеджмент в условиях экономики импортозамещения. Монография. СПб.: СПбГЭТУ («ЛЭТИ»). 91 с.
5. Управление рисками корпорации: учебное пособие/А.М. Аронов [и др.]; под ред. А.Н. Петрова. – СПб.: Изд-во СПбГЭУ, 2019. 289 с.
6. Чалдаева Л. А. Риски цифровой экономики и технологии контроля на микро- и макроуровне/ [Электронный ресурс]/ http://debaty.club/sites/default/files/dd2017/Chaldaeva_Kilyachkov_Presentation_DD2017.pdf (Дата обращения 19.06.2020)
7. Что такое технология распределенного реестра [Электронный ресурс]// <https://beincrypto-ru.turbopages.org/s/beincrypto.ru/chto-takoe-tehnologiya-raspredeleennogo-reestra/> (Дата обращения 09.05.2020).