DOI: http://dx.doi.org/10.21686/2413-2829-2024-5-200-209

КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ УПРАВЛЕНИЯ: ПРИЧИННО-СЛЕДСТВЕННЫЕ СВЯЗИ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ

О. Ю. Кириллова, С. Г. Васин
Российский экономический университет имени Г. В. Плеханова,
Москва, Россия

Понятие корпоративной безопасности появилось в конце XIX в., но широкое использование этого термина и его распространение в бизнес-среде произошло во второй половине XX в. Это понятие вводилось в оборот для обозначения системы мер и практик, направленных на защиту корпоративных интересов и ресурсов компании от внутренних и внешних угроз. Корпоративная безопасность компании является сложным комплексом мер и процедур управления рисками и объектом управления с принципиально новым содержанием, актуальность которого обостряется рисками устойчивого развития. Партнеры по бизнесу, компаньоны, клиенты компании и другие заинтересованные в ее деятельности лица все чаще переносят свое общение в электронную среду, где происходят непредсказуемые изменения и возникают новые виды рисков. Это вызывает трансформацию отдельных видов рисков, таких как финансовый, инвестиционный, репутационный, регуляторный и др. Перманентное изучение трансформации рисков, важности и значимости их влияния на бизнес и экономику, на устойчивое развитие компаний необходимо внедрить как обязательную функцию в рамках подсистемы корпоративной безопасности компании. В статье авторами обосновано, что для своевременной оценки влияния новых рисков и внешних факторов на устойчивое развитие компаний и их бизнеса необходима реструктуризация систем внутреннего контроля в организациях с учетом корпоративной безопасности как элемента системы корпоративного управления.
Ключевые слова: бизнес-процессы, ESG-риски, внутренние и внешние угрозы, институциональная среда бизнеса, корпоративное управление, управление рисками, устойчивое развитие организации (компании).

CORPORATE SECURITY AS SUBJECT TO MANAGEMENT: CAUSE-AND-EFFECT RELATIONS IN ARISING AND DEVELOPMENT

Oksana U. Kirillova, Sergey G. Vasin
Plekhanov Russian University of Economics,
Moscow, Russia

The notion of corporate security came into being in the late 19th century, however the use and spread of the term in business-environment took place only in the second half of the 20th century. This notion was introduced into circulation to name a system of measures and practices aimed at protection of corporate interests and resources from internal and external threats. Corporate security of the company is a complicated set of measures and procedures for managing risks and at the same time a subject to management with a brand new content, whose topicality is sharpening due to risks of sustainable development. Business partners, company clients and other concerned persons often transfer their communication to the e-environment, where unpredictable changes take place and new risks arise. It can result in transformation of certain types of risks, such as finance, investment, reputational, regulatory, etc. Continuous study of risk transformation, importance of their impact on business and economy, sustainable development of companies shall be introduced as a mandatory function within the frames of sub-system of company corporate security. The authors showed that for timely appraisal of new risk and external factor impact

on sustainable development of companies and their business it is necessary to restructure the system of in-company control with regard to corporate security as an element of the system of corporate management.
Keywords: business-processes, ESG-risks, internal and external threats, institutional environment of business, corporate management, risk management, sustainable development of the organization (company).

Вопросы обеспечения и сохранения капитала, вложенного в ту или иную компанию, его преумножения интересуют многих собственников. Многих из них также интересуют аспекты роста капитализации активов и устойчивое развитие компаний, в которых они разместили свои инвестиции. На решение этих задач направлен принцип рискориентированности систем корпоративного управления, требующий от каждой конкретной компании создания контура корпоративной безопасности, обеспечивающей превентивное предотвращение внешних и внутренних рисков, угрожающих ее жизнестойкости в рыночной среде.

В общем смысле корпоративная безопасность (КБ) подразумевает готовность компании противостоять любым угрозам, снижающим ее устойчивость. Это комплексное многоаспектное понятие сформировалось как концепция предотвращения разнообразных рисков, предусматривая противостояние им не в отдельности, а в понимании их взаимосвязи и взаимовлиянии, возможности трансформации внешних рисков во внутренние, меняющей значимость ущерба и неотложность принятия мер по их нейтрализации.

Корпоративная безопасность охватывает широкий спектр аспектов, включая физическую, информационную и финансовую безопасность, защиту интересов акционеров, соблюдение законодательства и этических норм.

Влияние концепции корпоративной безопасности на систему корпоративного управления и оргструктуру компании заключается в интеграции безопасности в стратегическое планирование и принятие решений. Оно может привести к созданию специализированных отделов или должностей по безопасности, установлению политик и процедур, обеспечению обучения и осведомленности сотрудников. Кроме того, корпоративная безопасность может потребовать изменений в оргструктуре компании, чтобы усилить координацию и синергию работы между различными функциональными подразделениями и защитить интересы организации от потенциальных угроз.

Понятие корпоративной безопасности эволюционировало на протяжении длительного времени, и его начало можно проследить с конца XIX в. Однако более широкое использование этого термина и его распространение в бизнес-среде произошло во второй половине XX в.

Введение понятия корпоративной безопасности в оборот связывают с ученым Эдвардом Гиббсом, который в 1954 г. опубликовал свою работу Industrial Espionage and Technology Transfer: Europe vs. the United States, в которой предложил использовать понятие «корпоративная безопасность» для обозначения системы мер и практик, направленных на защиту корпоративных интересов и ресурсов от внутренних и внешних угроз. Являясь экспертом в области корпоративной безопасности, Э. Гиббс разработал концепцию под названием «треугольник безопасности», согласно которой корпоративная безопасность – это сбалансированное сочетание мер по защите, предупреждению и реагированию на угрозы, которые могут причинить ущерб организации, ее сотрудникам, активам и репутации.

В своей концепции Э. Гиббс выделил три компонента корпоративной безопасности:

1. *Физическая безопасность* – обеспечение защиты физической инфраструктуры организации и ее активов от угроз, таких как кражи, вандализм или террористические акты.

2. *Информационная безопасность* – обеспечение защиты информационных ресурсов и данных организации от несанкционированного доступа, кибератак и других угроз, которые могут повлечь утечку конфиденциальной информации или нарушение бизнес-процессов.

3. *Организационная безопасность* – это разработка и реализация политик, процедур и практик, которые обеспечивают безопасное и эффективное функционирование организации. Она включает в себя управление рисками, обучение сотрудников, планирование и реагирование на чрезвычайные ситуации и другие меры, направленные на минимизацию потенциальных угроз.

Таким образом, по определению Э. Гиббса, корпоративная безопасность включает в себя не только физическую охрану, но и превентивные и реагирующие меры для защиты информации и обеспечения безопасного функционирования организации в целом.

Корпоративная безопасность является комплексным подходом к обеспечению защиты организации от внутренних и внешних угроз, включая защиту персонала, имущества, информации и бизнес-процессов. Она содержит превентивные меры и мероприятия реагирования на возможности возникновения угроз, методы и практики, которые помогают минимизировать риски и обеспечить безопасность предприятия в условиях современного бизнеса.

Отдельные исследователи под определением термина «корпоративная безопасность» понимают такое состояние компании, при котором при прогнозировании ее деятельности мала вероятность возникновения внештатных ситуаций и действий неизвестных факторов. Другими словами, они подразумевают, что компания находится в безопасности, если результаты ее работы предсказуемы для руководства и она стабильно показывает требуемые результаты [5].

К наиболее зарекомендовавшим себя на практике *принципам корпоративной безопасности* относятся [6]:

1) комплексность;
2) актуальность;
3) целесообразность;
4) постоянность;
5) законность;
6) плановость;
7) дублирование;
8) специализация;
9) модернизация;
10) централизация.

Каждый из перечисленных принципов необходимо учитывать при построении подсистемы корпоративной безопасности как элемента системы корпоративного управления.

Понятие корпоративной безопасности тесно переплетается с системой контроля компании на всех уровнях – от операционного до корпоративного.

Под понятием «корпоративная безопасность» подразумевается совокупность мер и процессов, направленных на защиту организации от внутренних и внешних угроз. На текущем этапе экономического развития к корпоративной безопасности организации относятся:

1. *Физическая безопасность*: обеспечение безопасности зданий, территорий, сетей и систем компании, контроль доступа, видеонаблюдение, охрана.

2. *Информационная безопасность*: защита конфиденциальной информации, противодействие кибератакам, управление правами доступа, сетевая безопасность.

3. *Кадровая безопасность*: проверка сотрудников при приеме на работу, контроль над доступом к важным данным и ресурсам, обучение сотрудников правилам безопасности.

4. *Юридическая безопасность*: соблюдение законодательных требований, защита прав и интересов компании, управление регуляторными рисками и обеспечение соответствия нормативам.

5. *Бизнес-континуитет*: разработка планов на случай кризисных ситуаций, меры

для минимизации потерь при возникновении чрезвычайных ситуаций.

6. *Аналитика и мониторинг*: систематический анализ рисков и угроз, мониторинг ситуации и принятие мер для предотвращения инцидентов.

Рассмотрим, как данные аспекты реализуются на различных уровнях управления (рисунок).

Рис. Реализуемые виды и меры КБ по уровням в системе корпоративного управления

Институциональная среда бизнеса охватывает правила, нормы, законы и институты, которые регулируют деятельность организаций. Корпоративная безопасность и институциональная среда взаимосвязаны и влияют друг на друга. Эти правила определяют, как организации (компании) могут обеспечивать безопасность своих активов, сотрудников и операций. Институциональная среда влияет на корпоративную безопасность через создание законодательных и нормативных требований, которым организации должны соответствовать (комплаенс-меры). Она также может предоставлять поддержку и ресурсы для реализации мер безопасности.

С другой стороны, корпоративная безопасность может влиять на институциональную среду путем активного сотрудничества с правоохранительными органами, участия в разработке политик и законодательных инициатив в рамках процесса оценки регулирующего воздействия, направленных на повышение безопасности бизнеса. Таким образом, корпоративная безопасность и институциональная среда взаимосвязаны и дополняют друг друга, обеспечивая безопасность и защиту интересов организации.

ESG-повестка, актуализирующая ESG-риски (Environmental, Social, Governance), также накладывает ощутимый отпечаток на процессы и механизмы обеспечения корпоративной безопасности. На современном этапе экономического развития корпоративная безопасность связана с уче-

том факторов окружающей среды, социальной ответственности и управления в рамках бизнес-практик. Осознание и регулирование ESG-рисков становится все более важным для компаний, так как они включают в себя различные аспекты, такие как изменение климата, социальная справедливость и этические стандарты взаимодействия. Следовательно, корпоративная безопасность должна включать меры по управлению и снижению влияния ESG-рисков.

Содержание дефиниции «корпоративная безопасность» во многом зависит от определения сути корпоративного управления и корпорации как его субъекта. Понятие «корпоративное управление» до сих пор не имеет общепринятого определения, поэтому оно может толковаться и как способ управления компанией, и как отчетность управленцев перед акционерами, и как взаимодействие компании с ее стейкхолдерами. Мы придерживаемся точки зрения на предмет корпоративного управления компанией как на обеспечение эффективного взаимодействия всех заинтересованных в ее деятельности лиц. В исследованиях ряда российских ученых [5–7] понятие корпорации и корпоративности перешагивает барьеры акционерной формы собственности и количества участников компании. По нашему мнению, именно корпоративное поведение, выражающееся в следовании принципам ESG, определяет суть корпорации как объекта управления.

На основании проведенных исследований понятий «корпоративное управление» и «корпоративная безопасность» считаем возможным предложить следующее определение корпоративной безопасности как подсистемы корпоративного управления: *корпоративная безопасность компании – это совокупность мер и действий, направленных на защиту интересов организации (корпорации) от внутренних и внешних угроз, влияющих на взаимосвязи традиционных рисков, трансформирующих и меняющих их масштабы и вероятность наступления в системе функциональных составляющих, обусловленных соответствием материальных, финансовых, кадровых, технико-технологических, информационных потенциалов и организационной структуры компании ее стратегическим целям и задачам в текущей геополитической ситуации*.

В настоящее время приоритеты в учете рисков при обеспечении корпоративной безопасности зависят от конкретных потребностей и целей каждой организации. К общим приоритетам, которые учитывают многие компании, относятся следующие аспекты:

1. *Кибербезопасность*: защита от киберугроз, включая хакерские атаки, утечку данных, вредоносное программное обеспечение и другие киберпреступления.

2. *Физическая безопасность*: обеспечение безопасности зданий, помещений, периметра и доступа, включая контроль доступа, видеонаблюдение, охрану и противопожарные меры.

3. *Риски внутреннего характера*: учет угроз со стороны сотрудников, внутренних мошенничеств, воровства информации, несоблюдения политик и процедур.

4. *Управление кризисными ситуациями*: разработка и реализация планов действий в случае чрезвычайных ситуаций, таких как природные катастрофы, теракты, технологические аварии и т. д.

5. *Репутационные риски*: защита репутации компании, включая управление коммуникациями в случае инцидентов или кризисов.

6. *Регуляторные риски*: соблюдение законодательства и нормативных требований, соответствие законодательству о защите информации, требованиям по защите персональных данных, интеллектуальной собственности, финансовой отчетности и т. д.

Организации могут по-разному расставлять акценты, выстраивая систему корпоративной безопасности в зависимости от особенностей своей деятельности и бизнес-приоритетов. Важно, чтобы каждая компания разработала свою стратегию обеспечения безопасности, учитывая воз-

можные угрозы и риски, и обновляла ее в соответствии с изменяющейся обстановкой.

В настоящее время трансформация (видоизменение) рисков, влияющих на российский бизнес и экономику страны в целом, вызвана ростом воздействия внешних факторов, таких как международные санкции, неопределенность стратегий партнеров по бизнесу, хозяйственных связей в экономической системе и пр. Партнеры по бизнесу, компаньоны, клиенты компании и другие заинтересованные в ее деятельности лица все чаще переносят свое общение в электронную среду, где происходят непредсказуемые изменения и возникают новые виды рисков.

В своем исследовании Е. В. Жукова максимально полно оценивает значимость рисков. Ее вывод гласит, что «…. результаты оценки значимости рисков используются при определении подходов к управлению, в том числе методов оценки рисков, подходов к установлению риск-аппетита, методике стресс-тестирования, а также при формировании риск-отчетности» [4. – С. 620].

При реализации задач и стратегий устойчивого развития компании (в любой отрасли и сфере бизнеса) сталкиваются с тем, что происходит бифуркация (трансформация) тех или иных видов риска, факторов их проявления.

Корпоративная безопасность компании является сложным комплексом мер и процедур управления рисками и объектом управления с принципиально новым содержанием, актуальность которого обостряется рисками устойчивого развития. Традиционные риски бизнеса, к которым относятся экономические, финансовые, репутационные, политические, кадровые, а также риски форс-мажорных обстоятельств, под влиянием современных внешних воздействий и бурно развивающейся институциональной среды трансформируются, меняя свою важность и значимость для компании.

Рассмотрим новые и классические риски, которые тяжело предвидеть и от которых практически невозможно застраховаться.

Политический риск

Политика и ее наименее приятные последствия всегда были одними из главных факторов риска для бизнеса, но сегодняшние политические течения отличают особая непредсказуемость и глобальное влияние. Никто не мог предположить, что такая небольшая страна, как Греция, повлияет на мировые рынки, но политический кризис в стране повлек за собой экономический, а он в свою очередь привел к цепной реакции на мировых рынках. Кризисы, подобные греческому, и более громкие политические перевороты, как, например, Brexit, сегодня регулярно вторгаются в деятельность бизнеса по всему миру, и даже самые опытные аналитики не могут предсказать каждый из них. Из России в 2022 г. ушли многие иностранные компании. Не обсуждая суть политических решений, однозначно мы можем сказать, что уход иностранных компаний существенным образом отразился на экономико-хозяйственной деятельности российского бизнеса.

Риски, связанные с ликвидностью (финансовые риски)

Нестабильность мировых финансовых потоков была в полной мере выявлена во время международного кризиса 2008 г., но предвидеть похожие случаи в будущем по-прежнему крайне сложно. В одну минуту рынок может нормально функционировать, а в следующую – один из крупных банков может заявить о потере ликвидности. Такие риски атакуют бизнес быстро и внезапно, из-за чего менеджмент компаний особенно опасается их.

Риски, связанные со стоимостью ресурсов

Эти риски проще поддаются страховке, чем многие другие. Компании, которые в большой степени зависят от цены на природные ресурсы, должны постоянно следить за резкими изменениями на этих

рынках, чтобы заблаговременно компенсировать потери.

Риски форс-мажорных ситуаций

Природные катастрофы, массовые отключения электроэнергии, забастовки, взрывы и другие массовые непредсказуемые события – самые ощутимые риски для бизнеса. Статистика показывает, что 80% компаний, которые попали в эпицентр одного из таких форс-мажорных событий, не могут успешно восстановить бизнес и принимают решение о закрытии в течение месяца.

Риск отставания от инноваций

Достижения технологий делают нашу жизнь проще и удобнее, но для многих компаний инновации в их сфере деятельности могут стать непреодолимым препятствием. Бизнес-модели стареют со скоростью загрузки мобильного приложения, и компании, которые не успевают за инновациями, рискуют потерять многолетний прибыльный бизнес, однозначно столкнутся с появлением новых для них рисков и усилением важности существующих.

Кадровые риски

Кадровые риски реализуются в следующих случаях:

– при несоблюдении работниками трудовой дисциплины и нарушении требований этического кодекса;

– повышении уровня деструктивной конфликтности и стрессогенности организационной среды компании;

– неэффективной организационной структуре – дисбалансе полномочий и ответственности;

– недостаточном уровне профессиональной квалификации работников;

– текучести кадров;

– финансовых потерях (мошенничестве);

– свершении угроз информационной безопасности;

– невосприимчивости персонала к инновациям и изменениям;

– нарушениях трудового законодательства и некоторых других.

Репутационные риски

Это риски потери прибыли, клиентов или поставщиков вследствие неблагоприятного восприятия имиджа компании. Негативные отзывы и компрометирующие компанию материалы могут в одночасье уничтожить годами создаваемый ею имидж. При этом с ростом информационной прозрачности и доступности количество угроз для репутации компании по мере развития общественного сознания также растет.

Конкурентные риски

На любом рынке, в любой отрасли бизнеса всегда шла конкурентная борьба, механизмы которой достаточно подробно были описаны М. Портером в 5-факторной модели конкуренции (5 сил конкуренции) [8].

В настоящее время необходимо учитывать, что конкурентная борьба переходит в цифровое информационное пространство, которое меняет концепцию маркетинга, технологии продаж и формирования потребительских предпочтений.

Так, например, многие компании перешли не только к активной рекламе в Интернете, но и к прямым продажам и предложениям своих услуг на Big Data, OZON, Wildberries, Amazon.com и других подобных площадках. Это, несомненно, обостряет конкурентную борьбу и приводит к новым конкурентным и даже информационным рискам.

Регуляторные риски

Это риски несоблюдения внешних законодательных, административных и внутренних норм и правил, касающихся любых аспектов деятельности компании и, как следствие, возникновения риска финансовых потерь или иных негативных последствий для развития организации и ее функционирования. Существенную часть регуляторных рисков составляют внутрен-

ние комплаенс-риски, связанные с несоответствием деятельности компании ее внутренним процедурам, положениям, актам и иному локальному регулированию.

Риски изменчивости внешней среды

Последствия кризиса 2008 г. продолжают оказывать влияние на экономику, создавая многочисленные препятствия и угрозы развитию бизнеса по всему миру. Даже исторически стабильные государства зачастую вынуждены снижать целевые показатели экономического развития, а многие подающие надежды экономики, например, бразильская, и вовсе приходят к неожиданному краху. Следует отметить, что экономика большинства стран Евросоюза в настоящее время испытывает значительные затруднения из-за экспансии на их рынок дешевой сельскохозяйственной продукции. Изменчивость и неопределенность внешней среды также являются одними из основных рисков бизнеса, которые необходимо учитывать компаниям в любой отрасли промышленности и сфере бизнеса для организации своевременного реагирования на них.

Появляющиеся под воздействием внешних политических и экономических (санкционных) факторов новые риски вызывают изменение и традиционных (старых) рисков. Механизмы влияния новых рисков на старые постоянно меняются, нередко имеют латентный характер, что также не способствует стабильности и существенно затрудняет прогнозирование развития компаний. Перманентное изучение трансформации рисков, важности и значимости их влияния на бизнес и экономику, на устойчивое развитие компаний необходимо внедрить как обязательную функцию в рамках подсистемы корпоративной безопасности компании.

Для своевременной оценки влияния новых рисков и внешних факторов на устойчивое развитие компаний и их бизнеса необходима реструктуризация систем внутреннего контроля в организациях с учетом корпоративной безопасности как элемента системы корпоративного управления, позволяющей своевременно выявлять механизмы влияния рисков на устойчивое развитие. Корпоративную безопасность можно ассоциативно представить как двойную оболочку: внешний щит, как озоновый слой планеты, защищает компанию от «астероидов» – внешних негативных воздействий, а внутри – как фильтр, сдерживающий информацию, действия и контакты менеджмента компании, способные повлечь за собой существенные риски.

Список литературы

1. *Васин С. Г.* Проблемы управления корпоративной безопасностью в целях обеспечения устойчивого развития организации // Сборник докладов Всероссийской научно-практической конференции «Проблемы развития добросовестной конкуренции в эпоху цифровой экономики». – М. : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2024. – С. 8–15.

2. *Григорьев Н.* Построение корпоративной безопасности: как определить угрозы и обеспечить комплексную защиту бизнеса. – URL: https://www.cleverence.ru/articles/biznes/postroenie-korporativnoy-bezopasnosti-kak-opredelit-ugrozy-i-obespechit-kompleksnuyu-zashchitu-bizne/

3. *Жаринов И. О.* Корпоративное управление в цифровой экономике // Вестник Российского экономическолго университета имени Г. В. Плеханова. – 2021. – Т. 18. – № 6 (120). – С. 158–169.

4. *Жукова Е. В.* Стратегические приоритеты устойчивого развития и формирование алгоритма управления ESG-рисками // Креативная экономика. – 2022. – Т. 16. – № 2. – С. 611–628.

5. Корпоративная безопасность предприятия. – URL: https://falcongaze.com/ru/pressroom/publications/articles/korporativnaja-bezopasnost-predprijatija.html

6. Корпоративная безопасность предприятия: как определить угрозы и обеспечить комплексную защиту бизнеса. – URL: https://xn--80aidjgwzd.xn--p1ai/news/korporativnaya_bezopasnost/?captcha=done&apply=y

7. Корпоративное управление в рамках концепции ESG. – URL: https://journal.ecostandard.ru/esg/ustoychivoe-razvitie/korporativnoe-upravlenie-v-ramkakh-kontseptsii-esg/

8. *Магретта Дж.* Ключевые идеи. Майкл Портер. – М. : Манн, Иванов и Фербер, 2013.

9. *Панарина М. М.* Основы корпоративной безопасности предприятия : монография. – М. : Русайнс, 2019.

10. *Уминская А.* Правила корпоративной безопасности. – URL: https://journal.sovcombank.ru/glossarii/pravila-korporativnoi-bezopasnosti

11. *Четыркина Д. К.* Оценка значимости рисков в коммерческом банке // Финансовые рынки и банки. – 2018. – № 4. – С. 52–55.

References

1. Vasin S. G. Problemy upravleniya korporativnoy bezopasnostyu v tselyakh obespecheniya ustoychivogo razvitiya organizatsii [Managing Corporate Security to Ensure Sustainable Development of Organization]. *Sbornik dokladov Vserossiyskoy nauchno-prakticheskoy konferentsii «Problemy razvitiya dobrosovestnoy konkurentsii v epokhu tsifrovoy ekonomiki»* [Collection of Reports of the All-Russian Conference 'Problems of Developing Just Competition in Era of Digital Economy']. Moscow, Plekhanov Russian University of Economics, 2024, pp. 8–15. (In Russ.).

2. Grigorev N. Postroenie korporativnoy bezopasnosti: kak opredelit ugrozy i obespechit kompleksnuyu zashchitu biznesa [Building Corporate Security: How to Identify Threats and Provide Complex Protection of Business]. (In Russ.). Available at: https://www.cleverence.ru/articles/biznes/postroenie-korporativnoy-bezopasnosti-kak-opredelit-ugrozy-i-obespechit-kompleksnuyu-zashchitu-bizne/

3. Zharinov I. O. Korporativnoe upravlenie v tsifrovoy ekonomike [Corporate Management in Digital Economics]. *Vestnik Rossiyskogo ekonomicheskolgo universiteta imeni G. V. Plekhanova* [Vestnik of the Plekhanov Russian University of Economics], 2021, Vol. 18, No. 6 (120), pp. 158–169. (In Russ.).

4. Zhukova E. V. Strategicheskie prioritety ustoychivogo razvitiya i formirovanie algoritma upravleniya ESG-riskami [Strategic Priorities of Sustainable Development and Elaboration of Algorithm of ESG-Risks]. *Kreativnaya ekonomika* [Creative Economics], 2022, Vol. 16, No. 2, pp. 611–628. (In Russ.).

5. Korporativnaya bezopasnost predpriyatiya [Corporate Security of the Enterprise]. (In Russ.). Available at: https://falcongaze.com/ru/pressroom/publications/articles/korporativnaja-bezopasnost-predprijatija.html

6. Korporativnaya bezopasnost predpriyatiya: kak opredelit ugrozy i obespechit kompleksnuyu zashchitu biznesa [Corporate Security of the Enterprise: How to Identify Treats and Provide Complex Protection of Business]. (In Russ.). Available at: https://xn--80aidjgwzd.xn--p1ai/news/korporativnaya_bezopasnost/?captcha=done&apply=y

7. Korporativnoe upravlenie v ramkakh kontseptsii ESG [Corporate Management within the Frames of ESG Concept]. (In Russ.). Available at: https://journal.ecostandard.ru/esg/ustoychivoe-razvitie/korporativnoe-upravlenie-v-ramkakh-kontseptsii-esg/

8. Magretta Dzh. Klyuchevye idei. Maykl Porter [Key Ideas. Michael Porter]. Moscow, Mann, Ivanov i Ferber, 2013. (In Russ.).

9. Panarina M. M. Osnovy korporativnoy bezopasnosti predpriyatiya: monografiya [Principles of Corporate Security of the Enterprise: monograph]. Moscow, Rusayns, 2019. (In Russ.).

10. Uminskaya A. Pravila korporativnoy bezopasnosti [Rules of Corporate Security]. (In Russ.). Available at: https://journal.sovcombank.ru/glossarii/pravila-korporativnoi-bezopasnosti

11. Chetyrkina D. K. Otsenka znachimosti riskov v kommercheskom banke [Assessing the Importance of Risks in Commercial Bank]. *Finansovye rynki i banki* [Finance Markets and banks], 2018, No. 4, pp. 52–55. (In Russ.).

Сведения об авторах

Оксана Юрьевна Кириллова
доктор экономических наук, профессор,
профессор базовой кафедры Федеральной
антимонопольной службы России
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 109992, Москва, Стремянный пер., д. 36.
E-mail: Kirillova.OY@rea.ru

Сергей Григорьевич Васин
кандидат экономических наук, доцент,
доцент базовой кафедры Федеральной
антимонопольной службы России
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 109992, Москва, Стремянный пер., д. 36.
E-mail: Vasin.SG@rea.ru

Information about the authors

Oksana U. Kirillova
Doctor of Economics, Professor,
Professor of the Specialized Department
of Federal Antitrust Authority of Russia
of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 109992, Russian Federation.
E-mail: Kirillova.OY@rea.ru

Sergey G. Vasin
PhD, Assistant Professor, Assistant Professor
of the Specialized Department
of Federal Antitrust Authority of Russia
of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 109992, Russian Federation.
E-mail: Vasin.SG@rea.ru