Комплексный подход в обеспечении корпоративной безопасности

Integrated Approach in Ensuring Corporate Security

DOI: 10.12737/2306-627X-2024-13-4-27-33 Получено: 02 июля 2024 г. / Одобрено: 13 июля 2024 г. / Опубликовано: 25 декабря 2024 г.

Ломейко А.А.
Аспирант экономического факультета, кафедра менеджмента, ФГАОУ ВО «Российский университет дружбы народов имени Патриса Лумумбы», г. Москва,
e-mail: 1142220832@rudn.ru

Lomeiko A.A.
Postgraduate Student, Faculty of Economics, Department of Management, Peoples' Friendship University of Russia named after Patrice Lumumba (RUDN University), Moscow,
e-mail: 1142220832@rudn.ru

Аннотация
Статья посвящена актуальной проблеме обеспечения корпоративной безопасности в современных условиях. Автор исследует различные подходы в обеспечении корпоративной безопасности на предприятии, акцентируя внимание на социальном, техническом и стейкхолдерском, системном и синергетическом подходах. Анализ существующих практик и теоретических концепций помог выявить основные проблемы и тенденции корпоративной безопасности. В статье представлена авторская модель корпоративной безопасности, основанная на синергетическом и системном подходах. Модель предполагает комплексный анализ внутренних и внешних факторов, влияющих на корпоративную безопасность организации, а также учет интересов всех заинтересованных сторон. **Целью** статьи является разработка комплексного подхода в обеспечении корпоративной безопасности. В статье применяется **метод** обзора литературы для анализа существующих исследований по корпоративной безопасности. Также используют сравнительный анализ для оценки различных подходов к корпоративной безопасности, таких как статистические, экономико-математические и риск-ориентированные методы. **Основные выводы** исследования заключаются в том, что определена важность комплексного подхода, учитывающая интересы заинтересованных сторон в обеспечении корпоративной безопасности. Предложены системный и синергетический подходы, сочетающие системное мышление и взаимодействие для создания надежной системы корпоративной безопасности.

Ключевые слова: корпоративная безопасность, стейкхолдерский подход, системный подход, синергетический подход, управление рисками, безопасность предприятия.

Abstract
The article is devoted to the urgent problem of ensuring corporate security in modern conditions. The author investigates various approaches in ensuring corporate security at the enterprise, focusing on social, technical and stakeholder, systemic and synergetic approaches. The analysis of existing practices and theoretical concepts helped to identify the main problems and trends of corporate security. The article presents the author's model of corporate security based on synergetic and systemic approaches. The model involves a comprehensive analysis of internal and external factors affecting the corporate security of the organization, as well as consideration of the interests of all stakeholders.
The purpose of the article is to develop an integrated approach in ensuring corporate security.
Methods. The article uses the literature review method to analyze existing research on corporate security. Also use comparative analysis to evaluate different approaches to corporate security such as statistical, economic-mathematical and risk-based methods.
Results. The main conclusions of the study are that the importance of an integrated approach that takes into account the interests of stakeholders in ensuring corporate security has been determined. A systemic and synergetic approach combining systemic thinking and interaction is proposed to create a reliable system of corporate security.

Keywords: corporate security, stakeholder approach, systemic approach, synergetic approach, risk management, enterprise security.

1. ВВЕДЕНИЕ

Опыт многих компаний показал, что необходимо создать эффективную организацию по обеспечению корпоративной безопасности, отвечающую бизнес-потребностям российских предприятий. Компании, работающие в рамках группы, имеют дочерние компании или филиалы, которые полностью интегрированы, чтобы без проблем внедрять политику корпоративной безопасности. Однако многие компании работают под финансовым контролем, что требует участия группы в вопросах корпоративной безопасности.

Проблема заключается в стратегическом размещении служб безопасности в данном сложном вопросе. Нормативные требования вынуждают некоторые компании привлекать внешних подрядчиков для оказания определенных услуг в области безопасности. Однако, несмотря на все прилагаемы усилия, система корпоративной безопасности остается несовершенной.

В современном бизнес-пространстве, где цифровая трансформация является непрерывным процессом, а нормативно-правовая база активно развивается, руководители служб информационной безопасности часто стремятся оптимизировать стратегии обеспечения корпоративной безопасности в соответствии с постоянно меняющимися требованиями. Некоторые компании вложили много средств в создание виртуальных структур корпоративной безопасности, однако данные инициативы не принесли желаемых результатов.

2. МЕТОДЫ ИССЛЕДОВАНИЯ

Данное исследование основано на сборе, обобщении (синтез), систематизации (системный подход) и сравнительном анализе (комплексный и сравнительно-аналитический методы) информации, полученной из официальных источников и других доступных источников.

3. РЕЗУЛЬТАТЫ

В контексте российской деловой практики концепция корпоративной безопасности является относительно новой, а ее исторические истоки восходят к английскому термину «корпоративное управление».

Э.М. Коротков подчеркивает важность обеспечения высокой эффективности корпоративного управления путем укрепления корпоративной культуры, охватывающей принципы, обычаи, отношение и поведение всех заинтересованных сторон [3]. В.Н. Гринева и А.Е. Попов подробно развивают корпоративное управление, подчеркивая его важность для создания позитивной рабочей среды и содействия успеху организации [1]. Таким образом, корпоративные отношения применимы ко всем процессам, происходящим на предприятии.

По мнению А. Ломейко, «корпоративная безопасность — это комплексная система мер, направленных на защиту активов, данных, сотрудников и репутации организации от потенциальных угроз» [9].

S. Reka утверждает, что в то время как общественное, национальное и социальное обеспечение получили существенное академическое внимание, корпоративная безопасность была относительно проигнорирована, несмотря на ее растущую важность [10]. Учитывая динамичную и сложную бизнес-среду, компании все чаще сталкиваются с новыми угрозами безопасности. Автор стремится понять, как корпоративная политика безопасности интегрируется в общую бизнес-стратегию [11]. Изучая взаимосвязь между корпоративной безопасностью и стратегическим планированием, исследование стремится выявить новые проблемы и возможности в этой области.

Обеспечение корпоративной безопасности является комплексной задачей, требующей применения различные подходы, каждый из которых имеет особенности и сферы применения. Рассмотрим три основных подхода: статистический, экономико-математический и рисковый.

Статистический подход основан на сборе, анализе и интерпретации количественных данных о прошлых инцидентах безопасности. Статистика помогает выявить закономерности, тенденции и уязвимые места в системе корпоративной безопасности предприятия.

Экономико-математический подход заключается в применении математических моделей для оценки экономических последствий различных угроз и выбора оптимальных мер безопасности.

Рисковый подход фокусируется на идентификации, оценке и управлении рисками, связанными с безопасностью предприятия.

Сравнительная характеристика походов указана в табл. 1.

Таблица 1

Сравнительная характеристика походов корпоративной безопасности

Характеристика	Статистический подход	Экономико-математический подход	Рисковый подход
Направление	Анализ статистических данных	Оценка экономических последствий	Идентификация и управление рисками
Методы	Статистический анализ	Математическое моделирование	Оценка рисков, анализ уязвимостей
Преимущества	Оценка вероятности возникновения различных угроз. Помогает выявить эффективные меры безопасности. Обеспечивает объективную оценку эффективности существующих систем безопасности	Оценивает экономическую эффективность различных мер безопасности. Помогает оптимизировать затраты на безопасность. Учитывает взаимосвязь между различными факторами, влияющими на корпоративную безопасность	Комплексный подход, гибкость. Выявляет и оценивает все возможные угрозы. Способствует разработке эффективных мер реагирования на инциденты. Учитывает как внутренние, так и внешние факторы риска
Недостатки	Ограничен рамками имеющихся данных. Не учитывает качественные факторы и новые угрозы. Требует больших объемов данных и статистических знаний	Необходимо построение сложных математических моделей. Зависит от точности исходных данных. Сложный для понимания неспециалистами	Требует глубокого понимания бизнеса и его процессов. Является субъективным из-за необходимости оценки вероятности и последствий различных угроз

Каждый из рассмотренных подходов имеет сильные и слабые стороны. Для обеспечения эффективной корпоративной безопасности рекомендуется комбинировать их. Статистический подход выявляет основные тенденции и распространенные угрозы. Экономико-математический подход помогает оптимизировать затраты на безопасность. Рисковый подход обеспечивает комплексный взгляд на проблему и позволяет разработать гибкую систему управления рисками.

Однако, по мнению Л.Н. Левановой, стейкхолдерский подход (заинтересованных сторон) является полезной методологической основой для понимания корпоративной безопасности. Он учитывает интересы заинтересованных сторон и то, как они влияют на корпоративную безопасность предприятий. Выявляя риски и конфликты между заинтересованными сторонами, компании могут предпринимать шаги по снижению рисков и улучшению системы корпоративной безопасности [4].

Подход с привлечением заинтересованных сторон — признание того, что безопасность компании заключается не только в защите физических активов и финансовой информации. Речь также идет о защите интересов всех людей, имеющих отношение к компании, таких как сотрудники, клиенты, инвесторы и поставщики. Учитывая интересы стейкхолдеров, руководители предприятий выявляют риски, которые угрожают их безопасности [6]. Например, компания, которая не учитывает интересы сотрудников, создает угрозу безопасности, которая приводит к травмам или даже смерти. Или компания, которая не учитывает интересы клиентов, способствует развитию угрозы безопасности, которая порождает утечку данных или кражу личных данных. Применяя стейкхолдерский подход к обеспечению корпоративной безопасности с учетом интересов заинтересованных сторон, компании улучшат общую систему безопасности и смогут защитить интересы всех тех, кто заинтересован в их успехе [7].

Таким образом, выбор оптимального подхода зависит от конкретных условий предприятия, включая его размер, отрасль, уровень развития информационных технологий и другие факторы. Необходимо отметить, что обеспечение корпоративной безопасности является непрерывным процессом, который требует постоянного мониторинга и адаптации к изменяющимся угрозам.

Чтобы заложить методологическую основу для разработки системы корпоративной безопасности на предприятии, крайне важно изучить точки зрения ученых относительно значимости человеческого фактора в безопасности предприятия. В данном контексте стоит сравнить социальный и технический подходы корпоративной безопасности.

Социальный подход предполагает, что основой системы корпоративной безопасности является человеческий фактор, а способность поддерживать надлежащий уровень безопасности зависит от способности человека обнаруживать изменения в уровнях безопасности, реагировать на признаки потенциальных рисков и угроз и принимать соответствующие защитные меры [5]. Ожидается, что отдельные лица, являющиеся неотъемлемым компонентом системы, будут вносить вклад в ее поддержание. Цель может быть достигнута путем согласования интересов отдельных лиц с интересами системы в целом.

Технический подход к вовлечению человека в различные процессы отводит отдельным лицам второстепенную роль, рассматривая их как простые компоненты сложного механизма, предназначенного для поддержания определенного уровня корпоративной безопасности [2]. Технический подход основан на понимании роли человека в социальных контекстах, где он утверждает, что люди, хоть и не могут избежать влияния на социальные процессы, активно стремятся изменить социальные условия.

На наш взгляд, в условиях, характеризующихся высоким уровнем неопределенности и растущим значением человеческих ресурсов в бизнес-операциях предприятий, актуальным является социальный подход.

Не исключая потенциальных угроз, возникающих в результате действий или бездействия сотрудников, или влияния «человеческого фактора», лояльный сотрудник, который стремится к продолжению работы и росту компании, должен составлять основу корпоративной безопасности. Речь идет не только о работниках службы безопасности, но и о трудовом коллективе в целом и акционерах, других заинтересованных лицах.

Важность создания методологической основы для создания системы корпоративной безопасности на предприятиях подчеркивает необходимость применения синергетического подхода, который включает не только системное мышление, но и синергию. Отметим, что синергетический подход в сочетании с системным дает возможность определить эффективные способы функционирования любой социально-экономической системы. Также выделяют два дополнительных аспекта синергии, таких как характер взаимодействия между системой и ее внешней средой и важность усиления связей между элементами.

Любая организация существует для решения конкретных задач внутри предприятия, и поэтому руководители должны уделять приоритетное внимание корпоративной безопасности по трем направлениям [8]:

- выполнение требований корпоративной безопасности, предъявляемых компанией;
- защита основных интересов бизнеса;
- содействие постоянному повышению устойчивости организации.

Необходимо понимать стратегическое видение компании и согласовывать меры корпоративной безопасности с различными бизнес-подразделениями и дочерними компаниями. Реализация любого корпоративного стратегического плана требует соответствующей организационной структуры для его поддержки, в противном случае план остается просто концепцией. Различия в отраслевой специфике, масштабах бизнеса, ассортименте продукции и корпоративной культуре требуют от организаций создания гибких организационных структур, способных адаптироваться к уникальным условиям функционирования. Даже в рамках одной и той же компании

стратегические корректировки требуют организационных изменений для обеспечения их эффективной реализации. Например, предприятие, стремящееся преуспеть в цифровой трансформации, столкнется с трудностями, если нет специализированной команды по работе с большими данными.

Аналогичным образом, если компания стремится выйти на зарубежные рынки, но нет команды, ответственной за международные операции, то будет трудно добиться успеха в данном направлении. То же самое относится и к мерам корпоративной безопасности. В организации существует необходимость в специальном подразделении, которое отвечало бы специфическим требованиям корпоративной безопасности. Ведь различные отрасли промышленности, предъявляют различные требования к корпоративной безопасности, которые приводят к определенным изменениям в организационной структуре.

Присутствие технических угроз в сфере цифровых технологий обусловливает необходимость привлечения высококвалифицированных специалистов по безопасности для защиты критически важных активов организации и предотвращения несанкционированного доступа к интеллектуальной собственности. Создание специализированных подразделений по обеспечению безопасности является необходимым условием для успешной деятельности предприятий в современных условиях. Промышленные компании нуждаются в таких подразделениях для контроля соблюдения нормативных требований, а интернет-компании — для защиты информационных систем от киберугроз. Наличие специализированных подразделений по информационной безопасности является обязательным требованием для компаний, работающих с конфиденциальными государственными данными. Такие подразделения призваны обеспечить выполнение законодательных норм по защите информации.

Несмотря на то что потребность в службах корпоративной безопасности может меняться в зависимости от конкретных условий деятельности предприятия, современные тренды, такие как цифровизация, Интернет вещей и искусственный интеллект, обусловливают постоянное повышение требований к информационной безопасности.

Корпоративная безопасность является фундаментальным компонентом эффективного управления рисками, обеспечивающим устойчивый рост организации. Она выступает ключевым фактором стабильного развития компании, требуя комплексного подхода на уровне всей организации.

Необходимо четко определить и внедрить основные принципы корпоративной безопасности, обеспечив их соблюдение всеми подразделениями. Система мотивации и поощрений будет способствовать повышению осведомленности сотрудников о стандартах безопасности.

Для успешной реализации системы корпоративной безопасности требуется комплексный подход, включающий разработку соответствующей корпоративной культуры и создание специализированной команды. Такой подход гарантирует, что все подразделения организации действуют в рамках единых правил и норм безопасности.

Интеграция требований корпоративной безопасности в бизнес-процессы часто сопряжена с определенными проблемами. Во-первых, бизнес-подразделения могут воспринимать меры безопасности как дополнительные затраты, не приносящие прямой коммерческой выгоды. Во-вторых, отсутствие четкого понимания бизнес-подразделениями рисков, связанных с корпоративной безопасностью, приводит к формальному отношению к требованиям безопасности. В-третьих, для преодоления проблем необходимо обеспечить тесное взаимодействие между службой безопасности и бизнес-подразделениями, а также разработать систему мотивации, стимулирующую соблюдение требований корпоративной безопасности.

Несмотря на наличие подразделений корпоративной безопасности в крупных организациях, отсутствие формализованных процессов оценки и управления рисками зачастую приводит к децентрализованной модели обеспечения безопасности, где каждое подразделение самостоятельно принимает решения. Отсутствие единых стандартов и централизованного контроля затрудняет достижение оптимального уровня защищенности. Такой подход затрудняет достижение согласованности и эффективности в реализации мер корпоративной безопасности на уровне всей организации.

Для эффективного противодействия угрозам необходимо создание гибкой системы управления корпоративной безопасностью, способной адаптироваться к динамично меняющейся внутренней и внешней среде.

Комплексный подход к корпоративной безопасности предполагает вовлечение всех подразделений организации. Команда по корпоративной безопасности должна координировать усилия по идентификации, оценке и снижению рисков, обеспечивая согласованность действий на уровне всей организации. Команда, отвечающая за корпоративную безопасность, должна разрабатывать и согласовывать стратегию управления рисками, определяя ключевые угрозы, устанавливая цели и планируя мероприятия

по повышению уровня безопасности организации. Цель такой стратегии — обеспечить единое понимание значимости корпоративной безопасности для всех подразделений и способствовать непрерывному совершенствованию системы защиты.

Ведь управление корпоративной безопасностью представляет собой динамический процесс, тесно связанный с развитием бизнеса. По мере роста организации и расширения ее деятельности увеличивается и спектр потенциальных угроз. Для обеспечения адекватного уровня защиты необходимо регулярно проводить оценку рисков и адаптировать меры корпоративной безопасности к изменяющимся условиям ведения бизнеса.

Однако часто возникает разрыв между восприятием безопасности как центра затрат и пониманием ее стратегической ценности для бизнеса. Для преодоления такого разрыва необходимо выстроить эффективные коммуникации между службой безопасности и другими подразделениями, а также обеспечить интеграцию мер безопасности в общие бизнес-процессы.

Проекты по обеспечению корпоративной безопасности требуют комплексного подхода, аналогичного управлению продуктом. Необходимо создать междисциплинарную команду, включающую специалистов по безопасности, маркетингу, эксплуатации, технологиям и другим смежным областям. Важнейшим аспектом является вовлечение всех заинтересованных сторон в процесс принятия решений и обеспечение согласованности действий.

4. ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

Для успешной реализации системы корпоративной безопасности необходимо:

- обеспечить комплексный подход к управлению и руководству компании активно участвовать в формировании стратегии безопасности и интегрировать ее в общие бизнес-цели;
- сформировать команду с четко определенными ролями и обязанностями для совершенствования корпоративной безопасности;
- выстроить открытые и прозрачные каналы коммуникации между службой безопасности и другими подразделениями;
- своевременно анализировать риски организации и адаптировать меры безопасности к изменяющимся угрозам;
- оказывать постоянную поддержку инициативам совершенствования корпоративной безопасности, выделяя ресурсы и полномочия.

Опираясь на обобщение результатов исследований международных и отечественных ученых, а также на их собственные идеи и вклад, разработана модель системы корпоративной безопасности в масштабах всего предприятия (рис. 1).

Уместно обосновать только некоторые аспекты разработанной модели. Действия участников, объединенных в рамках системного подхода к корпоративной безопасности, направлены на выполнение важнейших функций, а именно, сохранение целостности организации и обеспечение реализации интересов всех заинтересованных сторон. Предлагается внедрение системного и синергетического подходов, которые необходимы для организации, поддержания и эволюции корпоративной безопасности.

Процесс распада системы в первую очередь связан с неспособностью преследовать интересы, которые приводят к ослаблению корпоративной безопасности. Применение системного подхода к обеспечению корпоративной безопасности способствует сохранению целостности системы путем решения всех основополагающих проблем безопасности.

Рис. 1. Модель формирования системы корпоративной безопасности предприятия

Важно признать, что корпоративные конфликты представляют собой серьезную внутреннюю угрозу для предприятий и требуют разработки надежной системы корпоративной безопасности.

Внедрение синергии на основе надежной системы корпоративной безопасности имеет решающее значение, поскольку она предполагает выявление потенциальных проблем в корпоративной системе и прогнозирование их дальнейшего развития. Специалистам по корпоративной безопасности требуется проявлять инициативу в комплексном подходе, заблаговременно выявляя потенциальные изменения в стабильной работе предприятия. На рис. 1 модель закладывает основу для построения комплексной системы корпоративной безопасности, адаптированной к конкретным потребностям предприятия.

Предлагается перечень этапов, реализация которых будет способствовать интеграции корпоративной системы безопасности как в качестве подсистемы внутри предприятия, так и в качестве надсистемы, направленной на обеспечение безопасных условий ее существования и развития.

Начальный этап предполагает разработку комплексной модели предприятия, учитывающей точки зрения всех заинтересованных сторон, как общие, так и индивидуальные. Такой процесс поможет установить четкую цель, которая служит основой для укрепления корпоративной безопасности, а затем детализирована в ряд задач для служб безопасности. Кроме того, цель является ориентиром для оценки эффективности мер, принимаемых по корпоративной безопасности в будущем.

На втором этапе проводится тщательный анализ внешней среды с целью выявления возможностей для согласования общих интересов. Данный этап необходим для уточнения общих целей и приведения их в соответствие с устремлениями участников внешней сферы. Учитывая динамичный и непредсказуемый характер внешних воздействий, которые существенно влияют на стабильность систем, при формулировании задач для сотрудников службы корпоративной безопасности становится необходимым тщательно оценивать внешние взаимодействия элементов системы.

На третьем этапе необходимо сформулировать стратегические цели и согласовать их со стратегией роста компании. Стратегические директивы способствуют определению организационного и ресурсного обеспечения, необходимого для функционирования системы корпоративной безопасности.

На следующем этапе разрабатывается организационная архитектура корпоративной структуры безопасности, устанавливаются институциональные принципы, стандарты и нормативные акты, разъясняется ее положение в организационной структуре предприятия, отлаживаются вертикальные и горизонтальные связи с дальнейшим определением должностных обязанностей персонала на всех уровнях и закладывается фундамент для ресурсного обеспечения (финансового, информационного, материального, кадрового), основой которого является создание системы контроля и мониторинга эффективности работы системы корпоративной безопасности.

Можно утверждать, что выполнение указанных этапов поможет получить полное представление о системе корпоративной безопасности предприятия.

В заключение стоит еще раз подчеркнуть, что разработка надежной стратегии корпоративной безопасности зависит от уникальных характеристик корпоративной деятельности, в частности, от различий в индивидуальных задачах и неспособности достичь общих целей в условиях неблагоприятных внешних воздействий. Чтобы обеспечить надлежащий уровень корпоративной безопасности, который способствовал бы сохранению целостности предприятия как системы и заложил бы основу для перехода к желаемому позитивному синергетическому подходу, важно создать систему корпоративной безопасности, основанную на надежных методологических принципах.

Литература

1. *Гринева В.Н.* Организационно-экономические основы формирования системы корпоративного управления [Текст] / В.Н. Гринева, А.Е. Попов // Экономика. — 2023. — С. 32–34.
2. *Жмеренецкий В.Ф.* Теория безопасности социальных систем [Текст]: учеб. пособие / В.Ф. Жмеренецкий. — М.: Изд-во НОУ ВПО МПСИ, 2010. — 177 с.
3. *Коротков Э.М.* Антикризисное управление [Текст]: учебник / Э.М. Коротков. — 2-е изд., доп. и перераб. / под ред. Э.М. Короткова. — М.: ИНФРА-М, 2006. — 620 с.
4. *Леванова Л.Н.* Корпоративная безопасность: стейкхолдерский подход [Текст] / Л.Н. Леванова, А.В. Вавилина // Вестник МИРБИС. — 2022. — № 3. — С. 128–142. — DOI: 10.25634/MIRBIS.2022.3.14

References

1. Grineva V.N., Popov A.E. Organizational and economic foundations of the formation of the corporate governance system // Economics. 2023, pp. 32–34.
2. Zhmerenetsky V.F. Security theory of social systems: textbook. Moscow: NOU VPO MPSI, 2010. 177 p.
3. Korotkov E.M. Crisis management: textbook. 2nd ed. supplemented and revised / edited by prof. E.M. Korotkov. Moscow: INFRA-M, 2006. 620 p.
4. Levanova L.N. Corporate security: stakeholder approach / L.N. Levanova, A.V. Vavilina // MIRBIS Bulletin. 2022, no. 3, pp. 128–142. – DOI: 10.25634/MIRBIS.2022.3.14
5. Negreeva V.V. Target indicators of the effectiveness of corporate and social responsibility to ensure the economic security of the organization / V.V. Negreeva, M.B. Sultygova, Yu.D. Vasilyeva // Strategies and tools for economic man-

5. *Негреева В.В*. Целевые индикаторы эффективности корпоративной и социальной ответственности для обеспечения экономической безопасности организации [Текст] / В.В. Негреева, М.Б. Султыгова, Ю.Д. Васильева // Стратегии и инструменты управления экономикой: отраслевой и региональный аспект: Материалы VIII Международной научно-практической конференции, Санкт-Петербург, 23 мая 2019 г. — СПб.: Изд-во НПО ПБ АС, 2019. — С. 446–451.
6. *Ткаченко И.Н*. Актуализация стейкхолдерского подхода корпоративного управления в условиях коронакризиса: от декларирования приверженности к прикладным моделям [Текст] / И.Н. Ткаченко // Управленец = The Manager. — 2021. — № 12(2). — С. 2–16. — DOI: 10.29141/2218-5003-2021-12-2-1
7. *Ткаченко И.Н*. Оценка стейкхолдерской стоимости: эволюция методологического подхода и прикладные модели [Текст] / И.Н. Ткаченко // Актуальные проблемы развития корпоративного управления и бизнеса: материалы Международной научно-практической конференции, Екатеринбург, 15 ноября 2018 г. — Екатеринбург: Изд-во Уральского гос. эконом. ун-та, 2019. — С. 85–91.
8. *Djekic M*. The Corporate Security at a Global Scale. Global Journal of Social Sciences Studies. 2022, no. 8, pp. 56-61. DOI: 10.55284/gjss.v8i2.730
9. *Lomeyko A*. Factors Affecting the Corporate Security of Companies. Scientific Research and Development. Economics of the Firm. 2024, pp. 22–28. DOI: 10.12737/2306-627X2024-13-2-22-28
10. *Reka S*. Examining the Strategic Embeddedness of Corporate Security. The Eurasia Proceedings of Educational and Social Sciences. 2024, pp. 151–157. DOI: 10.55549/epess.1412834
11. *Reka S*. Conceptualization of Corporate Security Responsibility (CSecR) as Perceived by Security Experts. 2023, pp. 000211-000216. DOI: 10.1109/SISY60376.2023.10417959

agement: industry and regional aspect: Proceedings of the VIII International scientific and practical conference, St. Petersburg, May 23, 2019. St. Petersburg: Izd-vo NPO PB AS, 2019, pp. 446–451.
6. Tkachenko I.N. Updating the stakeholder approach to corporate governance in the context of the coronavirus crisis: from declaring commitment to applied models // The Manager. 2021, no. 12(2), pp. 2–16. DOI: 10.29141/2218-5003-2021-12-2-1
7. Tkachenko I.N. Stakeholder Value Assessment: Evolution of the Methodological Approach and Applied Models // Actual Problems of Corporate Governance and Business Development: Proceedings of the International Scientific and Practical Conference, Yekaterinburg, November 15, 2018. Yekaterinburg: Ural State University of Economics, 2019, pp. 85–91.
8. Djekic M. The Corporate Security at a Global Scale. Global Journal of Social Sciences Studies. 2022, no. 8, pp. 56–61. DOI: 10.55284/gjss.v8i2.730
9. Lomeyko A. Factors Affecting the Corporate Security of Companies. Scientific Research and Development. Economics of the Firm. 2024, pp. 22–28. DOI: 10.12737/2306-627X2024-13-2-22-28
10. Reka S. Examining the Strategic Embeddedness of Corporate Security. The Eurasia Proceedings of Educational and Social Sciences. 2024, pp. 151–157. DOI: 10.55549/epess.1412834
11. Reka S. Conceptualization of Corporate Security Responsibility (CSecR) as Perceived by Security Experts. 2023, pp. 000211–000216. DOI: 10.1109/SISY60376.2023.10417959