Факторы, влияющие на обеспечение корпоративной безопасности компаний

Factors Affecting the Corporate Security of Companies

DOI: 10.12737/2306-627X-2024-13-2-22-28 Получено: 17 декабря 2023 г. / Одобрено: 24 декабря 2023 г. / Опубликовано: 25 июня 2024 г.

Ломейко А.А.
Аспирант Экономического факультета, кафедра менеджмента, ФГАОУ ВО «Российский университет дружбы народов», 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, Moscow, e-mail: 1142220832@rudn.ru

Аннотация
Корпоративная безопасность является комплексной системой мер, предназначенных для защиты активов, данных, сотрудников и репутации организации от потенциальных угроз. В данной статье рассматриваются различные факторы, которые могут повысить уязвимость организации к угрозам безопасности. Исследуются независимые и комбинированные эффекты внутреннего контроля, такие как учебные программы и протоколы защиты данных, а также внешние угрозы, такие как кибератаки, физические вторжения и экономический шпионаж.
Ключевым аспектом анализа является идея синергии в области безопасности. В статье утверждается, что хорошо скоординированный подход, сочетающий различные меры безопасности в единое целое, создает более эффективную стратегию защиты. Анализ взаимозависимостей между различными элементами управления подчеркивает важность внедрения стратегической программы управления угрозами, которая выходит за рамки индивидуальных решений. Способствуя всестороннему пониманию уязвимостей и эффективности синергетических мер безопасности, статья направлена на то, чтобы снабдить организации знаниями и инструментами для разработки и внедрения эффективных программ управления угрозами, которые защищают их критически важные активы и способствуют долгосрочному успеху.

Ключевые слова: корпоративная безопасность, угрозы, уязвимость, меры безопасности, синергия, управление рисками.

Abstract
Corporate security is a comprehensive system of measures designed to protect an organization's assets, data, employees, and reputation from potential threats. This article discusses various factors that can increase an organization's vulnerability to security threats. The independent and combined effects of internal controls, such as training programs and data protection protocols, as well as external threats such as cyber-attacks, physical intrusions and economic espionage, are being investigated.
A key aspect of the analysis is the idea of synergy in the field of security. The article argues that a well-coordinated approach combining various security measures into a single whole creates a more effective protection strategy. The analysis of the interdependencies between the various controls highlights the importance of implementing a strategic threat management program that goes beyond individual solutions. By contributing to a comprehensive understanding of vulnerabilities and the effectiveness of synergistic security measures, the article aims to equip organizations with the knowledge and tools to develop and implement effective threat management programs that protect their critical assets and contribute to long-term success.

Keywords: corporate security, threats, vulnerability, security measures, synergy, risk management.

1. ВВЕДЕНИЕ

В большинстве российских компаний миноритарные акционеры, будучи ограниченными в получении информации о текущей деятельности и участии в формировании стратегических задач, фактически не влияют на деятельность компании [1]. Важность обеспечения корпоративной безопасности становится приоритетной не только для акционерных обществ, но и для других форм предпринимательской деятельности.

На предприятиях существуют внутренние конфликты между участниками и менеджерами, между отдельными участниками и группами работников, предприятием и местными органами власти и обществом и т.д., которые традиционно не учитываются в процессе обеспечения экономической безопасности [6]. Обеспечение устойчивого развития предприятий в условиях высоких непредсказуемых изменений нестабильной внешней среды возможно только при условии уделения должного внимания проблеме безопасности, в частности корпоративной.

История становления корпоративного сектора в России относительно коротка, а проблемы являются последствиями как трансформационных процессов в национальной экономике, так и изменений в мировом экономическом пространстве. Разработка необходимой методологической базы обеспечения корпоративной безопасности призвана создать необходимые безопасные условия для устойчивого развития каждого предприятия, обеспечивая тем самым стабилизацию экономических, политических и социальных процессов в стране.

Проблема обеспечения безопасности предприятий приобрела особую остроту в последние два десятилетия, что в наибольшей степени обусловлено трансформационными изменениями в национальной экономике и формированием сектора негосударственных предприятий. Собственник, а не только государственные учреждения, должен заботиться о формировании безопасных условий для функционирования и развития определенного субъекта хозяйствования, что требует как изменения восприятия самого понятия «безопасность», так и разработки соответствующей научной базы, основанной на реальных условиях ведения бизнеса. бизнес в нашей стране.

А.А. Ширенина представляет корпоративную безопасность как «состояние корпоративной системы

в пределах ее возможностей и способность противодействовать угрозам и обеспечивать реализацию собственных интересов» [9], тем самым подчеркивая важность формирования корпоративной системы безопасности для эффективного противодействия угрозам.

Концепция корпоративной безопасности — это научно обоснованная система взглядов на определение основных направлений, условий и порядка практического решения задач по защите хозяйствующих субъектов от противоправных действий и недопустимой конкуренции [8].

Концепция корпоративной безопасности была разработана с учетом необходимости скорейшей адаптации предприятий, осуществляющих внешнеэкономическую деятельность, к европейским стандартам безопасности ISO и предусматривает [10]:

- мониторинг, прогнозирование, своевременное выявление и устранение угроз безопасности предприятий, причин и условий, способствующих нанесению финансового и материального ущерба, нарушению их функционирования и развития;
- обоснование и формирование комплексной организации обеспечения безопасности хозяйствующих субъектов;
- создание механизма и условий для оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании;
- эффективное устранение угроз персоналу и посягательств на ресурсы предприятия при применении правовых, организационных и технических средств для достижения требуемого уровня безопасности;
- формирование эффективных механизмов взаимодействия государственных структур и хозяйствующих субъектов в вопросах безопасности;
- изучение и внедрение положительного опыта в области корпоративной безопасности, накопленного в странах ближнего и дальнего зарубежья;
- создание единой информационной базы данных о состоянии угроз и опасностей для участников системы корпоративной безопасности;
- изучение новых, перспективных направлений деятельности и совершенствование работы по созданию благоприятных условий для безопасной предпринимательской деятельности;
- участие в разработке законов, способствующих развитию предпринимательской деятельности и обеспечивающих устойчивое функционирование предприятий;
- проведение независимых экспертиз и аудитов, связанных с изучением вопросов безопасности предприятий [10].

Таким образом, сегодня видны признаки научного прогресса, который заключается в переходе от вышеупомянутой трактовки безопасных условий для развития предприятий путем обеспечения экономической безопасности к их формированию посредством корпоративной безопасности.

2. МЕТОДЫ ИССЛЕДОВАНИЯ

В качестве основы для исследования использованы данные, предоставленные предприятием АО «Мосэнергосбыт». 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, в том числе нормативных правовых актов, материалов толкования нормативных правовых актов (формально-юридический метод), анализа практики. Информационной базой являются статистическая информация, представленная на официальном сайте Росстата, на портале правовой статистики Генеральной прокуратуры РФ, статистические данные МВД РФ, материалы периодической печати, а также из сети Интернет.

3. РЕЗУЛЬТАТЫ

Постоянная потребность в корпоративной безопасности обусловлена сложным и постоянно меняющимся ландшафтом, в котором работает бизнес. Понимание этих факторов и внедрение эффективных мер противодействия имеет решающее значение для любой организации, стремящейся к процветанию. На рис. 1 приведен перечень некоторых ключевых факторов, которые могут повлиять на корпоративную безопасность компаний.

Рис. 1. Факторы, влияющие на корпоративную безопасность [6]

Рассмотрим подробнее каждый фактор, который указана на рис. 1.

1. ***Кибербезопасность.*** Век цифровых технологий ознаменовался непрекращающейся волной киберугроз. Злоумышленники атакуют данные компаний с помощью изощренных методов взлома, фишинга и внедрения вредоносных программ. Надежные меры кибербезопасности, включая брандмауэры, шифрование данных и обучение сотрудников кибергигиене, необходимы для усиления защиты от этих цифровых атак.

2. ***Физическая безопасность.*** Физические активы, персонал и объекты требуют защиты от кражи, вандализма и других физических повреждений. Такие меры безопасности, как системы контроля доступа с многофакторной аутентификацией, охранники и видеонаблюдение с мониторингом в режиме реального времени, играют жизненно важную роль в предотвращении нарушений физической безопасности и реагировании на них.

3. ***Непрерывность бизнеса.*** Сбои, вызванные стихийными бедствиями, перебоями в подаче электроэнергии, кибератаками или даже глобальной пандемией, могут серьезно подорвать бизнес-процессы. Внедрение комплексного плана обеспечения непрерывности бизнеса позволяет организации быстро восстановиться и свести к минимуму время простоя. Комплексный план должен включать резервное копирование данных, протоколы аварийного восстановления и четкие стратегии коммуникации, позволяющие информировать сотрудников и заинтересованные стороны во время сбоев.

4. ***Безопасность сотрудников.*** Сотрудники являются как активами, так и уязвимыми местами. Инсайдерские угрозы, непреднамеренная утечка данных из-за человеческой ошибки и недовольные сотрудники представляют собой значительные риски. Обучение сотрудников навыкам выявления попыток фишинга, использованию паролей и важности защиты данных имеет решающее значение для снижения этих рисков. Проверка личных данных на ответственных должностях также может повысить уровень безопасности.

5. ***Соблюдение законодательства.*** Нормативно-правовая база представляет собой сложную сеть положений о конфиденциальности данных, стандартов информационной безопасности и отраслевых требований к соблюдению требований. Несоблюдение требований приводит к крупным штрафам, ущербу репутации и даже судебным последствиям. Организации должны быть в курсе меняющихся нормативных актов и внедрять процессы, обеспечивающие их соблюдение.

Помимо простого устранения отдельных угроз, в корпоративной безопасности первостепенное значение имеет целостный подход, основанный на законе синергии. Синергия — это принцип, согласно которому совокупный эффект двух или более элементов может превышать сумму их индивидуальных эффектов. В контексте безопасности это означает хорошо интегрированную стратегию, которая сочетает в себе различные меры безопасности для создания надежной защиты.

Синергия укрепляет корпоративную безопасность компаний, а именно:

- интегрированные системы безопасности. Разнообразный подход к обеспечению безопасности оставляет пробелы, которыми могут воспользоваться злоумышленники. Сочетание систем физического контроля доступа с системами видеонаблюдения и обнаружения вторжений создает многоуровневую защиту, которая более надежна, чем изолированные меры. Например, видеозапись можно использовать для проверки активности карты доступа и выявления подозрительного поведения;
- взаимодействие человека и технологии. Передовое программное обеспечение для обеспечения кибербезопасности — мощный инструмент, но его эффективность зависит от осведомленности пользователей и ответственного поведения. Программное обеспечение для обеспечения кибербезопасности наиболее эффективно в сочетании с информированностью и обучением сотрудников. Такая синергия позволяет сотрудникам выявлять попытки фишинга и другие подозрительные действия и сообщать о них, создавая защитную систему от атак социальной инженерии;
- управление рисками. Комплексная стратегия управления рисками предполагает упреждающий подход к обеспечению безопасности. Она выявляет потенциальные угрозы в масштабах всей организации, анализирует их вероятность и потенциальное воздействие и определяет приоритетность ресурсов для принятия эффективных контрмер.

Такой комплексный подход оптимизирует распределение ресурсов и укрепляет общую систему безопасности. Эффективное управление рисками выходит за рамки простого выявления угроз; оно включает в себя постоянный мониторинг, оценку уязвимостей и регулярное тестирование протоколов безопасности для обеспечения их эффективности [5].

Принимая во внимание опыт зарубежных и отечественных ученых в области количественной оценки безопасности и учитывая качественные особенности нестабильности внешней среды компаний, предлагаем оценивать уровень корпоративной без-

опасности на основе следующих основных критериев:

1) сложность, критерий характеризует среду, основанную на принципе «простое-сложное». Простая среда имеет ограниченное количество факторов, влияющих на нее, в то время как сложная среда включает в себя значительное количество таких факторов;
2) взаимозависимость факторов. Этот фактор определяет тип, направление и силу взаимосвязей между факторами окружающей среды;
3) изменчивость используется для определения характера и спонтанности изменений факторов окружающей среды;
4) неопределенность позволяет отразить степень неопределенности в информации, касающейся поведения переменных безопасности [4].

Основные критерии, которые помогают понять сложность, взаимозависимость, изменчивость и неопределенность внешней среды, что, в свою очередь, помогает принимать обоснованные решения для обеспечения устойчивости и безопасности сотрудников и функционирования организации. Оценка уровня корпоративной безопасности для компаний проводится с помощью комплексного подхода, в котором используется трехуровневая система.

Разработанная трехуровневая система основана на принципе «от частного к общему». На первом уровне оцениваются показатели нестабильности отдельных факторов в рамках каждого компонента внешней среды на основе предложенных четырех критериев. На втором уровне оценивается общий уровень нестабильности для каждого компонента. Наконец, на третьем уровне, определяется общий интегральный уровень нестабильности внешней среды.

Данная система поможет детально изучить и оценить нестабильность отдельных факторов корпоративной безопасности, их взаимосвязь и их влияние на общий уровень нестабильности внутри каждого компонента.

На заключительном этапе комплексная оценка общего уровня корпоративной безопасности позволяет получить целостное представление и понимание того, насколько уязвима ситуация в целом. Такая оценка помогает предприятиям лучше управлять рисками и обеспечивать устойчивость своей деятельности в изменяющихся условиях окружающей среды (рис. 2).

Существует множество причин корпоративной безопасности, и в данном случае попытаемся оценить общий уровень внешней нестабильности, возникающий в результате сочетания независимых изменений, которые могут быть оценены коллективно. Принимая во внимание предложенные критерии, выделим показатели оценки, позволяющие определить уровень факторов, связанных с каждым компонентом корпоративной безопасности компаний [3].

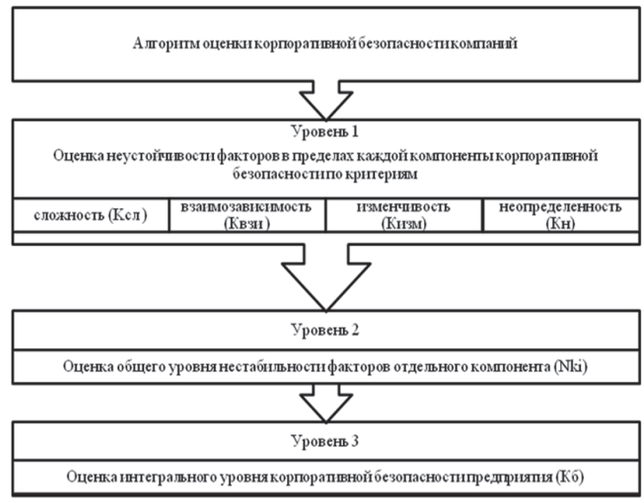

Рис. 2. Система оценки корпоративной безопасности в условиях нестабильности внешней среды компаний [7]

Сложность факторов в каждом отдельном компоненте корпоративной безопасности хозяйствующих субъектов может быть оценена с использованием соотношения факторов в каждом компоненте, к общему количеству факторов:

$$K_{\text{сл}} = \frac{n_{fci}}{n}, \quad (1)$$

где $K_{\text{сл}}$ — коэффициент сложности для i-го компонента внешней среды

n_{fci} — количество факторов в i-м компоненте, которые эксперты определили как наиболее значимые с точки зрения анализа этого компонента

n — общее количество факторов, учитываемых при анализе общей безопасности предпринимательской деятельности.

Считаем, что более высокое значение $K_{\text{сл}}$ указывает на более высокий уровень сложности отдельного компонента с диапазоном значений от 0 до 1. Взаимозависимость между факторами 1-го компонента внешней среды $K_{\text{сл}}$ определяется с помощью коэффициента корреляции Пирсона, который является широко используемым методом для определения определение степени связи между двумя переменными.

АО «Мосэнергосбыт» является одной из крупнейших энергосбытовых компаний в России. Оценка корпоративной безопасности АО «Мосэнергосбыт» проведена по методике, представленной на рис. 1.

Таблица 1

Оценка факторов корпоративной безопасности АО «Мосэнергосбыт»

Фактор	Описание	Уровень
Факторы, обусловливающие сложность	Компания работает с большим количеством клиентов, что увеличивает риск возникновения различных инцидентов	0,6
	Компания имеет филиалы и отделения в разных регионах, что усложняет контроль над безопасностью	
	Компания использует различные информационные системы и технические средства, что требует повышенного внимания к вопросам информационной безопасности	
Факторы, обусловливающие изменчивость	Появление новых технологий приводит к новым угрозам безопасности	0,75
	Изменение законодательства может привести к необходимости изменения мер безопасности	
	Экономическая ситуация влияет на платежеспособность клиентов и на деятельность компании в целом	
Факторы, обусловливающие неопределенность	Геополитическая ситуация способствует возникновению новых угроз безопасности	0,8
	Стихийные бедствия повреждают объекты инфраструктуры компании	
	Человеческий фактор обуславливает возникновение различных конфликтных инцидентов	

Составлено автором по данным АО «Мосэнергосбыт».

Для оценки неустойчивости факторов в пределах каждой компоненты корпоративной безопасности будут использоваться следующие критерии:

- сложность ($K_{сл}$) — уровень сложности реализации мер по защите от угрозы;
- взаимозависимость ($K_{взи}$) — степень взаимосвязи угрозы с другими угрозами;
- изменчивость ($K_{изм}$) — скорость изменения характера угрозы;
- неопределенность ($K_{н}$) — степень неопределенности информации об угрозе.

Оценка каждого фактора по каждому критерию будет осуществляться по шкале от 1 до 5, где:

1 — низкий уровень;

2 — средний уровень;

4 — высокий уровень;

4 — очень высокий уровень;

5 — максимально высокий уровень.

Общий уровень нестабильности факторов отдельного компонента (N_{ki}) будет рассчитываться по следующей формуле:

$$N_{ki} = \left(K_{сл} + K_{взи} + K_{изм} + K_{н}\right) / 4. \quad (2)$$

Интегральный уровень корпоративной безопасности предприятия ($K_{и}$) будет рассчитываться по следующей формуле:

$$K_{и} = \left(N_{ki1} + N_{ki2} + N_{ki3} + N_{ki4}\right) / 4. \quad (3)$$

Результаты оценки корпоративной безопасности АО «Мосэнергосбыт» будут представлены в виде таблиц.

Таблица 2

Оценка неустойчивости факторов в пределах каждой компоненты корпоративной безопасности АО «Мосэнергосбыт»

№ п/п	Компоненты	Фактор	$K_{сл}$	$K_{взи}$	$K_{изм}$	$K_{н}$	N_{ki}
1	Физический	Защита объектов инфраструктуры	5	4	4	3	4
2	Кадровый	Обеспечение безопасности персонала	4	3	3	2	3,2
3	Экономический	Предотвращение краж и диверсий	4	3	3	2	3,2
4	Информационный	Защита конфиденциальной информации	5	4	4	3	4
5	Репутационный	Управление репутацией	4	3	3	3	3,5
6	Организационно-правовой	Соблюдение законодательства	4	3	3	2	3,2
7	Управление рисками	Контроль рисков	4	3	3	3	3,5

Составлено автором по данным АО «Мосэнергосбыт».

Оценка интегрального уровня корпоративной безопасности предприятия (Ки) по формуле:

$$K_{б} = N_{ki} \times W_{ki}, \quad (4)$$

где W_{ki} — вес фактора.

Веса факторов (W_{ki}) даны в таблице.

Таблица 3

Веса факторов (W_{ki}) АО «Мосэнергосбыт»

Компонент	W_{ki}
Физическая безопасность	0.25
Кадровая безопасность	0.20
Информационная безопасность	0.10
Экономическая безопасность	0.10
Репутационная безопасность	0.25
Организационно-правовая безопасность	0.10
Управление рисками	0.10

Составлено автором по данным АО «Мосэнергосбыт».

Теперь, используя формулу $K_и = N_{ki} * W_{ki}$, рассчитаем интегральный уровень корпоративной безопасности предприятия ($K_и$) для каждого компонента АО «Мосэнергосбыт».

Таблица 4

Интегральный уровень корпоративной безопасности предприятия (Кб) для каждого компонента АО «Мосэнергосбыт»

Компонент	N_{ki}	W_{ki}	$K_и$
Физический	3,83	0,25	0,958
Кадровый	3,20	0,20	0,640
Экономический	3,20	0,25	0,800
Информационный	4,00	0,10	0,400
Репутационный	4,00	0,25	1,000
Организационно-правовой	3,60	0,10	0,360
Управление рисками	3,75	0,10	0,375

Составлено автором по данным АО «Мосэнергосбыт».

Для расчета итогового необходимо суммировать Ки всех компонентов:

$$K_б = 0,958 + 0,640 + 0,800 + 0,400 + 1,0 + \\ + 0,360 + 0.375 = 4,533.$$

Интерпретация результатов показала, что 4,533 — это высокий уровень корпоративной безопасности и означает, что компания обладает достаточно надежной системой защиты от различных угроз. Тем не менее всегда есть возможности для дальнейшего совершенствования системы безопасности.

На основании проведенной оценки можно сделать вывод о том, что уровень корпоративной безопасности АО «Мосэнергосбыт» является высоким.

4. ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

Обеспечение корпоративной безопасности АО «Мосэнергосбыт» является не только актуальной, но и сверхсложной для решения проблемой. Важность обуславливается развитием корпоративного сектора и его способностью стабилизировать ситуацию в национальной экономике, а затем уменьшить социальную и политическую напряженность.

Сложность проблемы обусловлена быстрым изменением ситуации и как следствие наличием трудностей по созданию информационной основы, проведению аналитических исследований, возможностью апробации и внедрению в практическую деятельность АО «Мосэнергосбыт». Имеет место ситуация, когда сложившиеся теоретические разработки не способны способствовать решению проблемы вследствие уже отличных фактических условий от заданных факторов.

В динамично меняющейся экономической среде ученые вынуждены постоянно корректировать свои представления и совершенствовать теоретические и методологические аспекты обеспечения корпоративной безопасности на предприятиях. При этом они опираются на ценный опыт действующих компаний, анализируя их успехи и промахи в конкретных ситуациях.

Отдельные факторы, несмотря на изменчивость параметров функционирования предприятий, остаются доведенными, и к их числу относится необходимость создания системы корпоративной безопасности. Именно в соответствии с системным подходом, о чем неоднократно отмечалось выше, сохранение предприятия как социально-экономической системы требует создания системы корпоративной безопасности, которая и должна обеспечить надлежащий уровень устойчивости, адаптивности, жизнеспособности, надежности предприятия. Условия ведения бизнеса в нашей стране заставили субъектов хозяйствования усовершенствовать или же инстинктивно создать разного уровня сложности системы корпоративной безопасности. Их задачи заключаются от физической защиты территории до осуществления деловой разведки и реализации контрразведывательных мероприятий. Характерно и существенное отличие в ресурсном и организационном обеспечении, интенсивности взаимодействия с правоохранительными органами и результативности действий субъектов безопасности. Общим является осознание того, что только через обеспечение корпоративной безопасности есть возможность сохранения и развития бизнеса.

Понимая многогранную природу корпоративной безопасности и применяя синергетический подход, компании могут создать надежный механизм защиты от широкого спектра угроз. Такой проактивный подход способствует созданию безопасной среды, которая защищает ценные активы, повышает безопасность сотрудников и обеспечивает непрерывность бизнеса, что в конечном итоге приводит к долгосрочному успеху.

Литература

1. *Иванов А.В.* Система корпоративной финансовой безопасности [Текст] / А.В. Иванов // Современные финансовые рынки в условиях новой экономики: Материалы

References

1. Ivanov A.V. The system of corporate financial security // Modern financial markets in the new economy: Materials of the 3rd International Interuniversity Scientific and Practical

3-й Международной межвузовской научно-практической конференции, Москва, 22 февраля 2023 года. – М.: Изд-во Российского экономический ун-та имени Г.В. Плеханова, 2023. – С. 278–286.
2. *Истратов Б.И*. Корпоративная безопасность как аспект устойчивого развития бизнеса [Текст] / Б.И. Истратов // Экономика устойчивого развития. – 2022. – № 1. – С. 40–44.
3. *Леванова Л.Н*. Корпоративная безопасность: стейкхолдерский подход [Текст] / Л.Н. Леванова, А.В. Вавилина // Вестник Московской международной высшей школы бизнеса МИРБИС / Автономная некоммерческая организация высшего образования «Московская международная высшая школа бизнеса МИРБИС (Институт)». – М., 2022. – С. 128–142.
4. *Леванова Л.Н*. Корпоративный контроль: стейкхолдерский подход [Текст] / Л.Н. Леванова, А.В. Вавилина // Государственное управление. Электронный вестник. — 2023. — № 101. — С. 44–55
5. *Леванова Л.Н*. Мажоризация и оппортунистическое поведение менеджеров: противоречия и направления их разрешения [Текст] / Л.Н. Леванова, А.В. Вавилина // Вестник Московской международной высшей школы бизнеса МИРБИС / Автономная некоммерческая организация высшего образования «Московская международная высшая школа бизнеса МИРБИС (Институт)». – М., 2021. – С. 79–86.
6. *Никитина И.А*. Вопросы оценки угроз кадровой безопасности организации в современных условиях [Текст] / И.А. Никитина, К.В. Хмелевской, П.В. Назаров // Инновации и инвестиции. – 2023. – № 11. – С. 150–153.
7. *Соколова Е.О*. Роль корпоративной культуры в обеспечении кадровой безопасности организации [Текст] / Е.О. Соколова, Я.А. Коренчук // Журнал социологических исследований. – 2024. – Т. 9. — № 1. – С. 51–57.
8. *Фролов А.В*. Корпоративная безопасность и обеспечение защиты данных от утечки в условиях удаленной работы [Текст] / А.В. Фролов, Ю.В. Дымченко // Промышленные АСУ и контроллеры. – 2023. – № 9. – С. 47–49.
9. *Ширенина А.А*. Роль информационной составляющей в формировании системы корпоративной безопасностив условиях цифровой трансформации [Текст] / А.А. Ширенина // Проблемы бизнеса и управления в современных условиях: сборник статей по материалам студенческой научно-практической конференции, Москва, 21 октября 2022 года / Российский университет транспорта (РУТ МИИТ), Российская открытая академия транспорта. – М.: МАКС Пресс, 2022. – С. 98–102.
10. *Якушкина А.А.* Кадровая безопасность как одна из составляющих экономической безопасности [Текст] / А.А. Якушкина, А.Ф. Юмангулов // XI Международный молодежный симпозиум по управлению, экономике и финансам: Сборник научных трудов, Казань, 24–25 ноября 2022 года. – Казань: Изд-во Казанского (Приволжского) федерального ун-та, 2022. – С. 758–761.

Conference, Moscow, February 22, 2023. Moscow: Plekhanov Russian University of Economics, 2023, pp. 278–286.
2. Istratov B.I. Corporate security as an aspect of sustainable business development // The economics of sustainable development, 2022, no. 1, pp. 40–44.
3. Levanova L.N., Vavilina A.V. Corporate security: a stakeholder approach // Bulletin of the Moscow International Higher School of Business MIRBIS / Autonomous non-profit Organization of Higher Education Moscow International Higher School of Business MIRBIS (Institute). Moscow, 2022, pp. 128–142.
4. Levanova L.N., Vavilina A.V. Corporate control: a stakeholder approach // Public administration. Electronic bulletin, 2023, no. 101, pp. 44–55.
5. Levanova L.N., Vavilina A.V. Majorization and opportunistic behavior of managers: contradictions and directions of their resolution // Bulletin of the Moscow International Higher School of Business MIRBIS / Autonomous non-profit Organization of Higher Education Moscow International Higher School of Business MIRBIS (Institute). Moscow, 2021, pp. 79–86.
6. Nikitina I.A., Khmelevskaya K.V., Nazarov P.V. Issues of assessing threats to the personnel security of an organization in modern conditions // Innovations and investments, 2023, no. 11, pp. 150–153.
7. Sokolova E.O., Korenchuk Ya.A. The role of corporate culture in ensuring the personnel security of an organization // Journal of Sociological Research, 2024, vol. 9, no. 1, pp. 51–57.
8. Frolov A.V., Dymchenko Yu.V. Corporate security and ensuring data protection from leakage in remote work // Industrial automated control systems and controllers, 2023, no. 9, pp. 47–49.
9. Shirenina A.A. The role of the information component in the formation of a corporate security system in the context of digital transformation // Problems of business and management in modern conditions: a collection of articles based on the materials of the student scientific and practical conference, Moscow, October 21, 2022 / Russian University of Transport (RUT MIIT), Russian Open Academy of Transport. Moscow: MAX Press LLC, 2022, pp. 98–102.
10. Yakushkina A.A., Yumangulov A.F. Personnel security as one of the components of economic security // XI International Youth Symposium on Management, Economics and Finance: Collection of scientific papers, Kazan, November 24–25, 2022. Kazan: Kazan (Volga Region) Federal University, 2022, pp. 758–761.