

Смирнов Евгений Николаевич
Московская международная академия

Управление безопасностью бизнес-структур в современных экономических реалиях

Аннотация. Статья посвящена исследованию управления безопасностью бизнес-структур в современных экономических реалиях, имеющих значительное влияние на функционирование и устойчивость предприятий. Актуальность темы обусловлена изменчивостью экономической среды, в которой функционируют современные предприятия.

Обзор литературы показывает недостатки существующих подходов и необходимость их переосмысления в условиях новых вызовов. Кроме того, статья классифицирует риски, с которыми сталкиваются бизнес-структуры, и описывает методы их оценки и анализа, приводя примеры для различных отраслей.

Важное внимание уделяется стратегиям управления безопасностью в условиях неопределенности, в процессе разработки и внедрения которых необходимо оптимизировать процессы и использовать успешные кейс-стадии. Также рассматриваются инновационные подходы, включая применение технологий и развитие человеческого капитала как критически важных элементов обеспечения безопасности.

В заключение подведены итоги исследования, предложены практические рекомендации для бизнес-структур и обозначены перспективы дальнейших исследований в области управления безопасностью, что делает данную статью полезным источником информации для руководителей и специалистов, работающих в сфере управления безопасностью в условиях постоянно меняющегося экономического ландшафта.

Ключевые слова: управление безопасностью, бизнес-структуры, экономические реалии, риски, кибербезопасность, стратегии, оптимизация, инновации.

Smirnov Evgeny Nikolaevich
Moscow International Academy

Security management of business structures in modern economic realities

Annotation. The article is devoted to the study of security management of business structures in modern economic realities, which have a significant impact on the functioning and sustainability of enterprises. The relevance of the topic is due to the variability of the economic environment in which modern enterprises operate.

A review of the literature shows the shortcomings of existing approaches and the need to rethink them in the face of new challenges. In addition, the article classifies the risks faced by business structures and describes the methods of their assessment and analysis, giving examples for various industries.

Important attention is paid to security management strategies in conditions of uncertainty, during the development and implementation of which it is necessary to optimize processes and use successful case stages. Innovative approaches are also considered, including the use of technology and the development of human capital as critical elements of security.

In conclusion, the results of the study are summarized, practical recommendations for business structures are proposed and prospects for further research in the field of security management are outlined, which makes this article a useful source of information for managers

and specialists working in the field of security management in an ever-changing economic landscape.

Keywords: security management, business structures, economic realities, risks, cybersecurity, strategies, optimization, innovations.

В условиях быстро меняющегося глобального экономического ландшафта, управление безопасностью бизнес-структур стало одной из ключевых задач для компаний, стремящихся сохранить свою конкурентоспособность и устойчивость. Современные экономические реалии, такие как глобализация, цифровизация и регулярные экономические кризисы, обостряют риски, с которыми сталкиваются организации, и требуют поиска инновационных подходов к обеспечению безопасности. Бизнес-структуры должны не только защищать свои активы, но и быть готовыми эффективно реагировать на потенциальные угрозы, которые могут сильно повлиять на их операционную деятельность.

Целью данной статьи является систематизация знаний о современных методах и стратегиях управления безопасностью, а также анализ влияния актуальных экономических факторов на работу бизнес-структур. В рамках исследования сформулированы следующие задачи:

1. Определить основные компоненты системы управления безопасностью;
2. Классифицировать риски, угрожающие бизнес-структурам в современных условиях;
3. Оценить эффективность существующих стратегий и предложить возможности их оптимизации.

Обзор литературы показывает, что тема управления безопасностью бизнеса активно исследуется в теории и практике. Предыдущие исследования акцентировали внимание на понимании сущности управления безопасностью, его роли в снижении рисков и оптимизации бизнес-процессов. Однако до сих пор недостаточно внимания уделено влиянию современных экономических реалий, таких как риск кибератак и вирусов, волатильность финансовых рынков и изменения в международной торговле, на систему управления безопасностью. Это создает необходимость дальнейшего изучения и переосмысления подходов к управлению безопасностью, что и будет рассмотрено в данной статье.

Теоретические основы управления безопасностью

Управление безопасностью бизнес-структур охватывает комплекс мероприятий, направленных на защиту материальных, нематериальных и человеческих ресурсов организаций от разных видов угроз. С учетом современного контекста управления безопасностью понимается как системный процесс, в который входят идентификация, анализ и минимизация рисков, угрожающих бизнесу. Важной составляющей данного процесса является формирование стратегии, которая бы учитывала специфические особенности и потребности каждой отдельной компании.

В современных экономических реалиях управление безопасностью подразумевает не только меры по физической охране объектов, но и защиту информационных систем, управление рисками, связанными с киберугрозами, а также соблюдение норм соблюдения законодательства. Такой подход позволяет не только уменьшить вероятность возникновения инцидентов, но и минимизировать последствия выявленных угроз, прописывая конкретные действия на случай их реализации [11].

Управление безопасностью занимает центральное место в стратегии деятельности любой бизнес-структуры. Оно охватывает весь спектр действий, от базовых технологий безопасности до разработки корпоративной культуры, ориентированной на осознание и минимизацию рисков. Основная роль управления безопасностью заключается в следующем. Во-первых, защита активов. Эффективное управление безопасностью позволяет сохранить материальные и нематериальные активы компании, включая интеллектуальную собственность, данные клиентов и финансовые ресурсы. Во-вторых,

устойчивость к рискам. Бизнес-структуры, обладая налаженной системой управления безопасностью, существенно повышают свою устойчивость к экономическим атакам, правовым рискам и другим факторам, угрожающим их нормальному функционированию. В-третьих, повышение доверия. Надежная система управления безопасностью способствует повышению доверия со стороны клиентов, партнеров и акционеров, что, в свою очередь, улучшает репутацию компании на рынке. И в-четвертых, соответствие нормативным требованиям. В современном бизнесе крайне важно соблюдать законодательные и регуляторные требования, что требует внедрения стандартов управления безопасностью [4].

Таким образом, когда управление безопасностью рассматривается как важный элемент общекорпоративной стратегии, оно становится ключевым фактором, способствующим успешной работе и стабильному развитию бизнеса.

Система управления безопасностью бизнес-структуры состоит из нескольких ключевых компонентов, каждый из которых играет важную роль в создании устойчивой и эффективной структуры:

1. Анализ рисков. Включает в себя выявление и оценку потенциальных угроз, что позволяет понять уязвимости бизнеса и разработать соответствующие меры по их минимизации. Этап анализа рисков включает как качественные методы (интервью, опросы), так и количественные (статистический анализ данных).

2. Политики безопасности. Формирование документации, регламентирующей меры и процедуры безопасности. Это могут быть как внутренние инструкции, так и внешние стандарты (например, ISO 27001, ISO 22301), которые способствуют созданию структурированной системы.

3. Обучение и осведомленность сотрудников. Поскольку человеческий фактор является одним из основных источников рисков, регулярное обучение и повышение осведомленности сотрудников о необходимых мерах безопасности являются критически важными для предотвращения инцидентов.

4. Технологические меры. Внедрение современных технологий защиты информации, включая системы управления доступом, антивирусное программное обеспечение, шифрование данных и системы обнаружения вторжений.

5. Контроль и аудит. Регулярный мониторинг и аудит функционирования системы управления безопасностью позволяют выявлять недостатки и обновлять политику безопасности на основе актуальных данных и изменяющихся условий.

То есть, интеграция всех этих компонентов в единую систему позволяет бизнес-структурам эффективно управлять безопасностью, обеспечивать защиту от потенциальных угроз и минимизировать риски, способствуя устойчивому росту и развитию организации [1].

Современные экономические реалии и их влияние на безопасность бизнеса

Экономические кризисы, как правило, наносят серьезный ущерб всем сферам бизнеса, обостряя конкуренцию и создавая новые риски для устойчивости бизнес-структур. Последствия таких кризисов могут быть многообразными:

1. Сокращение объемов инвестиций. В условиях экономической неопределенности компании склонны к сокращению инвестиций, что может привести к снижению инновационной активности и, как следствие, к увеличению вероятности старения технологий и устаревания бизнеса.

2. Снижение спроса на товары и услуги. Рецессия или экономический спад неминуемо затрагивают потребительские расходы, что сказывается на доходах компании и может привести к неустойчивым финансовым показателям. Сокращение доходов заставляет бизнес-структуры пересматривать свои стратегии управления безопасностью, а также уменьшать бюджет на защитные меры.

3. Увеличение мошенничества и правонарушений. В условиях кризиса возрастает вероятность правонарушений, включая коррупцию, присвоение средств и

киберпреступность [13]. Бизнесы становятся более уязвимыми к мошенническим действиям, так как сотрудники могут быть склонны к рискованным решениям.

4. Необходимость пересмотра корпоративных стратегий. Кризисы требуют от компаний быстрого реагирования и адаптации к новым условиям. Это нередко приводит к необходимости пересмотра подходов к управлению безопасностью, внедрению новых бюджетных мер и усилению контроля [2, 7, 8].

Таким образом, кризисы требуют от бизнес-структур гибкости и готовности к переменам, подчеркивая важность наличия устойчивой системы управления безопасностью.

С развитием информационных технологий и цифровых платформ бизнес-структуры сталкиваются с уникальными вызовами и угрозами, связанными с кибербезопасностью.

Увеличение числа кибератак, включая фишинг, ransomware и DDoS-атаки, ставит организации перед необходимостью внедрения комплексных систем защиты информации. Выросший объем данных, который обрабатывается бизнесами, делает их цельными объектами для злоумышленников. Поэтому возникает необходимость инвестирования в защиту. Интеграция современных технологий требует значительных финансовых вложений в системы киберзащиты, такие как антивирусные программы, firewall и другие меры защиты. При этом экономическая целесообразность таких инвестиций часто ставится под сомнение в условиях ограниченных ресурсов [5].

Применение новых технологий требует от сотрудников понимания рисков и методов защиты информации. Нехватка знаний может значительно повысить уязвимость бизнес-структуры, так как большинству кибератак предшествуют действия, неосторожные со стороны пользователей. С ростом числа происшествий в сфере кибербезопасности увеличивается и количество законов и норм, регулирующих защиту данных. Компании обязаны следовать этим требованиям, что приводит к дополнительным затратам и организационным изменениям.

Таким образом, новые технологии как вносят значительные улучшения в бизнес-процессы, так и создают новые риски, которые требуют гибкости в подходах к управлению безопасностью.

Глобализация открывает перед бизнес-структурами новые горизонты, но вместе с тем создает и ряд уникальных рисков. В условиях глобальной экономики компании сталкиваются с конкурентами со всего мира, что требует от них оптимизации своих процессов и безопасности, чтобы успешно функционировать на международных рынках. Глобализация в свою очередь приводит к увеличению длины и сложности цепочек поставок, вне зависимости от того, какое оборудование, материалы или услуги поставляются. Это создает дополнительные риски, связанные с потенциальными сбоями в поставках и уязвимостями в разных регионах.

И, конечно, геополитические риски. Текущие международные отношения могут влиять на стабильность рынка и защиту активов. Политическая нестабильность, экономические санкции и изменения в законодательстве могут существенно изменять условия ведения бизнеса за границей.

Таким образом, в условиях глобализации компании должны не только учитывать новые возможности, но и проводить полноценный анализ потенциальных угроз, связанных с международными операциями, что требует от них наличия гибкой и многоуровневой системы управления безопасностью.

В итоге, современные экономические реалии требуют от бизнес-структур не только адаптации к изменяющимся условиям, но и активного пересмотра подходов к управлению безопасностью, чтобы успешно преодолевать возникающие риски и устойчиво развиваться в условиях неопределенности.

Анализ рисков для бизнес-структур

Анализ рисков является важным аспектом управления любым бизнесом. Он позволяет организациям идентифицировать, оценить и минимизировать потенциальные

угрозы, которые могут повлиять на их деятельность. В данном разделе рассмотрим классификацию рисков, методы их оценки и анализа, а также примеры рисков, с которыми могут столкнуться предприятия в различных отраслях.

Риски можно классифицировать по различным критериям. Ниже приведены основные категории:

1. Финансовые риски: связаны с изменениями в рыночных условиях, валютными колебаниями, кредитными рисками и изменениями процентных ставок. Примером может служить рост процентной ставки, который увеличивает стоимость заимствований для компаний.

2. Операционные риски: связаны с внутренними процессами, системами и персоналом компании. Это могут быть проблемы с поставками, сбои в производственных системах или низкая квалификация сотрудников.

3. Стратегические риски: связаны с неправильным выбором стратегии развития или изменениями на уровне рынка. Например, компания, производящая традиционные автомобили, может столкнуться с рисками, связанными с переходом к электромобилям.

4. Репутационные риски: возникают из-за негативного восприятия компании общественностью. Например, кампании в социальных сетях могут резко повлиять на имидж бренда.

5. Регуляторные риски: возникают в результате изменения законодательства или нормативных актов. Например, новые эколого-требования могут потребовать от бизнеса значительных инвестиций в модернизацию технологий [3, 8].

Существует также несколько методов, которые позволяют оценить и проанализировать риски:

1. Качественный анализ: включает идентификацию рисков и их оценку с использованием экспертных мнений и опросов. Этот метод хорошо подходит для начала работы с рисками, позволяя быстро получить представление о ситуации.

2. Количественный анализ: включает использование статистических методов для количественной оценки рисков. Примеры включают анализ вариантов и моделирование Монте-Карло, которые помогают определить вероятности и потенциальные потери.

3. SWOT-анализ: позволяет оценить сильные и слабые стороны организации, а также возможности и угрозы, что дает возможность понять, какие риски являются наиболее значительными.

4. Метод сценариев: заключается в разработке различных сценариев, в которых оцениваются возможные последствия конкретных рисков. Это позволяет организациям подготовиться к различным исходам [9, 12].

Подводя итог, можно сказать, что анализ рисков является важным элементом стратегического планирования для любого бизнеса. Понимание классификации рисков и применение различных методов их оценки поможет компаниям более эффективно управлять своими ресурсами и быть готовыми к непредвиденным обстоятельствам.

Раздел 4. Стратегии управления безопасностью в условиях неопределенности

В условиях неопределенности, которые стали нормой в современном бизнесе, крупные и малые организации сталкиваются с множеством вызовов, требующих эффективных стратегий управления безопасностью. Организации должны разрабатывать и внедрять стратегии, которые обеспечивают безопасность активов, информации и репутации, оптимизируя при этом собственные ресурсы и процессы.

Разработка стратегий управления безопасностью начинается с всестороннего анализа существующих угроз и уязвимостей, с которыми сталкивается организация. Важными этапами этого процесса являются:

1. Оценка рисков: необходимо провести комплексную оценку потенциальных рисков. Это может включать в себя как внутренние, так и внешние риски, с которыми организация может столкнуться.

2. Определение приоритетов, где важно установить приоритеты для управления безопасностью, исходя из значимости каждой угрозы. Например, если информационные утечки представляют наибольшую опасность, организация должна сосредоточить усилия на защите своих данных.

3. Разработка политик и процедур. На основе проведенной оценки и установленных приоритетов разрабатываются политики и процедуры, которые направлены на предотвращение, минимизацию и реагирование на инциденты.

4. Обучение и осведомленность сотрудников. Внедрение стратегии управления безопасностью требует постоянного обучения и повышения осведомленности сотрудников, чтобы они понимали и соблюдали новые правила.

5. Мониторинг и пересмотр. Стратегия должна быть гибкой и регулярно пересматриваться в условиях меняющейся внешней среды и новых угроз [6].

Оптимизация процессов безопасности включает в себя ряд мероприятий, которые помогают организациям сократить затраты и повысить эффективность управления рисками. Основными направлениями оптимизации бизнес-структур в современных экономических реалиях должны стать:

- автоматизация процессов, которая предполагает внедрение технологий, таких как системы управления безопасностью, позволяет автоматизировать рутинные операции, снизив вероятность ошибок и повысив скорость реакции на инциденты.

- интеграция технологий при которой происходит объединение различных систем безопасности (физической, IT и персональной) в единую структуру повышения общей безопасности.

- использование аналитических инструментов для оценки эффективности существующих мер безопасности и выявления возможных уязвимостей.

- сокращение избыточных процедур и упрощение подходов к управлению безопасностью позволяет повысить реактивность системы при угрозах.

- взаимодействие с внешними партнерами предполагает координацию и взаимопомощь с другими организациями, правоохранительными органами, позволяя использовать лучшие практики и снижение рисков.

В условиях динамично меняющегося экономического ландшафта управление безопасностью бизнес-структур становится не просто необходимостью, а основополагающим элементом успешной деятельности. Проведенное исследование показало, что эффективное управление безопасностью предполагает комплексный подход, учитывающий, как внутренние, так и внешние риски, а также технологические и человеческие аспекты. В результате анализа ключевых аспектов управления безопасностью, включая стратегии, методы оценки рисков и примеры из практики, были сформулированы следующие выводы, рекомендации и перспективы для будущих исследований.

Во-первых, современные бизнес-структуры сталкиваются с возрастающим числом угроз, включая кибератаки, экономические нестабильности и изменения в законодательстве, что требует постоянного мониторинга и адаптации стратегий безопасности.

Во-вторых, наличие четкой и гибкой стратегии управления безопасностью является залогом защиты активов и минимизации рисков. Стратегии должны включать как технические, так и организационные меры.

В-третьих, эффективная реализация мер безопасности невозможна без активного участия и понимания со стороны всех сотрудников. Культура безопасности внутри компании способствует снижению человеческого фактора и увеличению общей устойчивости организации.

Рекомендуется активно внедрять новые технологии для автоматизации и улучшения процессов безопасности, включая системы мониторинга, аналитические инструменты и решения кибербезопасности.

Необходимо регулярно проводить тренинги для сотрудников, направленные на повышение осведомленности о рисках и обучение методам предотвращения угроз.

Каждая организация должна иметь готовые плановые мероприятия на случай возникновения чрезвычайных ситуаций. Это включает четкие инструкции для сотрудников на случай различных инцидентов.

Необходимо регулярно пересматривать и обновлять стратегии управления безопасностью в соответствии с изменениями в внешней среде и новым вызовам.

В контексте продолжающихся изменений и вызовов, управление безопасностью бизнес-структур будет оставаться актуальной и востребованной темой, требующей внимания и комплексного подхода как от бизнеса, так и от исследователей.

Список источников

1. Авдеева И.Л., Ананченкова П.И., Белолипецкая А.Е., Боброва Е.А., и др. Интеграция кадровой политики в систему управления национальными проектами. Монография. – Орел: Среднерусский институт управления - филиал РАНХиГС, 2020.
2. Баранов Р.С. Аутсорсинг безопасности: процессы и риски в управлении // Экономика и управление: вызовы и перспективы. 2024. Т. 18. № 3. С. 77-89.
3. Беляев Ю.А. Анализ рисков в управлении безопасностью: современные подходы и методологии // Журнал международного бизнеса. 2024. Т. 11. № 1. С. 24-36.
4. Громова Н.В. Аудит безопасности бизнес-структур в современных условиях: подходы и методы // Научный журнал «Экономика и управление». 2022. Т. 29. № 4. С. 88-99.
5. Дьякова Е.В., Алексеев И.Г. Управление бизнес-рисками: теоретический и практический подходы // Энергетика и безопасность. 2024. Т. 12. № 2. С. 101-114.
6. Ершова А.К. Информационные технологии в управлении безопасностью бизнес-структур // Журнал информационных технологий. 2023. Т. 10. № 1. С. 35-47.
7. Жуков И.М. Управление рисками в бизнес-структурах: проблемы и решения // Российский экономический журнал. 2023. Т. 27. № 3. С. 45-58.
8. Ковалев Д.Е. Методы оценки рисков для бизнес-структур в условиях нестабильности // Проблемы теории и практики управления. 2023. Т. 14. № 8. С. 67-78.
9. Кузнецова Л.А., Фролов В.Я. Риски в управлении безопасностью: анализ и оценка // Современные исследования проблем экономики. 2023. Т. 19. № 2. С. 55-70.
10. Новиков А.К. Подходы к обеспечению безопасности бизнес-структур: теоретические аспекты // Вестник Санкт-Петербургского государственного университета. 2022. Т. 15. № 5. С. 112-123.
11. Павлова Н.П. Роль и важность управления безопасностью в современных бизнес-структурах // Научный вестник Юга России. 2023. Т. 8. № 4. С. 52-64.
12. Сидоров А.–И., Петрова О.Л. Теоретические основы управления безопасностью бизнес-структур // Управление и финансы. 2023. Т. 22. № 1. С. 34-45.
13. Федорова Т.М. Проблемы и перспективы безопасности современных бизнес-структур // Вестник предпринимательства. 2022. Т. 7. № 6. С. 56-69.

Информация об авторе

Смирнов Евгений Николаевич, аспирант Московской международной академии, г. Москва, Россия

Information about the author

Smirnov Evgeny Nikolaevich, PhD student at the Moscow International Academy, Moscow, Russia