МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Факультет экономический
Кафедра теоретической экономики

КУРСОВАЯ РАБОТА
по дисциплине: «Бизнес-анализ»

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ООО «БОМББАР»

Работу выполнила Осипян 26.05.2025 А.О. Осипян
(подпись, дата)

Специальность 38.03.05 – Бизнес-информатика курс 3

Направленность (профиль) Бизнес в цифровой экономике

Научный руководитель
д. экон. наук, профессор 26.05.2025 В.А. Сидоров
(подпись, дата)

Нормоконтролер
д. экон. наук, профессор 26.05.2025 В.А. Сидоров
(подпись, дата)

Краснодар
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данная курсовая работа посвящена анализу экономической безопасности предприятия в условиях цифровой экономики.

Актуальность темы работы обусловлена стремительной цифровизацией экономики и переходом предприятий на принципы Индустрии 4.0. В современных условиях хозяйствования цифровые технологии проникают во все сферы бизнеса – от автоматизации производственных процессов до перехода на электронный документооборот и цифровые платформы взаимодействия с контрагентами. Этот процесс, с одной стороны, открывает новые возможности для повышения эффективности деятельности компании, а с другой – создает принципиально новые угрозы их экономической безопасности.

Целью работы является комплексное исследование эволюции концепций экономической безопасности предприятий – от традиционных подходов до современных цифровых трансформаций – с последующим анализом уязвимостей конкретного предприятия и разработкой практический рекомендаций по совершенствованию его системы защиты в условиях цифровой экономики.

Для достижения указанной цели необходимо выполнить следующие *задачи:*

– изучить теоретические основы формирования экономической безопасности предприятия,

– проанализировать ключевые элементы системы экономической безопасности организации,

– рассмотреть особенности трансформации экономической безопасности в условиях цифровой экономики,

– дать характеристику деятельности рассматриваемого предприятия,

– оценить текущее состояние цифровой безопасности предприятия,

– проанализировать внутренние и внешние угрозы цифровой безопасности, и на этой основе определить приоритетные направления по совершенствованию системы информационной безопасности предприятия.

Объект исследования – общество с ограниченной ответственностью «БОМББАР», ведущий производитель товаров спортивного питания в России. Компания неоднократно сталкивалась с вызовами в сфере цифровой безопасности производства, что делает её ключевым примером для анализа современных угроз и способов их минимизации в условиях цифровизации бизнес-процессов.

Предметом исследования являются процессы, методы и механизмы обеспечения экономической безопасности предприятия в условиях цифровой трансформации.

Для решения поставленных задач были использованы следующие *методы:* системный и сравнительный анализ, синтез, дедукция, анализ статистических данных, факторный анализ.

В качестве *информационной базы* исследования были использованы научные публикации, научные статьи, монографии, новостные статьи, Интернет-материалы, нормативно-правовые акты, устав предприятия, документы первичной отчётности.

1 Теоретические аспекты экономической безопасности организации

1.1 Развитие теории экономической безопасности

Экономическая безопасность – это способность экономики страны, региона или отдельного предприятия устойчиво развиваться, защищать свои интересы и противостоять внутренним и внешним угрозам. В зависимости от масштаба охвата и субъектов экономической безопасности она работает на разных уровнях: государственном, региональном и уровне предприятия [23].

Экономическая безопасность страны заключается в: суверенной экономике, финансовой стабильности, технологической независимости, энергетической и продовольственной безопасности, социальной защите и контроле стратегически важных ресурсов. Экономическая безопасность региона означает устойчивое развитие за счет: сбалансированной экономики, стабильных доходов бюджета, развитой инфраструктуры, социальной стабильности, а для предприятия в: минимизации рисков, сохранении платежеспособности, защите активов, обеспечении конкурентоспособности и отсутствии зависимости.

Развитие теории экономической безопасности тесно связано с цикличностью экономического развития. В периоды экономического благополучия интерес к этой теме снижается, тогда как в кризисные времена научный анализ рисков и угроз для национальной экономики становится приоритетным направлением исследований. Исторически, развитие теории экономической безопасности началось с 1930-х годов, когда западные ученые, такие как Джон Мейнард Кейнс, внесли значительный вклад в формирование концепции защиты от внутренних макроэкономических угроз. В России особое внимание к экономической безопасности стало актуальным в 1990-х годах, когда страна переживала глубокий экономический кризис и формировала новую концепцию национальной безопасности [11].

Современная теория экономической безопасности включает в себя синтез различных теорий, включая экономическую, системную, теории катастроф и конфликтов, что позволяет обеспечить комплексное понимание и управление экономическими рисками.

Основные этапы формирование теории экономической безопасности можно выделить следующим образом:

– 1930-е годы: начало формирование теоретических исследований в области экономической безопасности на Западе;

– 1990-е годы: в России особое внимание к экономической безопасности стало актуальным в связи с глубоким экономическим кризисом и формированием новой концепции национально безопасности;

– современный период: развитие теории экономической безопасности включает в себя синтез различных теорий, включая экономическую, системную, теории катастроф и конфликтов [22].

Эволюция теории экономической безопасности тесно связана с осмыслением экономических кризисов, каждый из которых стимулировал развитие новых концепций защиты национальной экономики.

Ф. Лист впервые обосновал необходимость протекционистских мер как инструмента противодействия внешним угрозам, заложив основы понимания экономической безопасности. Глобальный кризис 1930-х г. нашли отражение в трудах Дж. М. Кейнса, где впервые была предложена система государственного антикризисного регулирования, ставшая теоретической основой экономической безопасности на макроуровне. Распад СССР и системный кризис 1990-х г. актуализировали исследования в области экономической безопасности в России. Л. И. Абалкин сформулировал принципы устойчивости и стабильности экономики в переходный период. Дальнейшее развития теория получила в работах В. К. Сенчагова, где была предложена комплексная система классификаций угроз экономической стабильности. Современный этап, характеризующийся стремительной цифровизацией, отражается в работе В. А. Сидорова и А. Ш. Хуажевой.

Сегодня Россия является лидером по темпам развития теории экономической безопасности. В 1992 г. был принят Закон РФ от 05.03.1992 г. №2446-1 «О безопасности», в 1996 г. вступает в силу Указ Президента РФ от 29.04.1996 г. №608 «О государственной стратегии экономической безопасности Российской Федерации», который утратил свою силу в 2017 г., так как была принята Стратегия экономической безопасности Российской Федерации на период до 2030 г. [10, 19, 20].

В таблице 1 представлены основные теории развития экономической безопасности.

Таблица 1 – Основные теории развития экономической безопасности (составлена автором на основе [1, 16])

Автор	Произведение, год	Основные идеи
Лист Ф.	«Национальная система политической экономии» (1841 г.)	Протекционизм как инструмент защиты национальной экономики от внешней конкуренции.
Кейнс Дж. М.	«Общая теория занятости, процента и денег» (1936 г.)	Государственное регулирование экономики для предотвращения кризисов и безработицы.
Сото Э.	«Иной путь: экономический ответ терроризму» (1986 г.)	Важность институциональных реформ для предотвращения кризисов и безработицы.
Абалкин Л. И.	«Экономическая безопасность России: угрозы и их отражение» (1994 г.)	Независимость, устойчивость и стабильность как ключевые принципы экономической безопасности.
Сенчагов В.К.	«Экономическая безопасность как основа обеспечения национальной безопасности России» (2005 г.)	Классификация внутренних и внешних угроз, влияющих на экономическую стабильность.
Сидоров В.А., Хуажева А.Ш.	«Экономическая безопасность в новой реальности» (2024 г.)	Исследование теоретических и практических аспектов обеспечения экономической безопасности в условиях цифровизации и перехода к углеродной нейтральности.

Развитие теории экономической безопасности проходит через циклы

экономического развития, где кризисы выступают катализаторами для совершенствования методологии. Эта теория интегрирует различные экономические и системные подходы, позволяя обеспечить комплексную защиту национальной экономики от внутренних и внешних угроз. В современных условиях теория экономической безопасности становится все более актуальной, поскольку она помогает адаптироваться к меняющимся глобальным вызовам и обеспечивать устойчивость экономики.

1.2 Ключевые элементы системы экономической безопасности организации

Система экономической безопасности предприятия – стратегии и меры, применяемые предприятием для защиты своего финансового благополучия от различных угроз. Она направлена на мониторинг и предотвращение мошеннических действий, выявление потенциальных угроз и недостатков, обеспечение соблюдения законодательных и нормативных требований [8].

На рисунке 1 представлен перечень элементов, которые входят в систему экономической безопасности предприятия.

Рисунок 1 – Элементы входящие в систему экономической безопасности предприятия (составлен автором на основе [15])

Ключевыми элементами системы экономической безопасности предприятия обычно являются:

– финансовые ресурсы,

– материальные активы,

– интеллектуальная собственность,

– конфиденциальная информация или данные,

– технологическая безопасность,

– сотрудники и заказчики или клиенты.

Основополагающим элементом является защита финансовых ресурсов, которая включает в себя: контроль денежных потоков и ликвидности, предотвращение хищений и мошенничества, управление финансовыми рисками и обеспечение финансовой устойчивости. Материальные активы подразумевают следующие меры по защите: охрана производственных помещений и складов, учет и контроль движения материальных ценностей, техническая защита оборудования и страхование материальных активов. Интеллектуальная собственность – патентование изобретений и разработок, защита авторских работ, сохранение коммерческих тайн и предотвращение промышленного шпионажа. Информационные активы требуют обеспечения кибербезопасности, защиты данных и электронных документов, контроля доступа к информации, резервное копирование и предотвращение утечек [18].

Технологическая безопасность занимает особое место в системе защиты предприятия, так как современные производственные процессы становятся все сложнее и уязвимее. Этот элемент включает в себя не только защиту технологических разработок, но и обеспечение бесперебойности производственных циклов, контроль качества выпускаемой продукции, а также защиту от саботажа и технологического шпионажа. Не менее важным элементом является работа с персоналом и клиентами. Персонал – это одновременно и важнейший ресурс компании, и потенциальный источник угроз, поэтому кадровая безопасность включает в себя тщательный отбор сотрудников, постоянный мониторинг их лояльности и укрепление корпоративной культуры внутри

организации. Защита клиентской базы подразумевает сохранение персональных данных, предотвращение утечки клиентов к конкурентам и выстраивание долгосрочных доверительных отношений [18].

В большинстве случаев в группу методов, к которым прибегают компании для обеспечения безопасности организации входит: страховые, экономические, организационно-правовые, инженерно-технические, инновационные и морально-психологические.

При анализе угроз экономической безопасности предприятия, ключевым признаком выступают источники их возникновения, которые подразумеваются на внутренние и внешние (таблица 2).

Таблица 2 – Факторы внешней и внутренней среды предприятия [6]

Факторы внешней среды	Факторы внутренней среды
1. Текущая политическая ситуация в стране	1. Действие или бездействие персонала предприятия
2. Экономические кризисы	2. Состояние персонала
3. Законодательство РФ	3. Подрыв делового имиджа и репутации в бизнес-сообществе
4. Противоправные действия криминальных структур	4. Производственные и технологические недостатки, нарушения технологии, их текущее состояние
5. Давление на хозяйствующие субъекты со стороны государственных органов	5. Конфликтные ситуации с конкурентами, контролирующими правоохранительными органами
6. Недобросовестная конкуренция	6. Существенные упущения в тактическом и стратегическом планировании, управленческой деятельности
7. Монополизация рынка	-
8. Чрезвычайные ситуации природного и технического характера	-

Также, стоит отметить, что риски и угрозы присущи не всем организациям, некоторые из них зависят от отрасли, специфики деятельности и организационно-правовой формы. Поэтому для каждого предприятия необходимо проводить индивидуальный анализ, в котором будут выделены ключевые элементы системы экономической безопасности и угрозы [2].

Эффективность системы экономической безопасности предприятия во многом зависит от ее комплексности и способности адаптироваться к изменяющимся условиям внешней среды. Важно понимать, что все элементы системы взаимосвязаны, и слабость в одной из сфер может поставить под угрозу безопасность всего предприятия.

1.3 Трансформация экономической безопасности в условиях цифровой экономики

Современный этап экономического развития характеризуется стремительным переходом к шестому технологическому укладу, основу которого составляют цифровые технологии, искусственный интеллект, Интернет вещей и распределительные реестры. Этот переход кардинально преобразует традиционные подходы к обеспечению экономической безопасности предприятия.

Данная трансформация приводит к нескольким фундаментальным изменениям в подходе к экономической безопасности. Во-первых, происходит смещение фокуса с защиты физических активов на обеспечение цифровых активов и данных, которые становятся ключевым ресурсом современной экономики. Во-вторых, значительно усложняется сама природа угроз – кибератаки приобретают трансграничный характер, а использование искусственного интеллекта злоумышленниками делает угрозы более изощренными и труднопредсказуемыми [8].

Особенностью нового технологического уклада является резкое ускорение бизнес-процессов, что требует перехода от традиционных систем безопасности, к решениям, способным работать в режиме реального времени. Современные системы экономической безопасности все чаще используют технологии предиктивной аналитики, позволяющие не только реагировать на уже возникшие угрозы, но и прогнозировать потенциальные риски.

Еще одной важной характеристикой является изменение масштаба угроз

– от локальных к глобальным. В условиях цифровой экономики предприятие может столкнуться с атакой из любой точки мира, а последствия таких инцидентов часто носят системный характер. Это требует принципиально новых подходов к построению систем защиты, включая создание распределенных центров мониторинга безопасности и развитие международного сотрудничества в области кибербезопасности [17].

При этом переход к новому технологическому укладу создает и новые инструменты для обеспечения экономической безопасности. Технологии блокчейна позволяют создавать защищенные системы учета и документооборота, искусственный интеллект помогает выявлять аномалии в финансовых потоках, а Интернет вещей обеспечивает контроль за материальными активами в режиме реального времени. Это открывает перед предприятиями новые возможности для построения комплексных систем защиты, сочетающих традиционные подходы с инновационными решениями [9].

Современная Россия демонстрирует противоречивую картинку технологического развития. Несмотря на отдельные прорывы в цифровых технологиях и IT-секторе, страна в значительной мере остается в рамках пятого технологического уклада. Это заметно по ключевой в современной экономике сфере – производстве микроэлектроники и микропроцессоров.

Микропроцессоры на данный момент являются ключевым двигателем цифровизации экономики, они стоят в компьютерах, станках, машинах, смартфонах и т.д. Без наличия собственного производства полупроводников можно забыть об идее достижения технологического суверенитета и экономической безопасности страны. Через микропроцессоры производятся акты технологического шпионажа благодаря «бэк дорам», которые позволяют получить дистанционный доступ ко всей информации, хранящейся на устройстве или вовсе взять над ним полный контроль. На данный момент в мире существует лишь две страны у которых есть полностью своя процессорная архитектура – Россия и США. Развитие микропроцессорной отрасли США идет с 1970 г., когда был представлен первый образец, СССР также активно развивало эту

отрасль и даже обогнало конкурента, но события 1991 г., привели к полному застою этой индустрии. На данный момент в России налажена разработка двух отечественных микропроцессоров это полностью российские Elbrus и работающие на иностранной архитектуре Baikal, но из-за отсутствия производственных мощностей на территории страны и огромного количества экономических санкций их использование не так широко распространено, касаясь только государственного сектора [3].

Таким образом в первой главе нами были проанализированы следующие вопросы: понятие экономической безопасности и основные этапы развития теории, ключевые составляющие системы экономической безопасности организации и как цифровизация повлияла на её трансформацию. Из этого можно сделать вывод, что после внедрения цифровой экономики процессы обеспечения экономической безопасности, а также угрозы и риски потерпели значительные изменения. Появилось множество способов как можно обезопасить предприятие, тоже самое касается угроз и рисков. Одним из главных принципов достижения экономической безопасности предприятия является технологический суверенитет страны.

2 Анализ системы ИБ ООО «БОМББАР» в условиях цифровой экономики

2.1 Характеристика ООО «БОМББАР»

Анализ системы информационной безопасности в условиях цифровой экономики будет проводиться на примере ООО «БОМББАР».

ООО «БОМББАР» – российских производитель полезной снэковой продукции без сахара, высокобелковых перекусов, завтраков, протеиновой выпечки, топпингов, соусов, низкокалорийного шоколада и спортивного питания.

Организация была зарегистрирована 01.03.2018 г., юридический адрес: 445007, Самарская область, г. Тольятти, Тупиковый проезд, влд. 26, офис 3. Уставной капитал составляет 30000 рублей (приложение А, рисунок А.1, приложение Б, рисунок Б.1). На данный момент организация находится в процессе реорганизации в форме присоединения к ней других юридических лиц. Среднесписочная численность сотрудников 2024 г. составила 293 человека.

Виды деятельности указанные в Уставе организации (приложение Б, рисунок Б.1, приложение В, рисунок В.1):

– деятельность агентов, специализирующихся на оптовой торговле фармацевтической продукцией, изделиями, применяемыми в медицинских целях, парфюмерными и косметическими товарами,

– торговля оптовая молочными продуктами,

– торговля оптовая соками, минеральной водой и прочими безалкогольными напитками,

– торговля оптовая хлебобулочными изделиями,

– торговля оптовая гомогенизированными пищевыми продуктами, детским и диетическим питанием,

– торговля оптовая мороженным и замороженными десертами,

– торговля оптовая фармацевтической продукцией,

– торговля оптовая прочими пищевыми продуктами.

На данный момент организация реализует оптовую и розничную продажу следующих продуктов: батончики, печенье, шоколад, напитки, пасты, смеси, соус и специи, спортивное питание, энергетические и тонизирующие напитки.

Продукция компании широко представлена на рынке под разными торговыми марками. На данный моменты в состав ООО «БОМББАР» входят следующие бренды: Bombbar, Chikalab, Snaq Fabriq.

Для оценки экономического положения ниже представлены общие показатели хозяйственной деятельности предприятия.

Таблица 3 – Общие показатели хозяйственной деятельности предприятия ООО «БОМББАР» за 2020–2024 года (составлена автором на основе [22])

Показатель	2020 г.	2022 г.	2024 г.	Изменение 2024 г. к 2020 г.	
				Абсолютное (+;-)	Относительное, %
Выручка, тыс. руб.	962 448	2 644 066	17 851 801	16 889 353	1 754,9%
Себестоимость тыс. руб.	657 060	1 866 797	14 492 161	13 835 101	2 106,3%
Чистая прибыль тыс. руб.	213 242	252 836	2 758	- 210 484	-98,7%
Среднесписочная численность, чел.	51	64	293	242	474,5%
Объем продукции, тонн	1 800	4 000	12 200	10 400	577,7%
Количество наименований продукции, шт.	80	150	270	190	237,5%
Выпущено батончиков, шт.	36 000 000	120 000 000	360 000 000	324 000 000	900%

За анализируемый период выручка предприятия увеличилась на 1 754,9% в относительном выражении, что свидетельствует об успешной реализации продукта на рынке и, вероятно, о расширении географии сбыта и дистрибьюторской сети. Одновременно с этим объем производства в натуральном выражении вырос с 1,8 тонн до 12,2 тонн, а количество выпускаемых батончиков увеличилось с 36 млн шт. до 324 млн шт. При этом ассортиментная линейка расширилась с 80 до 270 наименований продукции, что указывает на активную товарную политику компании.

С другой стороны, несмотря на впечатляющий рост выручки, себестоимость продукции увеличилась еще более стремительными темпами – с 657 тыс. руб. до 14,5 млрд руб. Это привело к снижению чистой прибыли на 98,7% по сравнению с 2020 г. Такой резкий спад можно объяснить колоссальными тратами в обновление основных средств компании, расширении торговых марок и маркетинговыми расходами.

2.2 Оценка текущего состояния цифровой безопасности ООО «БОМББАР»

В условиях цифровой экономики важной целью организации является обеспечение информационной безопасности. Во-первых, в условиях высокой конкуренции на рынке спортивного питания особую ценность представляют рецептуры продукции и технологии производства, что является коммерческой тайной компании. Утечка этих данных может привести к подрыву конкурентных позиций, серьезным финансовым потерям. Во-вторых, активное развитие онлайн-продаж предполагает обработку значительных объемов персональных данных клиентов, а значит строгого соблюдения законодательства. Автоматизированные системы управления производством и продажами, CRM-системы, платформы электронной коммерции – все эти элементы цифровой инфраструктуры компании являются потенциальными мишенями кибератак [13].

Компания «БОМББАР» активно внедряет цифровые технологии в ключевые бизнес-процессы – от производства до продаж, это позволяет повышать эффективность, снижать затраты и улучшать качество продукции.

Для автоматизации работы с клиентами была внедрена CRM система, для учета сырья и готовой продукции, автоматизации планирования закупок и контроля сроков годности внедрена ERP система. Датчики на оборудовании и системы автоматического взвешивания и фасовки помогают цифровизировать и сам процесс изготовления. Также, уже давно внедрены технологии ИИ и анализа Big Data для более точной аналитики поведения клиентов и оптимизации рекламных компаний.

На данный момент у компании «БОМББАР» было несколько упоминаний в СМИ из-за качества выпускаемой продукции и достоверности информации на упаковке.

В сентябре 2024 г. Роскачество провело исследование ряда энергетических напитков, включая продукцию Bombbar. В результате проверки были выявлены следующие нарушения:

– присутствие незаявленного в составе бензоата натрия,

– превышение допустимого уровня мезофильных аэробных микроорганизмов (КМАФАнМ),

– обнаружение дрожжей, которые также не были указаны в составе,

– в напитке не было обнаружено заявленных на упаковке витаминов С, В9 и В3.

Ранее подобной критике подвергались протеиновые батончики:

– по данным независимых экспертиз содержание сахара было в 4 раза больше, чем указано на упаковке,

– производитель не учитывал калорийность некоторых ингредиентов,

– количество пищевых волокон в батончиках оказалось в 4 раза ниже заявленных 20 г.

Помимо этого, были обвинения от потребителей в скрытии информации о составе эквивалента какао-масла, который включал пальмовое масло, что

вызвало дополнительные вопросы о прозрачности маркировки продукции компании.

Выявленные Роскачеством и независимыми экспертами нарушения в составе продукции указывают на системные проблемы в управлении данными, которые затрагивают как аппаратурную, так и программную составляющую информационной безопасности компании.

Несоответствие состава продукта маркировке может свидетельствовать о несанкционированном изменении рецептур на этапе производства. Среди возможных причин, может быть, отсутствие защищенных систем ввода данных на производственных линиях или недостаточный контроль доступа к оборудованию, где загружаются рецептуры.

Лабораторные анализы и сертификаты качества могут храниться в незащищенных локальных системах, например, в компьютерах без крипто шифрования, из-за чего появляется риск подмены результатов тестов. Если рецептуры и данные о составе продуктов хранятся только на одном сервере, их можно удалить или изменить без возможности восстановления.

Одной из причин может быть отсутствие ведения журнала изменений или подтверждения изменения данных в ERP или же PLM системах, что значительно упрощает возможность фальсификаций данных.

Отсутствие автоматической синхронизации лабораторных данных с системой маркировки может привести к ошибкам в указании состава продукта или намеренному скрытию информации.

Помимо всего вышесказанного у компании неоднократно были выявлены случаи разглашения коммерческой тайны бывшими сотрудниками, что свидетельствует о системных недостатках в работе с конфиденциальной информацией и неэффективности действующих соглашений о неразглашении (NDA) [24].

2.3 Анализ внутренних и внешних угроз цифровой безопасности ООО «БОМББАР»

ООО «БОМББАР» активно внедряет цифровые решения в ключевые бизнес-процессы: от производства до продаж. В компании используются современные решения для автоматизации и цифровизации – CRM-системы для работы с клиентами, ERP-системы для управления сырьем, производством и планированием закупок, а также технологии искусственного интеллекта и анализа Big Data для оптимизации маркетинговых компаний. Документооборот полностью переведен в электронный формат, а обратная связь с клиентами осуществляется через чат-боты.

Выделяют три основные категории внутренних угроз: несанкционированный доступ к информации, утечка данных и саботаж. Основными факторами являются недостаточная осведомленность сотрудников, слабая организация доступа к информации и отсутствие эффективного контроля. Для компаний вендоров главную угрозу предоставляют менеджеры отдела снабжения и рядовые сотрудники. Если классифицировать утечки по видам информации, то на лидирующих позициях стоит финансовая информация, техническая информация и информация о клиентах и сделках [5]. Это чаще всего связано с отсутствием знаний и компетенций у этих работников. Одними из ключевых рекомендаций являются – внедрение системы управления доступом, использование технологий мониторинга для снижения рисков и регулярное обучение сотрудников.

Помимо этого, отсутствие регулярного аудита информационной безопасности и тестирования на проникновение извне не позволяет своевременно выявлять слабые места в защите информационной системы компании.

Тем не менее, несмотря на высокий уровень цифровизации и недавнего обновления состава основных средств, в деятельности компании можно выделить существенные уязвимости в обеспечении цифровой безопасности (таблица 4).

Таблица 4 – Анализ угроз внешней и внутренней среды ООО «БОМББАР» (составлена автором на основе [4, 12, 25])

Угрозы внешней среды	Угрозы внутренней среды
Текущая политическая ситуация в стране: Ужесточение законодательства в области защиты информации (законы «О персональных данных» №152-ФЗ) увеличивает риски привлечения к ответственности за нарушения обработки данных.	Ошибки и халатность персонала: По данным Positive Technologies, 80% инцидентов в сфере информационной безопасности связаны с человеческим фактором. В ООО «БОМББАР» автоматизированы все этапы производства и продаж, ошибка оператора ERP-системы может привести к производству продукции с неправильным составом и последующими штрафами.
Экономические кризисы: Из-за накаленной геополитической обстановки и отсутствия отечественных решений в производственном процессе, компания может столкнуться с промышленным шпионажем или вовсе приостановить свою деятельность	Низкий уровень киберкомпетентности сотрудников: Опрос HeadHunter показывает, что только 27% сотрудников в РФ обучены информационной безопасности, что объясняет неоднократное разглашение коммерческой тайны.
Законодательство РФ: Несоблюдение требований о маркировке продукции (ФЗ №425-ФЗ) грозит штрафами от 100 тыс. до 300 тыс. рублей.	Подрыв делового имиджа: После выявленных Роскачеством нарушений и публикаций в СМИ, согласно данным Nielsen, 65% покупателей перестают покупать продукты данного бренда, что является одной их главных угроз предприятия.
Противоправные действия криминальных структур: В 2023 г. уровень киберпреступности в России увеличился на 15% по сравнению с предыдущим годом.	Недостатки в производственном контроле: Отсутствие автоматической сверки фактического состава продукции с данными на упаковке привело к выявлению Роскачеством ряда нарушений.
Недобросовестная конкуренция: В отрасли спортивного питания отмечено более 50 случаев информационных атак на бренды-конкуренты за последние два года.	Отсутствие надежного контроля изменений данных: По статистике ISACA, 35% случаев утечки данных вызваны отсутствием контроля за изменениями в системах. У ООО «БОМББАР» ярко выраженная проблема защиты данных об изменениях рецептур продуктов.

Таким образом, несмотря на активное внедрение цифровых технологий в бизнес-процессы ООО «БОМББАР», компания сталкивается с рядом угроз, как внешних, так и внутренних. Внешние и внутренний факторы, среди которых: ужесточение законодательства, экономические кризисы, угрозы криминальных структур, ошибки персонала, низкий уровень киберкомпетенции и недостаточный контроль за изменениями данных, значительно увеличивают риски для цифровой безопасности компании и требуют серьезного внимания. Системны проблемы в области производственного контроля и защиты данных о составе продукции могут привести к значительным финансовым и репутационным потерям, как это уже неоднократно происходило с нарушениями, выявленными Роскачеством.

2.4 Приоритетные направления улучшения информационной безопасности ООО «БОМББАР»

Для минимизации описанных рисков и повышения уровня информационной безопасности, ООО «БОМББАР» необходимо внедрить комплексные меры, направленные на улучшение защиты данных, минимизацию внутренних и внешних угроз, а также улучшение контроля за изменениями в бизнес-процессах. Рассмотрим конкретные шаги и решения, которые могут значительно улучшить безопасность предприятия.

Одной из важнейших мер является внедрение системы управления доступом (СУД), которая будет ограничивать доступ сотрудников к критически важной информации в зависимости от их ролей и обязанностей описанных в матрице доступа. Система будет следить за действиями каждого пользователя и фиксировать любые попытки несанкционированного доступа. Подразумевается, что ИС работает на основе отечественной ОС – Astra Linux, в которой есть встроенный модуль МРД, который обеспечивает разграничение ролей на уровне ядра, а FreeIPA является службой каталогов для централизованной аутентификации пользователей.

Для защиты информации от внешних угроз, таких как кибератаки или утечка данных, необходимо внедрение системы защиты информации (СЗИ), которые обеспечат шифрование данных, защиту от вирусных атак и мониторинг уязвимостей. Например, отечественное решение Solar Dozor с модулями защиты от НСД, утечек данных и корпоративного мошенничества, совместно с криптографическим решением «КриптоПРО CSP» 5.0.

Для предотвращения кибератак и заражения системы вредоносными программами следует внедрить системы антивирусной и антиконтентной защиты, которые помогут обнаруживать и устранять угрозы, связанные с внешними атаками, а также предотвратить утечку конфиденциальной информации через веб-браузеры. Для этих задач подойдет Kaspersky Endpoint Security 12.

Для защиты критических данных на уровне производства, такие как рецептуры и данные о составе продукции, следует внедрить систему автоматического защищенного учета (САЗ), которая обеспечит защиту данных от несанкционированных изменений, лучшим вариантов является отечественное решение 1С:ERP.

Для предотвращения утечек информации, особенно финансовой и технической, важно внедрить системы защиты от утечек данных (DLP). Они помогают отслеживать и блокировать попытки утечек конфиденциальной информации через каналы, такие как email, USB-устройства и внешний облачные сервисы.

Главным программно-аппаратным решением является система обнаружения вторжений (СОВ), которая соединяет информационную систему предприятия с внешней средой. Она анализирует сетевой трафик и события безопасности для выявления атак и подозрительных действий. Еще одно отечественное решение Solar NGFW, которое выполняет роль межсетевого экрана, файрвола и VPN.

В соответствии с Актом классификации информационной системы общества с ограниченной ответственность «БОМББАР», его ИС классифицирована по требованиям безопасности информации, как:

– частная информационная система третьего класса защищенности (К3) согласно приказу ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [14];

– информационная система четвёртого уровня защищенности персональных данных (УЗ 4) при их обработке в информационной системе согласно «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

Режим доступа каждой категории пользователей представлен в матрице доступа к информационным активам (таблица 5).

Таблица 5 – Матрица доступа к информационным активам

№ п/п	Информационный актив	Внутренние привилегированные пользователи	Временные пользователи	Внутренние непривилегированные пользователи
1	Аналитическая, клиентская, мультимедиа информация	Полный доступ	Нет доступа	Полный доступ
2	Доступ к серверной инфраструктуре	Полный доступ	Чтение	Нет доступа
3	Доступ к сетевому оборудованию	Полный доступ	Чтение	Нет доступа
4	Интерфейсы API	Полный доступ	Чтение	Нет доступа
5	Конфигурационные файлы	Полный доступ	Чтение	Нет доступа
6	Лицензии и сертификаты ПО и технических средств	Полный доступ	Чтение	Нет доступа
7	Лог-файлы и журналы событий	Полный доступ	Чтение	Нет доступа
8	Системная документация	Полный доступ	Чтение	Нет доступа

На рисунке 2 реализована архитектура пользовательского сегмента информационной системы общества с ограниченной ответственностью «БОМББАР» с учетом всех аппаратно-программных усовершенствований для обеспечения информационной безопасности.

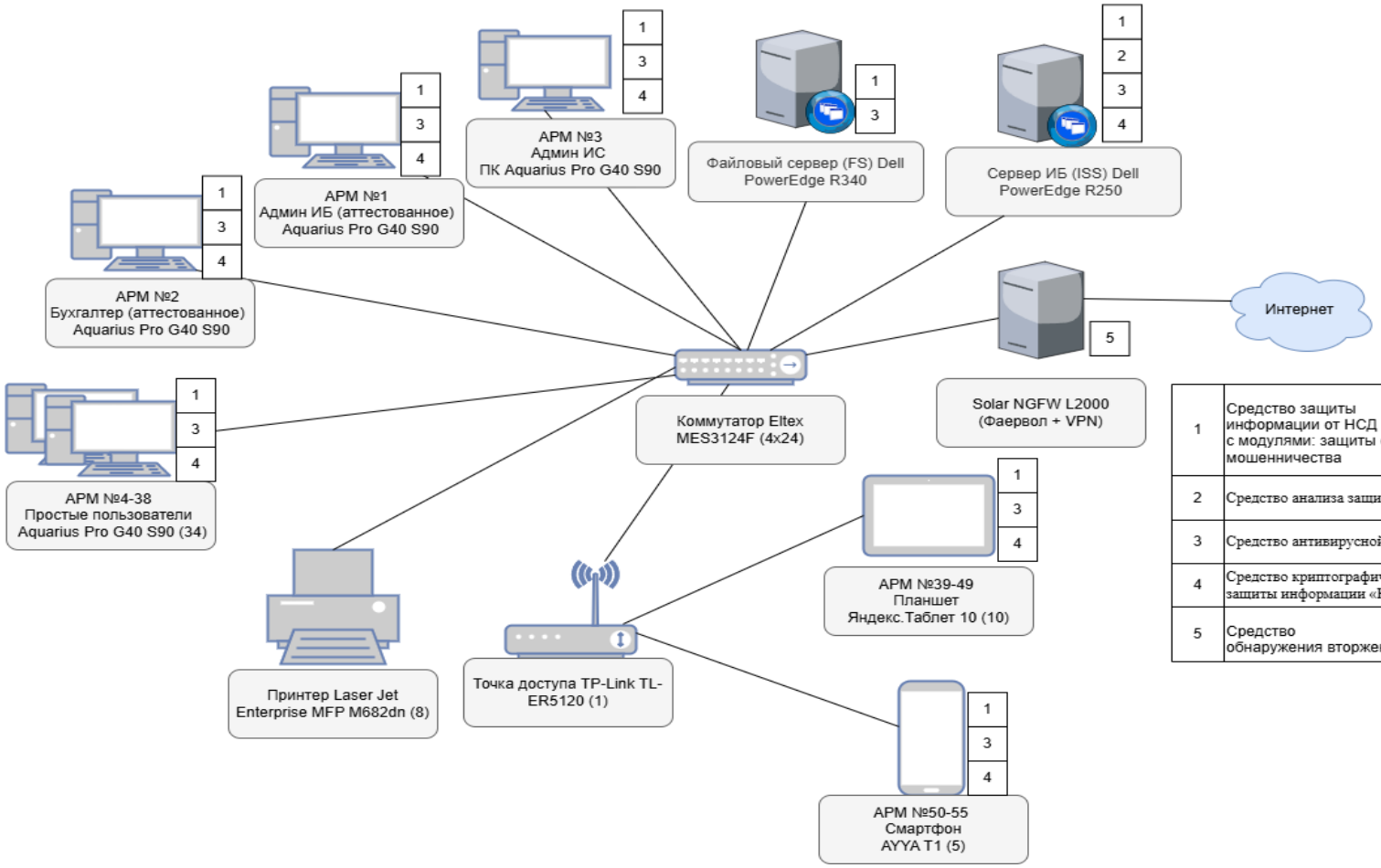


Рисунок 2 – Архитектура пользовательского сегмента информационной системы Общества с ограниченной ответственностью «БОМББАР»

Таким образом, во второй главе была проведена комплексная характеристика деятельности ООО «БОМББАР» в условиях цифровой экономики, а также дана оценка текущего состояния его информационной безопасности. В результате анализа внутренних и внешних угроз стало очевидно, что компания сталкивается с целым спектром рисков – от ошибок персонала и недостатков организационных процедур до внешних киберугроз и правового давления.

На основе выявленных проблем были предложены приоритетные направления для повышения уровня цифровой безопасности предприятия, включая внедрение современных систем защиты информации, управления доступом, организацию мониторинга инцидентов, а также повышение осведомленности и компетентности сотрудников.

ЗАКЛЮЧЕНИЕ

В заключение проведенного нами исследования можно сделать следующие выводы. В первой главе нами были рассмотрены теоретические аспекты экономической безопасности организации, которая предполагает защиту своих интересов и устойчивое развитие несмотря на внутренние и внешние угрозы. Активно теория экономической безопасности начала формироваться в 1930-х годах и активно развивалась в России с 1990-х годов. Её эволюция тесно связана с циклами экономических кризисов, которые обостряют необходимость защиты экономики.

Система экономической безопасности предприятия включает меры по защите финансовых ресурсов, материальных активов, интеллектуальной собственности, информации и технологий. Эффективная защита требует комплексного подхода, учета отраслевой специфики и постоянной адаптации к меняющимся условиям.

Переход к шестому технологическому укладу радикально изменил подходы к обеспечению экономической безопасности предприятий, сместив акцент на защиту цифровых активов и данных. Развитие технологий, таких как блокчейн и искусственный интеллект, открывает дополнительные возможности для повышения уровня безопасности.

Во второй главе была проведена комплексная характеристика деятельности ООО «БОМББАР» в условиях цифровой экономики, дана оценка текущего состояния его информационной безопасности, выявлены внешние и внутренние угрозы, и на их основе были предложены приоритетные направления для повышения уровня цифровой безопасности предприятия.

В условиях цифровой экономики обеспечение информационной безопасности стало для компании «БОМББАР» одной из ключевых задач. Активное внедрение цифровых технологий повысило эффективность бизнес-процессов, но также выявило уязвимости, связанные с управлением данными и защитой коммерческой тайны. Выявленные нарушения и утечки информации

указывают на необходимость усиления мер контроля доступа, защиты данных и повышения ответственности сотрудников.

Для повышения уровня информационной безопасности ООО «БОМБ-БАР» были предложены аппаратно-программные решения:

1 Внедрить межсетевой экран нового поколения с функциями VPN и защиты от вторжений – Solar NGFW.

2 Внедрить систему управления доступом на базе Astra Linux (МРД) и FreeIPA для контроля прав доступа и аутентификации пользователей.

3 Внедрить систему защиты информации Solar Dozor и криптографическое решение КриптоПРО CSP 5.0 для шифрования информации и защиты от утечек.

4 Внедрить DLP-систему для предотвращения утечек данных через email, USB и облачные сервисы.

Помимо этого была разработана матрица доступа к информационным активам, которая поможет разграничить права пользователей в зависимости от их статуса, что значительно повысить безопасность конфиденциальных данных, и упростит процесс нахождения «шпиона».

Этот комплекс мер поможет увеличить уровень информационной безопасности компании, понизит количество брака и производственных ошибок, защитит персональные данные как работников, так и клиентов предприятия.

Таким образом, проведенное исследование показало, что в современных условиях устойчивое развитие ООО «БОМББАР» невозможно без комплексного обеспечения экономической и информационной безопасности. Несмотря на активное внедрение цифровых технологий и рост деловой активности, компания сталкивается с серьезными внутренними и внешними угрозами, требующими оперативных и системных мер реагирования. Повышение уровня цифровой безопасности, оптимизация расходов и совершенствование контроля бизнес-процессов являются необходимыми условиями для укрепления конкурентных позиций компании на рынке.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Баранова, А. А. Актуальные тенденции развития теории экономической безопасности / А. А. Баранова // Экономическая безопасность. – 2024. – Т. 7, № 12. – С. 2975-2988. (дата обращения: 06.03.2025).

2 Букешев, Д. Б. Классификация угроз экономической безопасности предприятия / Д. Б. Букешев // ELS. – 2025. – № 28. (дата обращения: 20.03.2025).

3 Бутенко, Д. Е. Роль микропроцессоров в развитии цифровой экономики России / Д. Е. Бутенко, А. О. Осипян // Галактика науки–2024 : Материалы Всероссийской научно-практической конференции с международным участием, Краснодар, 24–27 апреля 2024 года. – Краснодар: Кубанский государственный университет, – 2024. – С. 116-121. – EDN OAFBYU. (дата обращения: 21.03.2025).

4 В каждой пятой российской компании сотрудники плохо знают основы ИБ. // rbc.ru : сайт. – 2024. – URL: https://companies.rbc.ru/ne-ws/54hkjYwi5m/v-kazhdoj-pyatoj-rossijskoj-it-kompanii-sotrudniki-ploho-znayut-osnovyi-ib/ (дата обращения: 21.04.2025).

5 Глухов, Н. И. Аналитика внутренних угроз информационной безопасности предприятий / Н. И. Глухов, П. Н. Наседкин // Доклады ТУСУР. – 2021. – №1. (дата обращения: 16.04.2025).

6 Горина, М. С. Оценка рисков и угроз экономической безопасности предприятия / М. С. Горина // ЕГИ. – 2024. – №3 (53). (дата обращения: 20.03.2025).

7 Государственная финансовая отчетность ООО «БОМББАР». // nalog.ru : сайт. – 2023. – URL: https://bo.nalog.ru/organizations-card/10566037 (дата обращения: 01.05.2025).

8 Докукина, А. А. Теоретические основы концепции экономической безопасности предприятия в контексте цифровой трансформации / А. А. Докукина // Экономика, предпринимательство и право. – 2023. – Т. 13, – № 4. – С. 1105-1124.

9 Еловская, М. А. Цифровая трансформация экономики: проблемы, перспективы и ее влияние на экономическую безопасность / М. А. Еловская // Известия СПбГЭУ. – 2024. – №4 (148).

10 Закон РФ «О безопасности» от 05.03.1992 №2446-1. // consultant.ru : сайт. – 2024. – URL: https://w-ww.consultant.ru/document/cons_doc_LAW_376/ (дата обращения: 06.03.2025).

11 Караева, И.В. Теория экономической безопасности суверенного государства в российской академической науке – к 300-летию РАН / И. В. Караваева // Экономическая безопасность. – 2024. – Т. 7, № 4. – С. 745-770.

12 МВД РФ // мвд.рф : сайт. – 2023. – URL: https://мвд.рф/reports/item/32109217/ (дата обращения: 21.04.2025).

13 Обиденко, А. В. Обоснование необходимости обеспечения информационной безопасности предприятия в эпоху цифровизации / А. В. Обиденко, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2021. – №. 7 (дата обращения: 08.04.2025).

14 Приказ ФСТЭК России от 11.02.2013 г. №17. // fstec.ru : сайт. – 2023. – URL: https://fstec.ru/d-okumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 04.05.2025).

15 Рыжкина, Я. А. Система экономической безопасности предприятия / Я. А. Рыжкина // Вестник науки. – 2023. – №4 (61). (дата обращения: 16.03.2025).

16 Сидоров, В. А. Экономическая безопасность в новой реальности / В. А. Сидоров, А. Ш. Хуажева // Краснодар : ФГБОУ ВО «Кубанский государственный университет», – 2024. – 189 С. – EDN HLECCO. (дата обращения: 06.03.2025).

17 Ся Сюйчэн Проблемы обеспечения экономической безопасности предприятия / Ся Сюйчэн // Экономика и социум. – 2023. – №5 (108). (дата обращения: 21.03.2025).

18 Терехина, Д. А. Методы обеспечения экономической безопасности предприятия /Д. А. Терехина, Т. В. Подольская // Вестник науки. – 2024. – №6 (75). (дата обращения: 16.03.2025).

19 Указ Президента РФ от 29.04.1996 №608 «О государственной стратегии экономической безопасности Российской Федерации. // kreml-in.ru : сайт. – 2024. – URL: http://www.kreml-in.ru/acts/bank/9261 (дата обращения: 6.03.2025).

20 Указ Президента РФ от 13.05.2017 №208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». // consultant.ru : сайт. – 2024. – URL: https://www.consultant.ru/document/cons_doc_LAW_2-16629/ (дата обращения: 06.03.2025).

21 Устав ООО «БОМББАР».

22 Чекмарев, В.В. Теория экономической безопасности: эволюционный аспект / В. В. Чекмарев // Экономическая безопасность. – 2020 – Т. 3, № 3. – С. 335-350.

23 Экономическая безопасность // banki.ru : сайт. – 2025. – URL: https://www.banki.ru/wiki-bank/ekonomicheskaya_bezopasnost/ (дата обращения: 05.03.2025).

24 Яриков, В. Г. Информационная безопасность и защита на предприятии / В. Г. Яриков, М. В. Пашков // NBI-technologies. – 2023. – №4. – (дата обращения: 08.04.2025).

25 82% утечек конфиденциальной информации происходит по ошибке сотрудников. // rbc.ru : сайт. – 2024. – URL: https://clck.ru/3MGVw3 (дата обращения: 22.04.2025).

ПРИЛОЖЕНИЕ А
Устав ООО «БОМББАР»


Учредительный документ юридического лица
ОГРН 1186313018264 в новой редакции
представлен при внесении в ЕГРЮЛ
записи от 27.09.2024 за ГРН 2246300753312

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

сведения о сертификате эп

Сертификат: 63EAE04B5E0B93ABADBF31937125EE7E
Владелец: МЕЖРЕГИОНАЛЬНАЯ ИНСПЕКЦИЯ
ФЕДЕРАЛЬНОЙ НАЛОГОВОЙ СЛУЖБЫ ПО
ЦЕНТРАЛИЗОВАННОЙ ОБРАБОТКЕ ДАННЫХ
МЕЖРЕГИОНАЛЬНАЯ ИНСПЕКЦИЯ ФЕДЕРАЛЬНОЙ
НАЛОГОВОЙ СЛУЖБЫ ПО ЦЕНТРАЛИЗОВАННОЙ
ОБРАБОТКЕ ДАННЫХ
Действителен: с 30.07.2024 по 24.04.2025

УТВЕРЖДЁН
Протоколом №1 от 30.08.2024г. совместного Общего собрания участников ООО «БОМББАР» и ООО «ОВЕРЛЕЙ»,.

УСТАВ

Общества с ограниченной ответственностью

«БОМББАР»

(новая редакция)

Самарская обл., г.о. Тольятти

2024 год

Рисунок А.1. – Устав ООО «БОМББАР», титульная страница [21]

ПРИЛОЖЕНИЕ Б
Устав ООО «БОМББАР»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общество с ограниченной ответственностью «БОМББАР», именуемое в дальнейшем «Общество», создано и осуществляет свою деятельность в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью» и иными нормативными актами действующего законодательства Российской Федерации.

1.2. Общество является юридическим лицом и осуществляет свою деятельность на основании настоящего Устава и действующего законодательства Российской Федерации.

1.3. Полное фирменное наименование Общества на русском языке:
Общество с ограниченной ответственностью «БОМББАР».

Сокращенное фирменное наименование на русском языке:
ООО «БОМББАР».

Полное наименование Общества на английском языке:
Limited Liabity Company "BOMBBAR"

Сокращенное фирменное наименование Общества на английском языке:
LLC «BOMBBAR».

1.4. Общество считается созданным как юридическое лицо с момента его государственной регистрации в установленном федеральными законами порядке.

1.5. Общество создается без ограничения срока.

1.6. Общество вправе в установленном порядке открывать банковские счета на территории Российской Федерации и за ее пределами.

1.7. Общество имеет печать, содержащую его полное наименование на русском языке, а также указание на его место нахождения.

Общество вправе иметь штампы и бланки со своим наименованием, собственную эмблему, а также зарегистрированный в установленном порядке товарный знак и другие средства индивидуализации.

1.8. Общество является собственником принадлежащего ему имущества и денежных средств и отвечает по своим обязательствам собственным имуществом.

1.9. Место нахождения Общества: Российская Федерация, Самарская область, г. Тольятти.

1.10. Общество имеет права, исполняет обязанности и несет ответственность в соответствии с действующим законодательством Российской Федерации.

2. ЦЕЛЬ, ПРЕДМЕТ, ВИДЫ ДЕЯТЕЛЬНОСТИ

2.1. Основной целью деятельности Общества является достижение максимальной экономической эффективности и прибыльности.

2.2. Для получения прибыли Общество вправе осуществлять любые виды деятельности, не запрещенные законодательством Российской Федерации, в том числе:

Деятельность агентов, специализирующихся на оптовой торговле фармацевтической продукцией, изделиями, применяемыми в медицинских целях, парфюмерными и косметическими товарами, включая мыло, и чистящими средствами;

Торговля оптовая молочными продуктами;

Торговля оптовая соками, минеральной водой и прочими безалкогольными напитками;

Торговля оптовая хлебобулочными изделиями;

Торговля оптовая гомогенизированными пищевыми продуктами, детским и диетическим питанием;

Торговля оптовая мороженым и замороженными десертами;

2

Рисунок Б.1. – Устав ООО «БОМББАР», общие положения и виды деятельности [21]

ПРИЛОЖЕНИЕ В
Устав ООО «БОМББАР»

Торговля оптовая текстильными изделиями;
Торговля оптовая парфюмерными и косметическими товарами;
Торговля оптовая фармацевтической продукцией;
Торговля оптовая прочими пищевыми продуктами.
Аренда и управление собственным или арендованным нежилым недвижимым имуществом.
Общество вправе осуществлять другие виды хозяйственной деятельности, не противоречащие законодательству Российской Федерации.

Все вышеперечисленные виды деятельности осуществляются в соответствии с действующим законодательством Российской Федерации. Отдельными видами деятельности, перечень которых определяется федеральными законами, Общество может заниматься только при получении специального разрешения (лицензии), членства в саморегулируемой организации или выданного саморегулируемой организацией свидетельства о допуске к определенному виду работ.

2.3. Общество для достижения целей своей деятельности вправе осуществлять любые гражданские права, предоставляемые законодательством Российской Федерации обществам с ограниченной ответственностью, от своего имени совершать любые допустимые законом сделки, быть истцом и ответчиком в суде.

2.4. Общество является собственником имущества, приобретенного в процессе его хозяйственной деятельности. Общество осуществляет владение, пользование и распоряжение находящимся в его собственности имуществом по своему усмотрению в соответствии с целями своей деятельности и назначением имущества.

2.5. Имущество Общества учитывается на его самостоятельном балансе.

2.6. Общество вправе иметь дочерние и зависимые общества с правами юридического лица.

2.7. Общество самостоятельно планирует свою производственно-хозяйственную деятельность, а также социальное развитие коллектива.

2.8. Общество несет ответственность за сохранность документов (управленческих, финансово-хозяйственных, по личному составу и др.); хранит и использует в установленном порядке документы по личному составу.

3. УСТАВНЫЙ КАПИТАЛ

3.1. Уставный капитал Общества составляется из номинальной стоимости доли его участника.

3.2. Размер уставного капитала Общества составляет 10 000 (Десять тысяч) рублей.

3.3. Уставный капитал Общества определяет минимальный размер его имущества, гарантирующего интересы его кредиторов.

3.4. Действительная стоимость доли участника Общества соответствует части стоимости чистых активов Общества, пропорциональной размеру его доли.

3.5. Оплата доли в уставном капитале Общества может осуществляться деньгами, ценными бумагами, другими вещами или имущественными правами либо иными имеющими денежную оценку правами.

3.6. К моменту регистрации Общества уставный капитал оплачен деньгами в размере 100%.

3.7. Увеличение уставного капитала Общества может осуществляться за счет имущества Общества, за счет дополнительных вкладов участника Общества.

3.8. Увеличение уставного капитала Общества за счет его имущества осуществляется по решению единственного участника Общества.

3.9. Общество вправе, а в случаях, предусмотренных Федеральным законом от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью», обязано уменьшить свой уставный капитал.

3.10. Уменьшение уставного капитала Общества может осуществляться путем уменьшения номинальной стоимости доли участника Общества в уставном капитале Общества.

3

Рисунок В.1 – Устав ООО «БОМББАР», виды деятельности и уставной капитал [21]

Отчет о проверке на заимствования №680728

Автор: Демонстрационный режим. Редактирование возможно в платном тарифе.
Проверяющий: Демонстрационный режим. Редактирование возможно в платном тарифе.

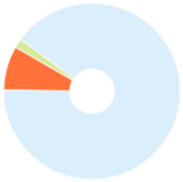
Организация: Демонстрационный режим. Редактирование возможно в платном тарифе.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 680728
Начало загрузки: 2025-05-25 16:49:53
Длительность загрузки: 00:00:16
Имя исходного файла:
2025_05_25_16_49_51_68334a2f1ac05.docx
Название работы:
2025_05_25_16_49_51_68334a2f1ac05.docx
Размер текста: 641670 байт
Символов в тексте: 47432
Слов в тексте: 5575
Число предложений:

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 2025-05-25 16:49:53
Длительность проверки: 00:01:06
Комментарии: не указано
Поиск с учетом редактирования: да
Модули поиска: ИПС Адилет, Библиография, Сводная коллекция ЭБС, Интернет Плюс, Сводная коллекция РГБ, Переводные заимствования (RuEn), Переводные заимствования по eLIBRARY.RU (EnRu), Переводные заимствования по Интернету (EnRu), Переводные заимствования издательства Wiley (RuEn), eLIBRARY.RU, СПС ГАРАНТ, Модуль поиска "КГАУ", Медицина, Диссертации НББ, Перефразирования по eLIBRARY.RU, Перефразирования по Интернету, Патенты СССР, РФ, СНГ, СМИ России и СНГ, Шаблонные фразы, Кольцо вузов, Издательство Wiley, Переводные заимствования, Коллекция НБУ, Перефразирования по коллекции издательства Wiley, Перефразирования по СПС ГАРАНТ: аналитика, СПС ГАРАНТ: аналитика, СПС ГАРАНТ: нормативно-правовая документация, Интернет



ЗАИМСТВОВАНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
8.1%	0%	1.66%	90.24%