

ИТ-технологии в обеспечении экономической безопасности хозяйствующих субъектов^{*}

IT-technologies in Ensuring Economic Security Business Entities

О. МАМАТЕЛАШВИЛИ, Д. РАФИКОВ

Мамателашвили Ольга Владимировна, д-р экон. наук, профессор кафедры экономического анализа и статистики ФГБОУ ВО «Уфимский государственный нефтяной технический университет» (УГНТУ).
E-mail: mar3169@yandex.ru

Рафиков Данил Талгатович, магистрант программы 38.04.01 «Экономическая безопасность» УГНТУ.
E-mail: pogonechik99@mail.ru

Актуальность темы обусловлена тем, что в условиях цифровизации экономики вопросы обеспечения экономической безопасности организаций приобретают особую значимость. Развитие информационных технологий создает как новые возможности для защиты экономических интересов организаций, так и новые угрозы, требующие комплексного решения. Существующие методы обеспечения экономической безопасности нуждаются в модернизации с учетом растущего влияния цифровых технологий. Необходимо исследовать эффективность применения ИТ-решений для защиты экономических интересов предприятий в условиях цифровой трансформации экономики. Целью исследования является анализ возможностей использования ИТ-технологий для повышения уровня экономической безопасности организаций. Анализ современных тенденций показывает, что внедрение ИТ-технологий позволяет существенно повысить эффективность систем экономической безопасности.

Ключевые слова: экономическая безопасность, информационные технологии, информационная безопасность, бизнес, технологии, искусственный интеллект, защита, блокчейн, машинное обучение.

The relevance of the topic is due to the fact that in the conditions of digitalization of the economy, the issues of ensuring economic security of organizations are becoming particularly important. The development of information technologies creates both new opportunities to protect the economic interests of organizations and new threats that require a comprehensive solution. The existing methods of ensuring economic security need to be modernized taking into account the growing influence of digital technologies. It is necessary to investigate the effectiveness of IT-solutions application to protect the economic interests of enterprises in the conditions of digital transformation of the economy. The purpose of the study is to analyze the possibilities of using IT technologies to improve the level of economic security of organizations. The analysis of current trends shows that the introduction of IT-technologies allows to significantly increase the efficiency of economic security systems.

Keywords: economic security, information technology, information security, business, technology, artificial intelligence, protection, blockchain, machine learning.

Введение

В современных условиях перманентных социально-экономических трансформаций вопросы обеспечения безопасности приобрели первостепенное значение для устойчивого развития российского социума и государственного аппарата. Особую актуальность приобретает проблематика кадровой безопасности, что подтверждается результатами многочисленных исследований в сфере различных аспектов безопасности [1].

Согласно данным глобального исследования, проведенного аудиторской компанией Ernst & Young, наиболее уязвимым звеном в системе информационной безопасности остается человек. Статистика показывает тревожную динамику: например, только за 2020 год количество

^{*} Ссылка на статью: Мамателашвили О.В., Рафиков Д.Т. ИТ-технологии в обеспечении экономической безопасности хозяйствующих субъектов // Экономика и управление: научно-практический журнал. 2025. № 4. С. 59–63. DOI: 10.34773/EU.2025.4.10.

преднамеренных утечек данных из коммерческих и государственных структур в России увеличилось на 60 %. При этом наблюдается рост случаев несанкционированного распространения корпоративной информации через фотографирование и создание скриншотов экранов, доля которых составляет 35 % от общего числа инцидентов. Примечательно, что сотрудники с высоким уровнем цифровой грамотности демонстрируют более ответственное отношение к защите данных, что существенно снижает вероятность компрометации информации.

Статистический анализ показывает, что около 80 % нарушений информационной безопасности совершается сотрудниками организаций, причем три четверти этих случаев носят умышленный характер и приходится на период пандемии. Высокий уровень выявления подобных инцидентов, особенно в банковской сфере и государственных органах, позволяет предположить, что реальная статистика может быть еще более значительной [1; 4].

Исследования научной литературы демонстрируют разнообразие подходов к оценке роли IT-технологий в обеспечении экономической безопасности. Академическое сообщество подчеркивает необходимость системного подхода, рассматривающего информационные технологии как неотъемлемый элемент стратегического риск-менеджмента. Эксперты в области кибербезопасности акцентируют внимание на комплексном подходе к защите информационных систем, включающем меры по предотвращению утечек данных и кибератак.

Практическая реализация показывает, что внедрение автоматизированных систем управления рисками, аналитических инструментов Big Data и облачных технологий существенно повышает оперативность реагирования на угрозы и минимизирует потенциальные потери. Синергетический эффект от сочетания традиционных методов управления с инновационными IT-решениями способствует формированию более устойчивой модели экономической безопасности предприятия [2].

Мировая практика подтверждает, что эффективность механизмов и развитость инфраструктуры, обеспечивающие экономическую устойчивость на государственном и корпоративном уровнях, являются ключевыми факторами формирования благоприятной экономической среды. Российская экономика, испытывая последствия глобального финансового кризиса конца 2000-х годов, демонстрирует уязвимость отдельных секторов и замедление темпов развития. В условиях необходимости принятия сложных экономических решений любая ошибка в сфере обеспечения экономической безопасности может иметь серьезные системные последствия.

Методы

Формирование информационного общества радикально трансформирует традиционные представления о механизмах обеспечения экономической безопасности. В этих условиях критически важным становится укрепление информационно-технологического потенциала как на государственном уровне, так и в рамках отдельных бизнес-структур. Внедрение и постоянное совершенствование современных цифровых решений должно стать стратегическим приоритетом развития любого предприятия.

Современные организации, стремящиеся к устойчивому положению на рынке, вынуждены не только реагировать на технологические изменения, но и активно участвовать в процессе цифровой трансформации. Использование передовых IT-решений, как показывает многочисленная практика, позволяет компаниям формировать конкурентные преимущества, определяющие их долгосрочную траекторию развития. К числу наиболее значимых технологий относятся [5]: интеллектуальная аналитика больших данных; облачные вычисления; искусственный интеллект; технологии интернета вещей; блокчейн-платформы; решения в области дополненной реальности; системы автоматизации производственных и управленческих процессов.

Внедрение данных технологий способствует оптимизации внутренних процессов, снижению операционных издержек и минимизации временных затрат, что приводит к повышению производительности труда, сокращению иерархических структур, снижению зависимости от человеческого фактора и повышению качества принимаемых решений.

При этом существующий теоретический фундамент в области анализа экономической

устойчивости характеризуется определенной ограниченностью, фокусируется преимущественно на финансовой составляющей, оставляя за рамками исследования такие важные аспекты, как технологическая безопасность, кадровый потенциал, информационная защищенность и институциональная зрелость.

В современных условиях ведения бизнеса критически важным становится не только обеспечение защиты текущих экономических интересов компании, но и разработка долгосрочных стратегий, направленных на устойчивое развитие. Интеграция в мировую экономику предъявляет к организациям повышенные требования, включая способность к адаптации в условиях высокой конкуренции, гибкое реагирование на внешние вызовы, минимизацию рисков, связанных с нестабильностью внешней среды, и эффективное управление неопределенностью и потенциальными конфликтами.

На сегодняшний день в академической среде наблюдается существенный пробел в исследовании практических аспектов обеспечения экономической безопасности бизнеса в контексте национальной модели развития. Особенно актуальной является проблема отсутствия комплексных методологий оценки устойчивости компаний в условиях жесткой конкуренции и глобальных вызовов современности. Особого внимания заслуживает вопрос цифровой безопасности бизнеса, который сегодня выступает одним из ключевых факторов не только корпоративного, но и общегосударственного экономического развития.

Под информационной безопасностью в широком смысле понимается комплексный подход к защите данных от несанкционированного доступа, использования, распространения, искажения, модификации, копирования, удаления или уничтожения. Это подразумевает реализацию целого спектра мер, направленных на обеспечение целостности, конфиденциальности и доступности информации. В условиях активной цифровизации защита информационных активов становится критически важной задачей для любого хозяйствующего субъекта.

Экономическая безопасность предприятия представляет собой многоаспектное понятие, включающее способность организации противостоять как внешним агрессивным воздействиям, так и внутренним дисбалансам, в том числе управленческие ошибки, структурные недостатки и кадровые проблемы. Основная цель экономической безопасности заключается в создании и поддержании такого состояния внутренней среды организации, которое обеспечивает устойчивость к различным рискам, сбоям и угрозам. Эффективно выстроенная система экономической безопасности не только минимизирует потенциальные угрозы, но и создает фундамент для долгосрочного развития предприятия.

Результаты

Ключевым аспектом обеспечения экономической безопасности является своевременное выявление и оценка различных типов угроз: экономических, технологических, информационных, социальных и правовых. Эти факторы могут носить как явный, так и скрытый характер, и при отсутствии адекватной реакции способны серьезно дестабилизировать функционирование организации. В современных условиях экономическая безопасность выступает не только как практическая сфера управления, но и как научная дисциплина, в рамках которой формируются системные знания о методах идентификации угроз и разработке эффективных механизмов их нейтрализации.

Информационные технологии приобретают все большую актуальность в повышении уровня защищенности и управляемости предприятий. Среди наиболее эффективных цифровых инструментов можно выделить: технологии больших данных (Big Data) и интеллектуальной аналитики, позволяющие проводить глубокий анализ массивов информации для выявления потенциальных угроз и выработки обоснованных управленческих решений; машинное обучение (Machine Learning), обеспечивающее построение прогнозных моделей и анализ поведенческих паттернов клиентов; искусственный интеллект (Artificial Intelligence), способный выполнять интеллектуальные задачи по анализу информации и автоматическому принятию решений; Интернет вещей (Internet of Things, IoT), обеспечивающий сбор данных в реальном времени

о различных параметрах производственных процессов; блокчейн-технологии (Blockchain), обеспечивающие защиту данных и повышение прозрачности финансовых операций.

Обсуждение

Применение этих технологий не только повышает уровень защищенности предприятия, но и создает стратегическое преимущество в условиях высокой конкуренции и цифровой трансформации. В совокупности они формируют современную платформу для развития концепции экономической безопасности, где защита информации, анализ данных и устойчивость бизнес-процессов тесно взаимосвязаны. Для эффективного обеспечения безопасности предприятия рекомендуется следовать алгоритму, включающему следующие шаги:

1) анализ потребностей и выявление проблемных зон, требующих решения с помощью IT-технологий;

2) определение конкретных задач, таких как управление рисками, противодействие финансовому мошенничеству или оптимизация финансовых процессов;

3) выбор подходящих IT-решений с учетом специфики деятельности, целей и задач организации;

4) внедрение выбранных технологий и их интеграция в существующую систему управления;

5) мониторинг эффективности внедренных решений и их корректировка при необходимости.

Одновременно с этим в процессе формирования комплексной системы экономической безопасности предприятия целесообразно придерживаться последовательного подхода, включающего несколько критически важных этапов:

1. **Профессиональная (пере)подготовка кадров**, которая выступает фундаментальным элементом внедрения IT-технологий в систему обеспечения экономической безопасности. Ключевым аспектом является не только освоение сотрудниками базовых программных продуктов, но и глубокое понимание принципов информационной безопасности. Программа обучения должна охватывать такие направления, как практическое освоение систем защиты информации; изучение современных методов криптографии; освоение техник безопасного управления паролями и их создания; практические занятия по работе с защитными программными комплексами.

2. **Многоуровневая защита информационных активов** требует комплексного подхода к обеспечению безопасности данных. В данном направлении необходимо внедрение надежных программных решений с подтвержденной защитой от внешних атак, применение современных криптографических методов для защиты информации, отбор облачных сервисов с учетом повышенных требований к безопасности, регулярное обновление защитных механизмов, а также внедрение многоуровневой системы контроля доступа к данным.

3. **Внедрение и использование специализированного программного обеспечения** должно осуществляться с учетом специфики бизнес-процессов предприятия. При выборе программных решений необходимо провести детальный анализ потребностей организации, оценить совместимость с существующими системами, проверить уровень защищенности программного обеспечения, убедиться в наличии необходимых функций для управления рисками, проверить возможности по борьбе с мошенничеством, оценить эффективность управления финансовыми потоками.

4. **Аудит информационной безопасности** является ключевым инструментом оценки защищенности предприятия. Данная методика позволяет выявить уязвимые места в системе управления информацией, провести комплексный анализ существующих рисков, оценить уровень защищенности от кибератак, определить эффективность внедренных защитных механизмов.

Заключение

Описанный комплексный подход позволяет создать надежную систему экономической безопасности, способную эффективно противостоять современным угрозам (мошенничество, взломы и атаки) и обеспечивать устойчивое развитие организации в условиях цифровой трансформации экономики.

Литература

1. Сапожникова С.М., Рейхерт Н.В. Экономическая безопасность: теоретические и практические подходы: монография. Чебоксары: ИД «Среда», 2021. 120 с.
2. Семчук И.А., Усков В.В. IT-технологии в экономической безопасности // Universum: экономика и юриспруденция. 2024. № 4-1(114). С. 5–9.
3. Сидоренко Г. Г., Сидоренко О.Г. Информационные технологии в сфере экономической безопасности // Вестник евразийской науки. 2024. Т. 16, № 6. [Электронный ресурс]. URL: <https://esj.today/PDF/63FAVN624.pdf>
4. Скворцов М.А. Применение IT-технологий для оценки экономической безопасности предприятия // Human Progress. 2023. Т. 9, № 2. С. 14. DOI: 10.34709/IM.192.14.
5. Харламов А.В., Арефьев М.А. Инфраструктурное обеспечение экономической безопасности хозяйственной деятельности // Экономика и управление. 2022. Т. 28, № 1. С. 33–41. DOI: 10.35854/1998-1627-2022-1-33-41.

DOI: [10.34773/EU.2025.4.11](https://doi.org/10.34773/EU.2025.4.11)

Анализ качества и конкурентоспособности продукции производственного предприятия*

Analyzing the Quality and Competitiveness of Products of a Manufacturing Enterprise

**Л. САЙФУТДИНОВА,
Г. НИГМАТУЛЛИНА, С. МИРОНОВ**

Сайфутдинова Лиана Рифовна, канд. экон. наук, доцент кафедры экономико-правового обеспечения безопасности Института истории и государственного управления ФГБОУ ВО Уфимский университет науки и технологий. E-mail: nigmatullina419@yandex.ru

Нигматуллина Гульнара Рашитовна, канд. экон. наук, заведующая кафедрой финансов, анализа и учетных технологий Башкирского государственного аграрного университета (БГАУ).

E-mail: nigmatullina419@yandex.ru

Миронов Сергей Владиславович, магистр кафедры финансов, анализа и учетных технологий БГАУ.

E-mail: nigmatullina419@yandex.ru

АО «Макфа» занимает доминирующие позиции в своей отрасли. Под этим брендом производится около 20 % всего объема макаронных изделий в РФ. Это подтверждается объемными показателями: ежегодно предприятия компании выпускают свыше 180 тыс. тонн макаронной продукции, около 450 тыс. тонн муки различных сортов и более 10 тыс. тонн круп и зерновых хлопьев. Такой масштаб производства делает компанию, которая обладает крупнейшим в России и Восточной Европе мукомольным комплексом, ведущим игроком рынка макарон и одним из лидеров на рынке муки.

Ключевые слова: прирост продаж, снижение себестоимости, факторы, анализ, методический аппарат, система качества.

“Makfa” holds a dominant position in its industry. The brand holds about 20 % of all pasta production in the Russian Federation. This is confirmed by volumetric indicators, annually the company's enterprises produce over 180 thousand tons of pasta products, about 450 thousand tons of flour of various grades and over 10 thousand tons of cereals and cereal flakes. This scale of production makes the company a major player in the pasta

* Ссылка на статью: Сайфутдинова Л.Р., Нигматуллина Г.Р., Миронов С.В. Анализ качества и конкурентоспособности продукции производственного предприятия // Экономика и управление: научно-практический журнал. 2025. № 4. С. 63–67. DOI: [10.34773/EU.2025.4.11](https://doi.org/10.34773/EU.2025.4.11).