

**Зуркова Ксения Олеговна**

студентка

*Научный руководитель*

**Маркарян Ирина Николаевна**

канд. экон. наук, доцент, доцент

Сочинский филиал ФГБОУ ВО «Всероссийский государственный  
университет юстиции (РПА Минюста России)»

г. Сочи, Краснодарский край

## **ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ**

***Аннотация:** в статье рассматривается роль цифровых технологий в системе экономической безопасности предприятий в условиях цифровой трансформации. Анализируются возможности цифровизации для повышения защищённости бизнеса, а также новые угрозы, возникающие при внедрении цифровых решений.*

***Ключевые слова:** цифровая трансформация, экономическая безопасность предприятия, цифровые технологии, кибербезопасность, цифровые риски, информационная безопасность.*

Современные процессы цифровизации экономики обусловлены быстрым развитием информационных технологий и коммуникаций. Цифровая трансформация экономики является приоритетным направлением развития России. Переход на новые технологические уклады даёт предприятиям конкурентные преимущества: ускорение бизнес-процессов, снижение транзакционных издержек, повышение прозрачности управления.

Актуальность статьи заключается в том, что в условиях нарастающей геополитической нестабильности, волатильности финансовых рынков и ужесточения санкционного давления, обеспечение экономической безопасности предприятия выходит за рамки классической защиты коммерческой тайны и переходит в плос-

кость стратегического управления устойчивостью, то есть способностью организации сохранять стабильность и эффективно развиваться за счёт грамотного распределения ресурсов, управления рисками и адаптации к изменениям. Цифровая трансформация бизнеса, с одной стороны, создает новые уязвимости, а с другой – предоставляет принципиально новые инструменты для прогнозирования рисков и оперативного реагирования. Актуальность исследования также обусловлена необходимостью пересмотра традиционных методик оценки экономической безопасности в пользу интеллектуальных систем, способных обрабатывать большие данные и выявлять скрытые угрозы на ранних стадиях их зарождения.

Цифровизация в контексте экономической безопасности представляет собой не просто автоматизацию учёта или переход на электронный документооборот, а комплексное изменение моделей управления, производственных цепочек и взаимодействия с контрагентами на основе информационных технологий, при котором безопасность становится встроенной функцией, а не надстройкой. Внедрение цифровых технологий ускоряет получение цифровых услуг, позволяет быстро находить нужную информацию по ценам, продуктам, услугам и поставщикам, выбирая наиболее интересные варианты без значительных усилий, но одновременно с этим возникают новые уязвимости, требующие пересмотра традиционных подходов к обеспечению экономической безопасности предприятий.

Цифровые технологии стали бесценным инструментом в области экономической безопасности предприятия по целому ряду причин. Они открывают возможность сбора, обработки и анализа огромных массивов данных, что позволяет предприятиям принимать обоснованные решения на основе точной информации. Применение алгоритмов машинного обучения и элементов искусственного интеллекта позволяет не только интерпретировать текущие показатели, но и прогнозировать макроэкономические и отраслевые тенденции, заблаговременно идентифицировать финансовые риски и оптимизировать внутренние бизнес-процессы с учётом выявленных закономерностей [1].

В условиях стремительного роста числа и сложности кибератак цифровые средства защиты становятся обязательным элементом корпоративной инфраструктуры: современные системы кибербезопасности обеспечивают многоуровневую защиту конфиденциальных сведений и финансовых данных, предотвращая несанкционированный доступ, утечки и разрушительные воздействия на критически важные информационные активы. Кроме того, Цифровизация существенно трансформирует финансовый блок деятельности предприятия, упрощая проведение онлайн-платежей, организацию электронной коммерции и автоматизацию бухгалтерского учёта, а внедрение таких инструментов, как электронные кошельки и криптовалюты, не только повышает скорость и удобство расчётов, но и усиливает контроль над транзакциями, снижая вероятность мошеннических операций и ошибок персонала [2].

Цифровые платформы позволяют автоматизировать управление рисками, контролировать финансовые потоки и анализировать потенциальные угрозы для предприятия. Это способствует улучшению уровня экономической безопасности и минимизации финансовых рисков.

Системы мониторинга и аудита на базе цифровых технологий позволяют в режиме реального времени осуществлять контроль над финансовыми операциями предприятия, проверять исполнение утвержденных бюджетов и осуществлять внутренний аудит, что помогает обнаруживать финансовые нарушения на самых ранних стадиях и предотвращать потери.

Однако цифровая трансформация порождает угрозы, которые отсутствовали в традиционной экономике. Среди них, например, внешние угрозы, такие как хакерские атаки, промышленный шпионаж, и внутренние, включающие ошибки сотрудников и злоупотребление доступом. Угрозы также могут быть техническими, связанными со сбоями оборудования, организационными, обусловленными недостаточной координацией служб, и кадровыми, возникающими из-за низкой цифровой грамотности персонала.

Особую опасность представляют комбинированные атаки, использующие одновременно технические уязвимости и социальную инженерию, а также зависимость от импортного программного обеспечения и оборудования, которая в условиях санкционных ограничений становится стратегическим риском для предприятия.

Среди ключевых проблем противодействия угрозам можно выделить отсутствие единых стандартов цифровой безопасности для разных отраслей, дефицит квалифицированных кадров в области кибербезопасности и экономической безопасности, низкую интеграцию между службой безопасности, ИТ-отделом и руководством предприятия, сложность оценки экономической эффективности мер защиты и быстрое изменение ландшафта угроз, опережающее развитие защитных решений [3]. Кроме того, большинство инцидентов в сфере информационной безопасности происходит по причине человеческих ошибок и недостаточной технологической компетентности персонала, что требует особого внимания к вопросам обучения и повышения квалификации кадров, а также формирования культуры цифровой гигиены среди всех сотрудников, а не только ИТ-специалистов.

Система обеспечения экономической безопасности предприятия в условиях цифровизации должна строиться на принципах комплексности, охватывающей все уровни управления и все виды активов, непрерывности, предполагающей постоянный мониторинг и анализ угроз, адаптивности, позволяющей системе перестраиваться при изменении внешней среды или внутренних условий и интеграции, означающей встраивание функций безопасности в бизнес-процессы [4]. В рамках цифровой трансформации предлагается создание и внедрение информационных технологий, устойчивых к киберугрозам, а также развитие механизмов обнаружения и предупреждения угроз с ликвидацией последствий их проявления, при этом особое значение имеет построение интегрированной системы сбора, передачи и анализа показателей деятельности предприятия, динамики внутренних и внешних угроз и ситуации на рынке по цифровым каналам с целью

использования данной информации для повышения уровня экономической безопасности.

Можно сделать вывод, что экономическая безопасность в условиях цифровизации экономики приобретает особое значение и в данной движение уже существующих активов должно соблюдаться с использованием цифровых носителей и каналами в их разных форматах. В связи с этим меняется сама суть производственных, а в дальнейшем и социально-экономических отношений. По этим причинам необходимы специалисты о области экономической безопасности, которые будут выявлять, а также предотвращать различного рода правонарушения. Цифровая трансформация системы безопасности не может быть сведена к установке отдельных программных продуктов – максимальная эффективность достигается при условии, что цифровизация охватывает все аспекты деятельности предприятия, а безопасность становится неотъемлемой частью корпоративной культуры и управленческих решений, интегрированной в общую структуру управления предприятием через выстраивание сквозных цифровых процессов сбора, передачи и анализа данных для оперативного принятия решений на всех уровнях.

### *Список литературы*

1. Дмитриев А.В. Внедрение инструментов цифровой безопасности в деятельность организаций / А.В. Дмитриев // Вестник АГТУ. – 2025. – С. 26–35.
2. Докукина А.А. Экономическая безопасность предприятий в фокусе задач управления в условиях цифровой трансформации / А.А. Докукина. – М.: РЭУ им. Г.В. Плеханова, 2024. – 159 с. EDN OBSKQH
3. Каснерик А.Ю. Экономическая безопасность организации в условиях цифровой трансформации / А.Ю. Каснерик, А.Д. Туфатулина // Бизнес-пульс: III Междунар. науч.-практ. студ. конф. – Минск, 2025. – С. 62–65.
4. Экономическая безопасность в эпоху цифровизации: вызовы, риски и стратегии устойчивого развития / И.С. Ферова, С.А. Козлова, Е.А. Осадченко, Н.Н. Подтихова. – М.: Русайнс, 2025. – 209 с. EDN FCYHNCN