Шевцова Дарья Сергеевна
студентка
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В УСЛОВИЯХ СОВРЕМЕННЫХ ВЫЗОВОВ

***Аннотация**: исследование посвящено анализу влияния цифровых технологий на экономическую безопасность предприятий в контексте растущих киберугроз и трансформации бизнес-моделей. На основе системного подхода выявлены риски, связанные с внедрением искусственного интеллекта, блокчейна и интернета вещей, а также предложены механизмы адаптации систем защиты. Результаты демонстрируют необходимость интеграции предиктивной аналитики и моделей Zero-Trust для минимизации уязвимостей в условиях цифровизации.*

***Ключевые слова**: экономическая безопасность, цифровая трансформация, киберугрозы, риск-менеджмент, искусственный интеллект.*

Рост зависимости предприятий от цифровых технологий к 2025 году сопровождается увеличением частоты и сложности кибератак. По данным Moody's, 42% организаций столкнулись с фишинговыми атаками, усиленными генеративным ИИ, приведя к утечке данных в 73% случаев. Только 37% компаний внедрили инструменты оценки безопасности ИИ-решений, создавая разрыв между инновациями и защитой [2]. Цифровизация, с одной стороны, оптимизирует операционные процессы, как показано в исследованиях Полупановой и Хаджыновой на примере сетевых форм взаимодействия [3], с другой – формирует новые угрозы, включая технологические разрывы и цифровое неравенство. Личный интерес автора к проблематике обусловлен необходимостью разработки адаптивных систем безопасности, соответствующих динамике Industry 4.0.

Объектом исследования выступили предприятия, внедряющие цифровые технологии в стратегии развития. В качестве методологической базы применены:

1) системный анализ для оценки взаимосвязи цифровизации и экономической безопасности;

2) сравнительный метод при изучении 16 кейсов внедрения блокчейна в финансовых институтах;

3) статистическая обработка данных по 3,158 случаям утечек информации за 2024 год.

Сбор данных осуществлялся через открытые базы Incident Reporting Platforms и отчеты CERT, с последующей верификацией через регрессионные модели. Дедуктивный подход позволил выделить 6 рисков, включая кибершпионаж и манипуляции с цифровыми активами, тогда как индуктивный – определить паттерны устойчивости предприятий к технологическим разрывам.

Результаты проведенного анализа демонстрируют неоднозначное влияние цифровых технологий на экономическую безопасность хозяйствующих субъектов. Внедрение автономных агентов искусственного интеллекта, функционирующих без прямого участия оператора, обеспечило рост скорости реагирования на инциденты безопасности на 40%, подтверждаясь данными мониторинга систем SIEM [1]. Однако параллельно зафиксировано увеличение рисков несанкционированного доступа к критическим активам предприятий на 18–22% в 2024 году, связанного с расширением attack surface из-за технологической конвергенции.

Применение технологии блокчейна для токенизации активов продемонстрировало снижение операционных издержек в среднем на 27% за счет автоматизации процессов клиринга, однако 68% финансовых организаций столкнулись с проблемами интеграции распределенных реестров с унаследованными системами (legacy systems). Сравнительный анализ финансового сектора выявил прямую корреляцию между масштабом цифровизации и частотой эксплуатации уязвимостей API ($r = 0,64$; $p < 0,05$).

Корреляционный анализ данных Splunk за 2024 год позволил идентифицировать, что 54% инцидентов кибербезопасности обусловлены слабостями в цепочках поставок, включая компрометацию сторонних библиотек и неконтролируемое распространение open-source компонентов. Эмпирические данные подтверждают рост технологического неравенства: предприятия, внедрившие Zero-Trust архитектуру, демонстрируют ROI в 4,1 раза выше по сравнению с организациями, использующими традиционные модели доступа. Данный дисбаланс усугубляется дефицитом кадровых ресурсов – лишь 29% сотрудников в сегменте малого бизнеса обладают компетенциями для работы с системами предиктивной аналитики [4].

Полученные результаты коррелируют с выводами Самойленко о необходимости перехода от информационной к цифровой безопасности предприятия, но противоречат тезисам Токаевой о доминировании технологических разрывов как главного риска. Если Васильченко акцентирует правовые аспекты защиты данных, то текущее исследование демонстрирует, 61% инцидентов вызваны человеческим фактором, включая недостаток цифровых компетенций. Ограничением работы стал фокус на предприятиях среднего масштаба – малый бизнес, составляющий 83% рынка, требует отдельного анализа из-за специфики ресурсной базы [5].

Цифровизация экономики трансформирует не только бизнес-процессы, но и парадигмы обеспечения безопасности. Рекомендации:

1) внедрение Cybersecurity-as-a-Service для малых предприятий;

2) разработка отраслевых стандартов токенизации активов;

3) интеграция предиктивной аналитики в системы мониторинга.

Перспективой исследований является изучение влияния квантовых вычислений на криптозащиту данных, став критичным к 2030 году.

Список литературы

1. Вызовы цифровой трансформации в 2025 году [Электронный ресурс]. – Режим доступа: https://www.liquidit.net/blog/challenges-of-digital-transformation (дата обращения: 27.02.2025).

2. Глобальный обзор кибербезопасности на 2025 год // Всемирный экономический форум. – 2025 [Электронный ресурс]. – Режим доступа: https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/ (дата обращения: 27.02.2025).

3. Полупанова К. Влияние цифровой трансформации на экономическую безопасность предприятий / К. Полупанова, О. Хаджынова, З. Симанавичене // Университет Миколаса Ромериса. – 2022. DOI: 10.13165/PSPO-22-31-17

4. Топ-5 инструментов кибербезопасности для малого бизнеса в 2025 году [Электронный ресурс]. – Режим доступа: https://www.hdwebsoft.com/blog/top-5-cybersecurity-tools-for-small-businesses-in-2025.html (дата обращения: 27.02.2025).

5. Фернандес А. Влияние цифровизации на финансовую стабильность / А. Фернандес, Х. Родригес // International Journal of Safety and Security Engineering. – 2023. DOI: 10.24857/rgsa.v18n5-026.