Чуприк Александр Александрович
студент
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ЦИФРОВИЗАЦИИ И ВНЕДРЕНИЯ НОВЫХ ТЕХНОЛОГИЙ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ

***Аннотация**: в современном локализованном мире, где информационные технологии стремительно развиваются, процессы цифровизации и внедрения новых технологий оказывают существенное влияние на различные аспекты включая экономическую безопасность, с пониманием того, что экономическая безопасность – это состояние защищённости национального экономического сектора от внутренних и внешних рисков, гарантирующее стабильное развитие.*

Цифровизация и внедрение новых технологий, таких как большие данные, искусственный интеллект, интернет вещей, блокчейн и облачные вычисления, открывают новые возможности для повышения эффективности производства, оптимизации логистических цепочек, развития электронной коммерции и появления инновационных бизнес-моделей. Однако вместе с этим возникают и новые риски, связанные с кибербезопасностью, зависимостью от технологических систем, защитой конфиденциальности данных и монополизацией рынков технологическими гигантами.

В этом контексте обеспечение экономической безопасности становится одной из ключевых задач для правительств, бизнеса и общества в целом. Необходимо найти баланс между использованием преимуществ цифровизации и внедрения новых технологий и минимизацией связанных с ними рисков, чтобы гарантировать устойчивое и безопасное развитие национальной экономики.

В статье рассмотрены основные положительные и отрицательные аспекты влияния цифровизации и внедрения новых технологий на экономическую безопасность, а также проанализированы возможные меры по обеспечению безопасности в цифровую эпоху.

***Ключевые слова**: цифровизация, новые технологии, экономическая безопасность, предприятия, влияние цифровизации, риски цифровизации преимущества цифровых технологий, кибербезопасность, информационная безопасность, защита данных, цифровая трансформация, инновации, конкурентоспособность, эффективность управление рисками, адаптация к изменениям, стратегия цифровизации, инвестиции в ИТ, обучение персонала, политика кибербезопасности.*

Внедрение цифровых технологий и процессов цифровизации открывает широкие возможности для повышения экономической безопасности, способствуя росту эффективности и конкурентоспособности национальной экономики. Рассмотрим основные положительные аспекты: Повышение эффективности производства и снижение издержек. Цифровые технологии, такие как автоматизация, роботизация и интернет вещей, позволяют оптимизировать производственные процессы, сократить затраты на рабочую силу и материалы, а также повысить качество продукции. Это способствует росту производительности и конкурентоспособности отечественных предприятий.

Улучшение логистики и управления цепочками поставок. Внедрение систем отслеживания и мониторинга, благодаря анализу крупных объемов информации позволяют оптимизировать логистические цепочки, уменьшить время доставки, снизить затраты на транспортировку и хранение, обеспечивая бесперебойное снабжение и повышая эффективность распределения ресурсов.

Развитие электронной коммерции и новых бизнес-моделей. Цифровые платформы и онлайн-торговля открывают новые рынки и возможности для предпринимательства, способствуя росту малого и среднего бизнеса. Появление инновационных бизнес-моделей, основанных на цифровых технологиях, стимулирует конкуренцию и диверсификацию экономики.

Повышение прозрачности и отслеживаемости финансовых операций. Технологии распределенного реестра, такие как блокчейн, обеспечивают надежное хранение и проверку данных о финансовых транзакциях, снижая риски мошенничества и коррупции. Это способствует укреплению доверия к финансовой системе и экономической безопасности страны.

Развитие цифровых государственных услуг. Внедрение электронного правительства и цифровых платформ для предоставления государственных услуг повышает их доступность, прозрачность и эффективность, сокращая бюрократические барьеры и издержки для граждан и бизнеса. Таким образом, цифровизация и внедрение новых технологий открывают значительные возможности для повышения эффективности и конкурентоспособности национальной экономики, способствуя укреплению экономической безопасности. Однако, наряду с положительными аспектами, существуют и потенциальные риски, требующие принятия соответствующих мер.

Несмотря на многочисленные преимущества цифровизации и внедрения новых технологий, они также создают ряд потенциальных рисков и угроз для экономической безопасности, которые необходимо учитывать и эффективно управлять.

Кибератаки и угрозы информационной безопасности. По мере роста цифровизации и зависимости от информационных систем, экономика становится более уязвимой для кибератак, хакерских взломов и утечек конфиденциальных данных. Это может привести к нарушению работы критически важной инфраструктуры, финансовым потерям, краже интеллектуальной собственности и другим серьезным последствиям для экономической безопасности.

Зависимость от технологических систем и возможные сбои. Высокая степень автоматизации и цифровизации производственных процессов, логистики и финансовых операций создает зависимость от бесперебойной работы технологических систем. Любые сбои или отказы в этих системах могут привести к значительным экономическим потерям и нарушению нормального функционирования экономики. Вопросы конфиденциальности и защиты данных. С ростом объемов

собираемых и обрабатываемых данных, включая личную информацию граждан и конфиденциальные корпоративные данные, возникают серьезные опасения по поводу конфиденциальности и защиты этих данных от несанкционированного доступа или злонамеренного использования.

Монополизация рынков технологическими гигантами. Концентрация рыночной власти в руках нескольких крупных технологических компаний может привести к ограничению конкуренции, завышению цен и зависимости от их продуктов и услуг, что негативно скажется на экономической безопасности.

Угрозы для рынка труда и занятости. Автоматизация и внедрение искусственного интеллекта могут привести к массовому сокращению рабочих мест в определенных секторах экономики, создавая социальную нестабильность и экономические проблемы.

Риски технологического отставания. Отставание в развитии и внедрении передовых технологий может снизить конкурентоспособность национальной экономики на мировом рынке, что может нанести ущерб экономической безопасности страны.

Для преодоления этих рисков и угроз необходимо принятие комплексных мер на государственном и корпоративном уровнях, включая инвестиции в кибербезопасность, совершенствование законодательства, развитие человеческого капитала и международное сотрудничество.

Детально рассмотрим меры по обеспечению экономической безопасности предприятия в цифровую эпоху:

Кибербезопасность: использование современных средств защиты периметра сети (межсетевые экраны нового поколения, системы предотвращения вторжений, сетевая антивирусная защита),развертывание систем защиты конечных точек и мобильных устройств (антивирусы, EDR, MDM решения),внедрение шифрования данных для защиты конфиденциальной информации в состоянии передачи и хранения, разворачивание SIEM-системы для централизованного сбора и анализа событий ИБ, создание центра мониторинга и реагирования на инциденты кибербезопасности (СОС), регулярное проведение тестов на

проникновение и оценок уязвимостей, разработка планов обеспечения непрерывности бизнеса и аварийного восстановления на случай кибератак.

Защита интеллектуальной собственности: внедрение систем управления правами интеллектуальной собственности (IPRM), регистрация торговых марок и знаков обслуживания, использование технических средств защиты авторских прав (DRM), мониторинг нарушений ИС в интернете и судебная защита, создание институтов лицензирования и трансферта технологий, управление жизненным циклом интеллектуальных активов предприятия.

Анализ больших данных: сбор данных из внутренних (ERP, CRM и др. системы) и внешних (социальные сети, датчики, государственные источники и пр.) источников, Data Mining и Text Mining для извлечения ценной бизнес-информации,машинное обучение для прогнозной аналитики и моделирования сценариев, интеграция ИИ для более глубокой аналитики, разработка дашбордов и инструментов визуализации для представления инсайтов руководству, обеспечение защиты и конфиденциальности больших данных.

Цифровая трансформация: внедрение технологий индустрии 4.0 (промышленный интернет вещей, роботизация, 3D печать), использование блокчейна для обеспечения прозрачности цепочки поставок и транзакций, разработка платформенных бизнес-моделей и экосистем, применение гибких методологий разработки программного обеспечения, развитие компетенций цифровой культуры у сотрудников, партнерства с технологическими компаниями и стартапами.

Управление рисками и комплаенс: соблюдение требований отраслевых регулирующих органов (FDA, SEC, GDPR и др.), система внутреннего контроля для обеспечения достоверности финансовой отчетности, разработка матриц рисков и контролей, использование технологий больших данных и визуализации для мониторинга рисков, создание комплаенс-функции во главе с комплаенс-офицером, оценка партнеров и контрагентов на предмет комплаенс-рисков.

Кадровая безопасность: развитие культуры информационной безопасности среди сотрудников, политики безопасности персонала (скрининг, проверки благонадежности, NDA), управление правами доступа к информационным

системам, обеспечение безопасности работы удаленных сотрудников, контроль использования служебных устройств и данных, обязательный инструктаж по информационной безопасности и конфиденциальности.

Важными факторами успеха являются руководство и поддержка мер безопасности на высшем уровне, соответствующие инвестиции, а также непрерывный мониторинг и совершенствование систем безопасности с учетом изменяющейся среды рисков.

Заключение: В эпоху цифровизации и стремительного технологического прогресса обеспечение экономической безопасности предприятия становится все более актуальной и сложной задачей. С одной стороны, цифровые технологии открывают новые возможности для роста, инноваций и повышения эффективности. С другой стороны, они несут новые риски и угрозы, связанные с кибербезопасностью, утечкой данных, нарушением прав интеллектуальной собственности и другими факторами [1, с. 122].

Поэтому крайне важно применять сбалансированный подход, максимизируя преимущества цифровизации, но при этом тщательно управляя рисками. Необходимо внедрять многоуровневые комплексные системы безопасности, охватывающие как технические, так и организационные и кадровые аспекты. Инвестиции в защиту данных, кибербезопасность, анализ рисков и управление ими должны рассматриваться не как расходы, а как критически важные вложения для обеспечения устойчивого роста бизнеса.

Перспективы развития в этой области включают внедрение передовых технологий (блокчейн, ИИ, квантовые вычисления) для повышения безопасности транзакций и данных, развитие культуры цифровой гигиены и кибербезопасности на всех уровнях, активное международное сотрудничество по вопросам кибербезопасности и защиты прав интеллектуальной собственности.

Безусловно, полностью исключить риски невозможно, но грамотно выстроенная стратегия информационной безопасности и управления рисками позволит предприятиям максимально реализовать потенциал цифровых технологий, оставаясь устойчивыми и конкурентоспособными в долгосрочной перспективе.

Список литературы

1. Моденов А.К. Особенности экономической безопасности в цифровой экономике / А.К. Моденов, М.П. Власов // Петербургский экономический журнал. – 2020. – №2. – С. 121–134. – DOI 10.24411/2307-5368-2020-10015. – EDN BPATYU.