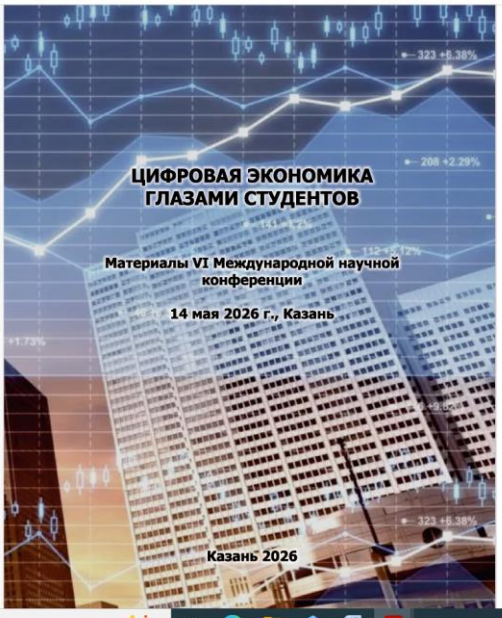


Цифровая экономика глазами студентов

Материалы VI Международной научной конференции

Казань, 14 мая 2026 г.

Под технической редакцией Г.Г. Мустафиной, Н.В. Кашиной

Электронное издание

Казань 2026

© Оформление.
Изд-во ИП Сагиев А.Р., 2026
ISBN 978-5-6055370-5-2

УДК 330.123
ББК 65.01
Ц75

Цифровая экономика глазами студентов: материалы VI Международной научной конференции. Казань, 14 мая 2026 г. /под технической редакцией Г.Г. Мустафиной, Н.В. Кашиной. – Казань: ИП Сагиев А.Р., 2026. – 1 электрон. опт. диск (CD-ROM). – ISBN 978-5-6055370-5-2. – Загл. с титул. экрана. – Текст: электронный.

Систем. требования: Intel от 1,3 ГГц; Windows XP/Vista/10; дисковод CD-ROM; Adobe Reader.

ISBN 978-5-6055370-5-2

Материалы **VI Международной научной конференции «Цифровая экономика глазами студентов»** освещают тренды развития промышленного сектора экономики в условиях цифровизации, особенности рынка информационных технологий, основы формирования цифровой безопасности, определяют подходы к формированию и развитию цифровой индустрии: моделей управления, маркетинга, экономики, управления персоналом, коммерциализации интеллектуальной собственности, а также цифровую трансформацию систем управления на предприятии и в организации.

Сборник адресован экономической общественности вузов, преподавателям вузов, специалистам по цифровой экономике, студентам, магистрам, аспирантам.

Статья приводится в авторской редакции. Мнение редакционной коллегии может не совпадать как с точкой зрения авторов на проблему, так и в отношении стилистики излагаемых материалов.

Редакционная коллегия:

Мустафина Г.Г., канд. экон. наук, доцент, и. о. заведующий кафедрой экономической теории и управления ресурсами (КНИТУ им. А.Н. Туполева-КАИ);

Кашина Н.В., канд. экон. наук, доцент кафедры экономической теории и управления ресурсами (КНИТУ им. А.Н. Туполева-КАИ);

ISBN 978-5-6055370-5-2

© Авторы, указанные в содержании, 2026
© Оформление.
Изд-во ИП Сагиев А.Р., 2026

Секция 1
Тренды развития промышленного сектора экономики в условиях цифровизации

Меню | Цифровая экономик... | Создать | Войти
Все инструменты | Редактировать | Преобразовать | Электронное подписание | Найти текст или инструмент

Чернушкина Е.А.
ИНДУСТРИЯ 4.0 И РОСТ ВВП: ОЦЕНКА МАКРОЭКОНОМИЧЕСКОГО ЭФФЕКТА ЦИФРОВИЗАЦИИ ПРОМЫШЛЕННОСТИ 284
Четит Д.О.
ЭКСПОРТНЫЙ ПОТЕНЦИАЛ ИННОВАЦИОННОЙ ПРОДУКЦИИ ФАРМАЦЕВТИЧЕСКОЙ ОТРАСЛИ РОССИИ: ОЦЕНКА В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И ВНЕШНИХ ОГРАНИЧЕНИЙ 288
Чистякова А.О.
УПРАВЛЕНИЕ ЗАТРАТАМИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ: ОТ СОКРАЩЕНИЯ К ПЕРЕСТРОЙКЕ 291
Шакуров Р.Д.
ПЕРЕХОД ОТ «АВТОМАТИЗАЦИИ» К «АВТОНОМНОСТИ»: ВНЕДРЕНИЕ АВТОНОМНЫХ РОБОТИЗИРОВАННЫХ СИСТЕМ (AGV/AMR) И ИНТЕЛЛЕКТУАЛЬНЫХ КОНВЕЙЕРОВ 293
Шаповалова А.К.
ИНВЕСТИЦИОННАЯ ПРИВЛЕКАТЕЛЬНОСТЬ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА КРАСНОДАРСКОГО КРАЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 294
Шкатова Р.Р.
ТРЕНДЫ РАЗВИТИЯ ПРОМЫШЛЕННОГО СЕКТОРА ЭКОНОМИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 296
Эгамурдиев А.-Х.М.
СЦЕНАРНОЕ ПЛАНИРОВАНИЕ КАК ИНСТРУМЕНТ СТРАТЕГИИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ 298
Юсупов Р.В.
АНАЛИЗ ВЕБ-ПРИЛОЖЕНИЙ ДЛЯ УЧЕТА И ПЛАНИРОВАНИЯ СЕМЕЙНЫХ РАСХОДОВ И ДОХОДОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ НА РОССИЙСКОМ РЫНКЕ 300

СЕКЦИЯ 5

РЫНОК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Абдулгазимова Р.Л., Девгиев С.М.
ИНВЕСТИЦИОННЫЙ ПОТЕНЦИАЛ НЕВЗАИМОЗАМЕНЯЕМЫХ ТОКЕНОВ В СОВРЕМЕННЫХ УСЛОВИЯХ 305
Автономова К.В.
ТЕНДЕНЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В БЮДЖЕТНОМ ПРОЦЕССЕ И ОЦЕНКЕ БЮДЖЕТНЫХ РИСКОВ 307
Алиабдиева Р.Н.
РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОПТИМИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ 311
Аминов Т.
КИБЕРСТРАХОВАНИЕ КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ РИСКАМИ 313
Анцыпалова П.П., Матвеева Ю.Е.
АНАЛИЗ УЯЗВИМОСТЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ И ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИХ ЗАЩИТЫ НА ПРИМЕРЕ КОММЕРЧЕСКОЙ КОМПАНИИ 315
Аминов Х.Г., Мокаллаева А.Д.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ СИСТЕМЫ 318
Аминуллаханова Д.
БРЕНД КАК ГАРАНТ НАДЕЖНОСТИ: КАК ЦИФРОВЫЕ ТЕХНОЛОГИИ ВЛИЯЮТ НА РЕПУТАЦИЮ КОМПАНИИ 321
Афанасьева А.А., Сигидинов А.В.
КАДРОВАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: УПРАВЛЕНИЕ ЧЕЛОВЕЧЕСКИМИ РИСКАМИ В ИТ-СФЕРЕ 324
Афанасьева А.А., Сигидинов А.В.
КАК ЦИФРОВАЯ БЕЗОПАСНОСТЬ ВЛИЯЕТ НА РАБОТУ С ПЕРСОНАЛОМ: РИСКИ И ПРОСТЫЕ РЕШЕНИЯ 326
Ахметзянов Р.Р.
ИНСТРУМЕНТЫ МОНИТОРИНГА МИКРОСЕРВИСНЫХ ПРИЛОЖЕНИЙ В KUBERNETES 327
Ахметзянов Р.Р.
СОВРЕМЕННЫЕ СРЕДСТВА УПРАВЛЕНИЯ НАГРУЗКОЙ МИКРОСЕРВИСНЫХ ПРИЛОЖЕНИЙ 329
Ахунова Д.З.
ВИЗУАЛИЗАЦИЯ КАРЬЕРНЫХ ТРАЕКТОРИЙ С ПОМОЩЬЮ ГРАФОВ: КАК ВЫБРАТЬ СВОЙ ПУТЬ В ИТ 331
Багаева А.Р., Полякарпа Н.С.
ВЛИЯНИЕ РОСТА КОМПЬЮТЕРНЫХ АТАК НА ПРАКТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОГО СЕКТОРА РОССИИ В 2021–2025 ГОДАХ 334
Бориченко А.О.
АЛГОРИТМ БРУСКАЛА В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ 337
Ботуева Д.А., Сидлов А.А.
АНАЛИЗ АРХИТЕКТУРНЫХ ПРИНЦИПОВ HADOOP (HDFS, MAPREDUCE, YARN) КАК ФУНДАМЕНТАЛЬНОЙ ПЛАТФОРМЫ ДЛЯ ПОСТРОЕНИЯ МАСШТАБИРУЕМЫХ СИСТЕМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ В КОММЕРЧЕСКИХ И ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЯХ 340

Бондаров Ш.Ф.
РЫНОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ЭКОНОМИКА, ПРОГРАММИРОВАНИЕ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ 343
Благодаров Э.А.
БУЛЕВЫ ФУНКЦИИ И КОМБИНАТОРНЫЕ МЕТОДЫ КАК ФУНДАМЕНТ СОВРЕМЕННОЙ КРИПТОГРАФИИ 346
Бойкова В.В.
КИБЕРБЕЗОПАСНОСТЬ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ 349
Бутенкова Е.Н.
РАЗВИТИЕ РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РОСТА КИБЕРУГРОЗ 353
Валиуллина А.Н.
АНАЛИЗ ЭКОНОМИЧЕСКИХ АСПЕКТОВ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КОМПЬЮТЕРНЫХ АТАК 355
Валиуллина А.Н.
ОЦЕНКА КОГНИТИВНОЙ НАГРУЗКИ И УСВОЕНИЯ МАТЕРИАЛА В УСЛОВИЯХ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ 357
Войнова К.А.
ЦИФРОВЫЕ ПЛАТФОРМЫ КАК ФАКТОР СТРУКТУРНЫХ ИЗМЕНЕНИЙ НА РЫНКЕ УСЛУГ 359
Волгина А.Д., Мирошников О.В., Шеро М.С.
АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СИСТЕМ В УСЛОВИЯХ ДИСТАНЦИОННОЙ РАБОТЫ 361
Воронов А.А.
РОСТ ЧИСЛА ФИШИНГОВЫХ АТАК КАК ФАКТОР РАЗВИТИЯ РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 364
Гайзутдинов М.М.
АНАЛИЗ ПОТРЕБНОСТИ В РАЗРАБОТКЕ ПРОГРАММНОГО КОМПЛЕКСА (СРЕДСТВА) В СФЕРЕ РОЗНИЧНОЙ ТОРГОВЛИ ДЛЯ ПРОГНОЗИРОВАНИЯ СПРОСА НА ТОВАРЫ И ОПТИМИЗАЦИИ ПРОЦЕССОВ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ 367
Гайзутдинов М.М., Волина М.Ф.
ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ТОЧНОСТИ НЕЙРОСЕТЕВЫХ АРХИТЕКТУР ДЛЯ ПРОГНОЗИРОВАНИЯ СПРОСА В РОЗНИЧНОЙ ТОРГОВЛЕ 371
Салахова Э.Е., Гарнова А.Р.
ЦИФРОВОЙ УТИЛИТ: НОВЫЕ ПРАВИЛА ОБЩЕНИЯ В РАБОЧИХ ЧАТАХ И ВИДЕО-ЗВОНКАХ 374
Гарипова А.Р.
ЭТИЧЕСКИЕ И ПРАВОВЫЕ РИСКИ ПРИМЕНЕНИЯ AI-ЧАТ-БОТОВ В КЛИЕНТСКОМ СЕРВИСЕ 376
Гатауллин А.А.
КИБЕРУГРОЗЫ И МЕТОДЫ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ 379
Гатина А.Р.
ТЕОРИЯ МНОЖЕСТВ КАК МОДЕЛЬ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ 380
Гучаров Т.М., Шарипзянов Э.Р., Сивостьянов Е.К.
ПРОБЛЕМЫ МОШЕННИЧЕСТВА В ЭЛЕКТРОННОЙ КОММЕРЦИИ: СТУДЕНТЫ И МАРКЕТПЛЕЙСЫ 383
Гучаров А.Н.
СРАВНЕНИЕ АЛГОРИТМОВ ПОСТРОЕНИЯ КРАТЧАЙШЕГО МАРШРУТА ДО ТОЧКИ ИНТЕРЕСА С МИНИМАЛЬНЫМ КОЛИЧЕСТВОМ ПЕРЕВОРОТОВ 385
Гурбольшева Б.Н.
ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ В ЦИФРОВЫХ БАНКОВСКИХ УСЛУГАХ 388
Давлетбаева А.Н.
АЛГОРИТМИЧЕСКОЕ РЕШЕНИЕ ЗАДАЧИ КОМБИНОЖЕКА В ЛОГИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ 391
Давлетбаева А.Н.
РОЛЬ БИОМЕТРИЧЕСКИХ ДАННЫХ В ОБЕСПЕЧЕНИИ ЦИФРОВОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ ПРИЛОЖЕНИЙ 393
Данг Д.А.
РАЗВИТИЕ РЫНКА СТРАХОВАНИЯ КИБЕРБЕЗОПАСНОСТИ ВО ВЬЕТНАМЕ: ТЕКУЩАЯ СИТУАЦИЯ, ПРОБЛЕМЫ И НАПРАВЛЕНИЯ РЕШЕНИЯ 395
Дауткул Д.Ф.
БУЛЕВЫ ФУНКЦИИ КАК ИНСТРУМЕНТ ПОСТРОЕНИЯ ПРЕДВАРИТЕЛЬНОГО ФИЛЬТРА В РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ 397
Демешкина С.О., Рыженкова А.А.
ПРОБЛЕМЫ РАЗРАБОТКИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ФИНАНСОВОЙ СФЕРЕ 399
Джуманов Р.
РАЗВИТИЕ ЦИФРОВОЙ ЭКОНОМИКИ ТУРКМЕНИСТАНА: НОВЫЕ УСЛУГИ В СОЦИАЛЬНОЙ СФЕРЕ 402

1804
1830
Поиск | РУС | 16:49 16.09.2026

Меню | Цифровая экономик... | Создать | Войти
Все инструменты | Редактировать | Преобразовать | Электронное подписание | Найти текст или инструмент

2. Проводить мониторинг инцидентов кибербезопасности отрасли. Оценивать уровень кибербезопасности Белорусской железной дороги. Обмениваться опытом обеспечения кибербезопасности с другими организациями Республики Беларусь.

3. Снизить зависимость Белорусской железной дороги от импортных информационных технологий и систем защиты информации. Устранять инвентаризацию их использования в системах, отказ или разрушение которых может причинить ущерб кибербезопасности.

4. Готовить кадры для Белорусской железной дороги, которые будут знакомы с принципами обеспечения кибербезопасности и понимающими необходимость и значимость данных мероприятий, а также повышать квалификацию сотрудников Белорусской железной дороги в данной сфере.

Таким образом, обеспечение кибербезопасности на железнодорожном транспорте, является одной из приоритетных задач государственной политики Республики Беларусь в условиях стремительной цифровизации экономики. XXI век, создает сложные вызовы, связанные с защитой критической информационной инфраструктуры от разрушающих воздействий.

Кибербезопасность на транспорте не ограничивается лишь защитой данных, а представляет собой комплексную систему, обеспечивающую безопасность движения поездов, сохранность персональных данных пользователей и устойчивость функционирования всех объектов транспортной инфраструктуры. Особенностью транспортной отрасли является необходимость сочетания двух взаимно связанных аспектов – информационной и функциональной безопасности, что наглядно иллюстрирует двухмерная модель кибербезопасности.

Актуальность проблемы подтверждается как мировыми тенденциями (рост числа целенаправленных компьютерных атак на критически важные объекты, включая транспорт), так и национальной статистикой, свидетельствующей о высоком уровне киберрисков для белорусских пользователей и организаций. В ответ на эти вызовы в Республике Беларусь была создана нормативно-правовая база (Указ Президента № 40), сформирована национальная система обеспечения кибербезопасности, а на Белорусской железной дороге – специализированный Центр кибербезопасности и реагирования на кибератаки. Создание и аттестация этого Центра стали важнейшим шагом, позволившим интегрировать отрасль в единую систему коллективной киберзащиты страны и повысить уровень осведомленности об актуальных угрозах.

Библиографический список

1. Шашкин, А. А. Основные направления обеспечения кибербезопасности на транспорте / А. А. Шашкин // Актуальные проблемы транспортной отрасли: сборник научных статей преподавателей, аспирантов и студентов [Электронный ресурс] // наш радиомай Л. Н. Логинова, В. И. Шаин: электронный журнал. – 2022. – Форма доступа: https://www.alibrary.ru/download/alibrary_30061956_27109598.pdf (дата обращения: 10.03.2026).
2. Даревская, В. Какие разновидности киберпреступлений существуют, и что такое буттфорс / В. Даревская [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. Форма доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-obluzh-prava/2021/october/66843/ (дата обращения: 10.03.2026).
3. Алдухов, С. Е. Информационная безопасность и защита информации на железнодорожном транспорте. [Текст] / С. Е. Алдухов, А. П. Глухов, А. А. Корниенко. – 2014. – 439 с.
4. Центр обмена информацией о компьютерной безопасности NIST: [Электронный ресурс] // Национальный институт стандартов и технологий. Форма доступа: http://csrc.nist.gov (дата обращения: 11.03.2026).
5. Малис, Э. Отчет: Страны готовятся к кибератаке [Электронный ресурс] // Э. Малис. Форма доступа: https://www.cnet.com/news/report-countries-preppingp-for-cyberwar/ (дата обращения: 11.03.2026).
6. Алдухов, С. Е. Международная кибербезопасность на железнодорожном транспорте: методологические подходы и современная методическая база [Электронный ресурс] / С. Е. Алдухов, С. В. Двоеносов, А. А. Корниенко, А.А. Скиба. // Вестник ВНИИЖТ: электронный журнал. – 2015. – № 6. – Форма доступа: https://www.alibrary.ru/download/alibrary_24871769_97649972.pdf (дата обращения: 11.03.2026).
7. Центр кибербезопасности и реагирования на киберинциденты создан на Белорусской железной дороге: [Электронный ресурс] / подготовил пресс-центр БЖД // Официальный сайт Белорусской железной дороги. Форма доступа: https://www.rw.by/corporate/pjsc_oasht/corporate_news/2026/01/tsentr-kiberbezopasnosti-i-reagirovaniya-na-kiberintsidenty-sozdan-na-belorusskoy-zheleznoy-doroge/ (дата обращения: 12.03.2026).
8. Центр кибербезопасности и реагирования на киберинциденты создан на Белорусской железной дороге [Электронный ресурс] // Информационный портал Федерации профсоюзов Беларуси. Форма доступа: https://belprofkurs.by/news/vesti-kibezbezopasnosti-i-reagirovaniya-na-kiberincidenty-sozdan-na-belorusskoy-zheleznoy-doroge/ (дата обращения: 28.03.2026).
9. О кибербезопасности: Указ Президента Республики Беларусь, 14 февр. 2023 г., № 40 // Президент Республики Беларусь. [Электронный ресурс] // Официальный интернет-портал. Форма доступа: https://president.gov.by/ftp/v1/508/document-thumb__45508__original/45508.1676445432.32ffbd2142.pdf (дата обращения: 28.03.2026).

РАЗВИТИЕ РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РОСТА КИБЕРУГРОЗ

Бутенкова Е.Н.
Научный руководитель: Аманатова Н.В.
ФГБОУ ВО Орловского ГАУ

Аннотация. В статье рассматривается современное состояние и перспективы развития рынка информационной безопасности в России в условиях роста киберугроз и усиления процессов цифровизации. Актуальность исследования обусловлена необходимостью обеспечения технологического суверенитета и определенной устойчивости бизнеса и государства. На основе анализа статистических данных, отраслевых отчетов и примеров кибератак 2024–2025 гг. автором выделены ключевые тенденции импортозамещения в сегменте средств защиты информации, рост спроса на централизованные системы мониторинга (SOC), внедрение многофакторной аутентификации, а также увеличение доли российских вендоров. Особое внимание уделено прогнозным показателям объема рынка, который, согласно представленным оценкам, к 2030 году может достичь 968 млрд руб. В заключение обосновывается вывод о формировании нового подхода к защите данных, основанного на платформенных решениях, интеграции технологий искусственного интеллекта и повышении киберустойчивости.

Ключевые слова: рынок информационной безопасности, рост киберугроз, цифровая безопасность, цифровизация бизнеса, информационные технологии, импортозамещение, цифровая экономика, кибербезопасность, технологический суверенитет.

DEVELOPMENT OF THE INFORMATION SECURITY MARKET IN THE CONTEXT OF GROWING CYBER THREATS

Bukhtoyarova E.I.
Scientific supervisor: Almatyeva N.V.
Oral State Agrarian University

Annotation. The article examines the current state and prospects for the development of the information security market in Russia in the context of growing cyber threats and increasing digitalization processes. The relevance of the research is determined by the need to ensure the technological sovereignty and operational sustainability of business and the state. Based on the analysis of statistical data, industry reports and examples of cyber attacks in 2024-2025. The author identifies key trends: import substitution in the information security segment, an increase in demand for centralized monitoring systems (SOC), the introduction of multifactor authentication, as well as an increase in the share of Russian vendors. Special attention is paid to the forecast indicators of the market volume, which, according to the presented estimates, may reach 968 billion rubles by 2030. In conclusion, the author substantiates the conclusion about the formation of a new approach to data protection based on platform solutions, the integration of artificial intelligence technologies and the strengthening of cyber literacy.

Keywords: information security market, growth of cyber threats, digital security, digitalization of business, information technology, import substitution, digital economy, cybersecurity, technological sovereignty.

Рынок информационной безопасности играет для цифровой экономики России. В условиях роста киберугроз, развития технологий и ужесточения требований к защите данных и бизнес, и государственные учреждения вынуждены адаптироваться к новым условиям и инвестировать в современные продукты [5]. В настоящее время темп повышения уровня цифровой безопасности является одним из ключевых вопросов стратегического управления как в России, так и во всем мире. Сегодня рынок кибербезопасности рассматривается как основополагающий фактор операционной устойчивости, финансовой стабильности. Он переживает стремительную трансформацию, обусловленную рядом ключевых факторов: интенсивной цифровизацией, усилением киберугроз, повсеместной технологической автономностью, повышением штрафов за утечки данных.

Период 2024–2025 гг. характеризуется ростом кибератак все более деструктивного характера. Десятого марта 2024 года количество этих из российских компаний выросло чем на 20% [1]. Злоумышленники все чаще действуют с целью получения финансовой выгоды [3]. В то же время организации укрепляют свою защиту. К основным рискам относятся атаки с использованием программ-вымогателей. «Российский бизнес больше не ограничивается антивирусным программным и базовыми мерами защиты. Среди наиболее востребованных практик – внедрение многофакторной аутентификации для всех сотрудников и подрядчиков, регулярные проверки информационной безопасности.

Более 60% атак начинается с фишинга, поэтому организации усиливают программы повышения киберграмотности [2].

Прогноз по российскому рынку кибербезопасности представлен во рисунке 1.

Мировой рынок кибербезопасности в 2024 г. достиг объема в 203,78 млрд долларов. За два года, с 2022 по 2024 гг., доля информационной безопасности в структуре российского сектора информационных технологий выросла и достигла 13-14%.

В 2024 году объем российского рынка кибербезопасности достиг 314 миллиардов рублей. Это означает, что общий объем рынка, включающий продукты и услуги, вырос на 26,3% по сравнению с показателями 2023 года, когда он составлял 248,5 миллиардов рублей [4]. Продолжались тенденция к уменьшению присутствия иностранных поставщиков, в то время как позиции отечественных компаний на рынке укрепились.

354
1830
Поиск | РУС | 16:50 16.09.2026

Меню | Цифровая экономик... | Создать | Войти
Все инструменты | Редактировать | Преобразовать | Электронное подписание | Найти текст или инструмент

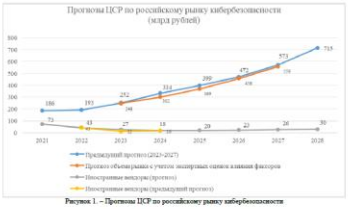


Рисунок 1. – Прогнозы ЦСР по российскому рынку кибербезопасности

По данным за 2024 год, доля иностранных решений в общих ИТ-закупках составила 7%. Замедление процессов импортозамещения связано с тем, что некоторые зарубежные вендоры (например, израильская Check Point) сохранили официальное присутствие на российском рынке, а также с постепенным по параллельному импорту тех продуктов, которые пока невозможно оперативно и полноценно заменить отечественными аналогами.

Летом 2025 года произошли две показательные кибератаки. Крупнейший авиаперевозчик «Аэрофлот» столкнулся с хакерской атакой, вызвавшей сбой ИТ-систем и отмену десятков рейсов. Почти одновременно сеть розничных магазинов «ВкусВсё» (входит в Novabev Group) подверглась атаке, которая временно нарушила работу части IT-инфраструктуры, парализовав точки продаж и онлайн-сервисы. В компании назвали инцидент «беспрецедентным». Оба случая демонстрируют, что современные кибератаки наносимы не разрушительные для бизнеса последствия: остановку процессов, потерю доверия и репутационный ущерб.

На основе оценок объёма рынка и влияния ключевых факторов был составлен прогноз его развития на период 2025–2030 годов. Прогноз развития рынка информационной безопасности до 2030 г. представим на рисунке 2.



Рисунок 2. – Прогноз развития рынка информационной безопасности до 2030 г.

К 2030 году рынок может достичь 968 млрд рублей. До 2030 года в России он сохранит положительную динамику, опираясь на внутренний спрос и государственную политику технологического суверенитета [1].

Подводя итог вышеизложенному, можно сказать, что информационная безопасность важна для улучшения и стабильности цифровой экономики. Развитие искусственных и платформенных решений, увеличение спроса на технологии и продукты информационной безопасности, расширение их интеграции в бизнес-процессы, использование ИИ в кибербезопасности и т.д., - эти факторы способны формировать новый подход к защите данных и интернет-сервисов.

Библиографический список:

1. Кибербезопасность и сохранение цифрового суверенитета экономики / У. Е. Пакина, М. А. Цукашина, М. М. Хаванов [и др.] // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2025. – № 211. – С. 374-387. – DOI 10.21515/1990-4665-211-030. – EDN DZTCFW.
2. Сокиев, И. С. Информационная безопасность в условиях цифровизации экономики: угрозы и меры защиты / И. С. Сокиев // Университетская наука - региону : Сборник материалов XI (68) ежегодной научно-практической конференции преподавателей, студентов и молодых ученых Северо-Кавказского федерального университета, Ставрополь, 01 апреля 2024 года. – Ставрополь: Северо-Кавказский федеральный университет, 2024. – С. 479-482. – EDN JPKCLK.
3. Сарычева, А. А. Проблемы информационной безопасности населения, или Как противостоять кибермошенникам / А. А. Сарычева // Молодежь. Наука. Будущее : СБОРНИК СТАТЕЙ В двух томах, Оренбург, 22–23 мая 2024 года. – Оренбург: Оренбургский государственный педагогический университет, 2024. – С. 164-166. – EDN ZFSMMX.
4. Центр стратегических разработок. Аналитический отчет «Рынок кибербезопасности России: итоги 2024 года и прогноз до 2030 года». – М., 2025. – 45 с.
5. Яковлева, Е. В. Кибертерроризм в XXI веке и обеспечение информационной безопасности: вызовы, тренды и стратегии защиты / Е. В. Яковлева // Актуальные вопросы обеспечения комплексной безопасности : материалы национальной научно-практической конференции с международным участием, посвященной 55-летию МЧС России и 85-летию Оренбургского ГАУ, Оренбург, 23 мая 2025 года. – Оренбург: Оренбургский государственный аграрный университет, 2025. – С. 647-650. – EDN NYKBHC.

АНАЛИЗ ЭКОНОМИЧЕСКИХ АСПЕКТОВ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Ветошкин А.И.
Научный руководитель: Юнусов И.А.
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, г. Казань, Россия

Аннотация. Данная статья посвящена изучению экономических факторов, влияющих на внедрение систем искусственного интеллекта (ИИ) в сферу защиты информации компаний. Используется, трансформация затрат на кибербезопасности при переходе от традиционных методов обнаружения угроз к алгоритмам машинного обучения. В статье анализируются первоначальные и текущие расходы, предлагается методика расчета совокупности стоимости владения (TCO) для ИСПС на базе искусственного интеллекта.

Ключевые слова: искусственный интеллект, кибербезопасность, экономическая эффективность, системы обнаружения атак, управление рисками.

ANALYSIS OF THE ECONOMIC ASPECTS OF USING ARTIFICIAL INTELLIGENCE IN COMPUTER ATTACK DETECTION AND PREVENTION SYSTEMS

Vetoshkin A.I.
Scientific supervisor: Yunusov I.A.
Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russia

Annotation. This article is devoted to the study of economic factors influencing the introduction of artificial intelligence (AI) systems in the field of information security of companies. The transformation of cybersecurity costs during the transition from traditional threat detection methods to machine learning algorithms is being investigated. The article analyzes the initial and current expenses, and suggests a methodology for calculating the total cost of ownership (TCO) for artificial intelligence-based IDS.

Keywords: artificial intelligence, cybersecurity, economic efficiency, attack detection systems, risk management.

В условиях стремительной цифровизации экономики, кибератаки становятся всё более масштабными. Крупные компании несут колоссальные убытки от инцидентов безопасности, которые часто могут оставаться экономическими мелочами. Стандартные системы защиты теряют свою эффективность против современных атак, что делает необходимым переход к интеллектуальным системам. Однако финансовое доказательство использования таких передовых решений остается проблемой для бизнеса из-за высоких начальных затрат, неопределенности оценки предотвращенного ущерба и отсутствия чётких методик расчёта окупаемости.

Меню | Цифровая экономик... | Создать | Войти
Все инструменты | Редактировать | Преобразовать | Электронное подписание | Найти текст или инструмент

В условиях управления предприятием часто возникает ситуация, когда отдельные критерии противоречат друг другу. Например, ускорение внедрения системы управления может повысить риск ошибок интеграции, а снижение затрат — уменьшить желаемый эффект. В этом случае полезно использовать Парето-оптимальный подход: стратегия считается рациональной, если нельзя улучшить один показатель без ухудшения хотя бы одного другого. После выделения множества Парето-эффективных альтернатив уже можно применять функцию полезности для окончательного выбора [2].

Практический смысл предлагаемой модели состоит в том, что она дает руководству инструмент обоснованного выбора между несколькими цифровыми проектами. Например, при ограниченном бюджете предпочтение может быть отдано автоматизации документооборота, поскольку она быстро сокращает административные издержки. При наличии стратегической цели цифровой интеграции может быть выбран проект внедрения единой ERP-системы, который обеспечивает более высокий интегральный эффект, но требует больших ресурсов и времени [3].

Дополнительным направлением развития предложенного подхода является интеграция методов математического анализа с технологиями искусственного интеллекта. В частности, использование алгоритмов машинного обучения позволяет выявлять скрытые зависимости между критериями и результатами цифровых проектов, которые сложно формализовать традиционными методами. Это особенно актуально в условиях высокой неопределенности и быстро меняющейся внешней среды. Комбинирование аналитических моделей с интеллектуальными алгоритмами обеспечивает более глубокий уровень анализа и позволяет формировать рекомендации, учитывающие как количественные, так и качественные аспекты управления.

Таким образом, математическое обоснование стратегий цифровой трансформации на основе функций полезности позволяет перейти от интуитивного выбора к формализованной процедуре принятия решений. Такой подход особенно релевантен, поскольку он непосредственно связан с цифровой трансформацией систем управления их предприятия и в организации [1]. Использование многокритериальной модели, нормированных показателей и ограничений оптимизации повышает качество управленческих решений, снижает неопределенность и обеспечивает более точное распределение ресурсов. В перспективе развитие модели может быть связано с использованием нечетких функций полезности и машинного обучения для уточнения весов критериев на основе эмпирических данных.

Библиографический список:

1. Теория и методы принятия решений / О. И. Ларичев. — М.: Логос, 2000. — 296 с.
2. Математические модели управления в цифровой экономике / Д. А. Новиков. — М.: ЛЕНАНД, 2021. — 240 с.
3. Организационно-экономическое моделирование / А. И. Орлов. — М.: Экзамен, 2011. — 576 с.
4. Цифровая трансформация системы управления предприятием: подходы, эффекты, ограничения / В. Н. Козлов, Е. А. Пономарева // Экономика и управление. — 2023. — № 4. — С. 45–53.

СОДЕРЖАНИЕ

СЕКЦИЯ 1
ТРЕНДЫ РАЗВИТИЯ ПРОМЫШЛЕННОГО СЕКТОРА ЭКОНОМИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аминов Т.
ЦИФРОВЫЕ ДВОЙНИКИ И ПЕРСПЕКТИВЫ ЕГО ВНЕДРЕНИЯ 4
Аметов Ш.
ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ В ПРОИЗВОДСТВЕННЫЕ ЦИКЛЫ 5
Ахидова Кубалаш С.А.
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИСПОЛЬЗОВАНИЯ ПРИНЦИПОВ «ЛЕЛЕНАЯ ЭКОНОМИКА» В РОССИИ 8
Ахмедханова Д.
ЗАЩИТА БРЕНДА И ИННОВАЦИЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ 10
Антонова А.С., Шайхутдинов А.А.
ТЕОРИЯ ДЛИННЫХ ВОЛН КОНДРАТЬЕВА И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРОМЫШЛЕННОСТИ: ТРЕНДЫ И ПРОГНОЗЫ 13
Агентьева С.Г.
ЦИФРОВИЗАЦИЯ В СОВРЕМЕННОЙ ЭКОНОМИКЕ: НОВЫЕ ВОЗМОЖНОСТИ И ВЫЗОВЫ КОНКУРЕНТОСПОСОБНОСТИ 16
Алтарева Л.Н., Зыкина А.С., Мамедханова И.Б.
ПЕРСПЕКТИВА ВНЕДРЕНИЯ КОМПЬЮТЕРНОГО ЗРЕНИЯ НА ОТЕЧЕСТВЕННЫХ И ЗАРУБЕЖНЫХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ 18
Багаутдинов И.Н.
ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА ПРОИЗВОДСТВЕННЫЕ ПРОЦЕССЫ В САМОЛЕТОСТРОЕНИИ: ОТ ЦИФРОВОГО МАКЕТА К КИБЕРФИЗИЧЕСКОЙ ЭКОСИСТЕМЕ 20
Бессонов А.А.
ЦИФРОВИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОИЗВОДСТВА: АНАЛИЗ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИНДУСТРИИ 4.0 НА РОССИЙСКИХ ПРЕДПРИЯТИЯХ 22
Бочкарева К.Т.
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ VR-ТЕХНОЛОГИИ В ИЗГОТОВЛЕНИИ ПРОГРЕССИВНЫХ ОРИОВЫХ ЛИНЗ 23
Булдов Р.А.
ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА ПРОИЗВОДИТЕЛЬНОСТЬ ТРУДА В ПРОМЫШЛЕННОСТИ 26
Буранова Ш.
ИНТЕРНЕТ ВЕЩЕЙ КАК ТЕНДЕНЦИЯ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ 28
Бутвинова Е.Н.
ЦИФРОВИЗАЦИЯ РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ 30
Валитова К.Р.
ЦИФРОВОЙ КОНВЕЙЕР: КАК КОММУНИКАЦИИ УСКОРЯЮТ БИЗНЕС-ПРОЦЕССЫ 32
Варич Д.В.
ЦИФРОВЫЕ ТЕХНОЛОГИИ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В РОССИИ 35
Веселько А.Л.
ДИСТАНЦИОННАЯ ЗАНЯТОСТЬ КАК ФОРМА ОРГАНИЗАЦИИ ТРУДА: ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ И РИСКИ 37
Веселько А.Л.
ЦИФРОВИЗАЦИЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ НА РОССИЙСКИХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ 40
Гаврилов Н.С., Копцев В.Л.
ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РАЗВИТИЕ ЦИФРОВОЙ ЭКОНОМИКИ 42
Гаврилов Н.С., Копцев В.Л.
ЦИФРОВЫЕ СТАРТАПЫ В МАШИНОСТРОЕНИИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ 45
Галиуллина Р.Р.
ИНВЕСТИЦИОННАЯ ПРИВЛЕКАТЕЛЬНОСТЬ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В ЭПОХУ ЦИФРОВИЗАЦИИ 46
Гайнетдинов Р.Р.
VR-ТРЕНАЖЕРЫ В СИСТЕМАХ ПОДГОТОВКИ ПЕРСОНАЛА: ЭФФЕКТИВНОСТЬ И ПРАКТИЧЕСКИЕ РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ 48
Галеев С.Р., Шаяхов Е.А.
РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ ПРОМЫШЛЕННЫМИ ПРЕДПРИЯТИЯМИ 51
Галиуллина А.М., Комплетникова Р.Р.
ТРЕНДЫ И ИННОВАЦИИ В ПРОИЗВОДСТВЕННОМ УПРАВЛЕНИИ 54

Таблица 1.1

Сравнение традиционной и IoT-ориентированной модели управления на примере предприятия ЖКХ

Показатель	Традиционная модель	IoT-модель
Периодичность сбора показаний ресурсов	1 раз в месяц	Режим реального времени (непрерывно)
Потери ресурсов (вода, тепловая энергия)	20–25 %	5–8 %
Время реакции на аварийную ситуацию	Часы / сутки	Минуты (автоматическое оповещение)
Численность персонала (контролеры, диспетчеры)	Высокая	Снижение на 40–60 %
Срок окупаемости инвестиций (ROI)	—	12–24 месяца

Наряду с очевидными преимуществами, широкое внедрение IoT сталкивается с рядом ограничений и вызовов:

1. Кибербезопасность — уязвимость миллионов подключённых устройств создаёт новые векторы атак.
2. Проблемы интероперабельности — несовместимость протоколов связи и форматов данных разных производителей.
3. Высокая стоимость первоначального развёртывания — установка датчиков и модернизация инфраструктуры требуют значительных капитальных вложений.
4. Дефицит квалифицированных кадров — острый недостаток специалистов, владеющих компетенциями одновременно в области аппаратного обеспечения, сетей передачи данных и аналитики.

Именно последний фактор для студентов представляет собой не столько угрозу, сколько кажущую возможность. По оценкам АИО «Цифровая экономика», в 2026 году потребность российской экономики в специалистах в области IoT-архитектуры, аналитики данных и разработки встроенных систем составляет не менее 50 000 человек.

Таким образом, Интернет вещей выступает не просто одной из частных технологических тенденций, а системообразующим элементом цифровой экономики 2020–2030-х годов. IoT меняет принципы сбора данных, механизмы принятия решений и модели оказания услуг, формируя экономику проактивного управления вместо реактивного. Для студентов участие в IoT-проектах представляет собой уникальную возможность применить на практике знания из области программирования, электротехники, экономики и менеджмента. В целях системного развития данного направления рекомендуется:

1. Внедрить в образовательные программы вузов (в том числе экономических и управленческих направлений) междисциплинарные модули или курсы по основам Интернета вещей.
2. Создать на базе студенческих кампусов и общежитий «живые лаборатории» (IoT-полигоны) для отработки реальных проектов.
3. Учредить систему конкурсов и акселераторов стартапов в области умных устройств с обязательным участием индустриальных партнёров.

Библиографический список:

1. Аналитика цифровой экономики 2025 / АИО «Цифровая экономика» [Электронный ресурс]. – Форма доступа: https://data-economy.ru/analytics2025 (дата обращения: 25.04.2026).
2. Кузнецов, Д.С. Интернет вещей: экономические эффекты и модели монетизации [Текст] / Д.С. Кузнецов // Журнал инноваций. – 2025. – № 3 (18). – С. 36–42.
3. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс] : Указ Президента РФ от 9 мая 2017 г. № 203. – Форма доступа: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 25.04.2026).
4. Промышленный интернет вещей в России: обзор рынка 2025 / iKS-Consulting [Электронный ресурс]. – Форма доступа: https://iksconsulting.ru/reports/iot2025 (дата обращения: 25.04.2026).
5. Шваб, К. Технологии Четвёртой промышленной революции [Текст] / К. Шваб, Н. Дэвис. – М. : Эксмо, 2024. – 320 с.
6. Федеральный проект «Кадры для цифровой экономики» [Электронный ресурс] // Официальный портал «Цифровая экономика РФ». – Форма доступа: https://d-rf.ru (дата обращения: 25.04.2026).

ЦИФРОВИЗАЦИЯ РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ

Болтенкова Е.И.
Научный руководитель: Дударева А.В.
ФГБОУ ВО Орловского ГАУ, Орел, Россия

Аннотация. В данной статье изучено современное состояние российского промышленного программного обеспечения; выявлена необходимость внедрения цифровизации и ее технологий в данную отрасль, составлен прогноз цифровой промышленности на 2030 г.

Ключевые слова: цифровизация, искусственный интеллект (ИИ), кибербезопасность, промышленное программное обеспечение, импортозамещение.

DIGITALIZATION OF THE RUSSIAN INDUSTRY

Bukhtenova E.I.
Scientific supervisor: Dudareva A.B.
Orel State Agrarian University, Orel, Russia

Abstract. This article examines the current state of Russian industrial software; identifies the need to introduce digitalization and its technologies into this industry; makes a forecast for the digital industry in 2030.

Keywords: digitalization, artificial intelligence (AI), cybersecurity, industrial software, import substitution.

Этап экстренной адаптации в российской промышленности остался позади. В 2024 году началась фаза планомерной цифровой трансформации. Если раньше компании переходили на отечественное ПО в основном под давлением извне, то сегодня это становится частью долгосрочной стратегии по созданию собственных технологических экосистем. Бизнес всё чаще сам инициирует этот процесс, понимая необходимость операционного суверенитета. За год объём рынка промышленного софта в РФ достиг примерно 60 миллиардов рублей. Это на 17,6% больше, чем в 2023 году, когда объём этой отрасли оценивался в 51 миллиард рублей. Данный прогресс обусловлен прежде всего активным курсом на импортозамещение и переходом к развитию собственных отечественных ИТ-решений в критически важных отраслях – оборонно-промышленном комплексе (ОПК), металлургии, энергетике. Прирост в среднем составил от 20% до 60% в зависимости от сектора направления. В ОПК и энергетике доля отечественного софта достигла 60-70%. В энергетике реализованы проекты по цифровизации ситуационных центров для отслеживания происшествий в Сибирском и Дальневосточном федеральных округах. Активно были внедрены цифровые двойники с использованием прогнозной аналитики для оптимизации технологических и бизнес-процессов.

Цифровая трансформация российской промышленности предполагает применение отказоустойчивых систем для бесперебойной работы объектов жизней, коммерческой недвижимости и транспорта с учётом актуальных отраслевых трендов. На фоне быстрого роста вложений в цифровизацию перед компаниями остро стоит задача повышения экономической эффективности и безопасности инженерной инфраструктуры.

Ключевыми факторами развития являются:

1) Обеспечение технологической независимости и переход на российское программное обеспечение в условиях санкций;
2) Растущий спрос на роботизированные решения;
3) Цифровая трансформация промышленности;
4) Повышение стойкой работы ранее импортированных решений с постепенным переходом на отечественные разработки.

Ключевые факторы развития цифровизации российской промышленности представлены на рисунке 1.

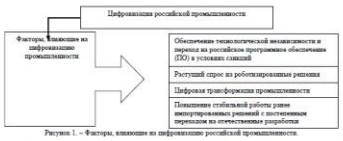


Рисунок 1. – Факторы, влияющие на цифровизацию российской промышленности.

Промышленные предприятия всё активнее применяют системы предиктивной аналитики и машинное зрение на базе ИИ – это помогает снижать число аварий и повышать эффективность работы. За четыре года (к 2025-му) правительство РФ выражало около 22 млрд рублей на разработку и внедрение отечественных программно-аппаратных комплексов. Стратегическая задача - создание промышленного ПО, способного заменить зарубежные аналоги в текущих геополитических условиях.[4]

В 2025 году рынок цифровых решений (особенно в промышленности и бизнес-процессах) демонстрирует умеренный, но стабильный рост -15–20% в год. Быстрее всего развиваются ИИ и машинное обучение, цифровые двойники, предиктивная аналитика и кибербезопасность.

ИИ дает ощутимый эффект: автоматическое выявление «узких мест», самостоятельный запуск улучшений, интерактивный диалог с бизнес-пользователями. Это ускоряет принятие решений и снижает нагрузку на персонал.[5]

На фоне роста числа кибератак спрос на российские средства защиты вырос более чем на 50%. Усиливается внимание к автономным и изолированным информационным системам, защищенным частным облаком, инструментам быстрого реагирования. Отмечается двойственная роль ИИ: он создаёт новые угрозы, но одновременно стимулирует развитие продвинутых методов защиты.

Ключевым ограничением становится дефицит квалифицированных кадров, способных работать на стыке IT и производства, понимать технологические процессы и внедрять комплексные решения. [3] Это подтверждает необходимость подготовки профессионалов нового типа - «супер-пользователей». К 2030 г. размер дополнительных инвестиций IT-компаний в разработку данного сектора экономики составит 174 млрд рублей. К этому времени темп роста закупок отечественного программного обеспечения и услуг составит 210%. В 2030 г. Министерство цифрового развития ожидает более 500 венчурных сделок с привлечением частного капитала, 990 проектов получат гранты на разработку цифровых решений.

Библиографический список:

1. Алексеев, А. Н. Цифровая трансформация промышленности: основы и перспективы импортозамещения ПО [Текст] / А. Н. Алексеев, Д. С. Петров // Экономика и управление. – 2024. – № 5. – С. 42–55.
2. Волков, Л. В. Цифровизация промышленности: направления исследования воздействия цифровых технологий на промышленную сферу и перспективные технологии цифровой трансформации промышленных предприятий / Л. В. Волков // Экономические науки. – 2025. – № 246. – С. 406-411. – DOI 10.14451/1.246.406. – EDN JGYMJQ.
3. Кузин, В. Д. Влияние цифрового маркетинга на организацию производственных процессов в условиях Industry 4.0 / В. Д. Кузин // Экономическое развитие России: тенденции, перспективы: Сборник статей по материалам XI Международной научно-практической конференции преподавателей и студентов. В 2-х томах, Нижний Новгород, 24 апреля 2025 года. – Нижний Новгород: Мининский университет, 2025. – С. 57-60. – EDN MKLFKZ.
4. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Итоги реализации национальной программы «Цифровая экономика» в 2024 году [Текст] : доклад / Минцифры России. – М., 2025. – 112 с.
5. Шпак, П. С. Цифровизация промышленности: переход к Индустрии 5.0 / П. С. Шпак // Цифровое общество: образование, экономика, технологии : Материалы III Международной научно-практической конференции, Новокузнецк, 18–19 марта 2025 года. – Москва: ООО "Актуальность.РФ", 2025. – С. 216-220. – EDN LGLACB.

ЦИФРОВОЙ КОНВЕЙЕР: КАК КОММУНИКАЦИИ УСКОРЯЮТ БИЗНЕС-ПРОЦЕССЫ

Valshtneva K.R.
Научный руководитель: Парфёнова Р.Р.
Казанский национальный исследовательский технический
университет имени А.Н. Туполева-КАИ, г. Казань

Аннотация. В данной статье рассматривается концепция цифрового конвейера как интегральной системы автоматизированного взаимодействия, направленной на минимизацию временных издержек в операционной деятельности современных предприятий. В работе применяется системно-функциональный анализ и методы моделирования бизнес-процессов для определения степени влияния синхронных и асинхронных цифровых коммуникаций на общую производительность труда.

Ключевые слова: цифровой конвейер, бизнес-процессы, цифровая трансформация, организационные коммуникации, автоматизация управления, информационные потоки, операционная эффективность, управленческие решения, оптимизация взаимодействия, индустрия 4.0.

DIGITAL CONVEYOR: HOW COMMUNICATIONS SPEED UP BUSINESS PROCESSES

Valshtneva K.R.
Scientific advisor: Parfilova R.R.
Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan

Annotation. This article discusses the concept of a digital conveyor as an integrated system of automated interaction aimed at minimizing time costs in the operational activities of modern enterprises. The paper uses system-functional analysis and business process modeling methods to determine the impact of synchronous and asynchronous digital communications on overall labor productivity.

Keywords: digital pipeline, business processes, digital transformation, organizational communications, management automation, information flows, operational efficiency, management decisions, interaction optimization, Industry 4.0.

В условиях цифровой трансформации экономики и перехода к индустрии 4.0 предприятия сталкиваются с парадоксальной ситуацией: технологические мощности растут, но скорость прохождения заказа от поступления до отгрузки увеличивается непропорционально. Причина кроется не в медленном оборудовании, а в «коммуникационных заторах» - потерях между завершением одного этапа и началом следующего, вызванных необходимостью ручной передачи информации. В связи с этим возникает потребность в концепции, которая рассматривает коммуникации не как вспомогательную функцию, а как основной механизм ускорения бизнес-процессов. Такой концепцией выступает цифровой конвейер.

Цифровой конвейер представляет собой операционную модель, при которой любое событие в производственной или управленческой системе (завершение операции, отклонение параметра, запрос согласования) автоматически инициирует целевое уведомление следующего исполнителя без ручных запросов и перезвонов контекста [2].

Основными элементами цифрового конвейера являются событийные брокеры, событийно-управляемая маршрутизация, интеграционные связи между информационными системами, автоматическая диспетчеризация задач, метрики коммуникационной плотности (табл. 1).

Таблица 1

Структура цифрового конвейера предприятия

Основные элементы	Состав
Событийные брокеры	Платформы потоковой передачи данных, обеспечивающие прием, хранение и распределение событий между подписанными системами
Событийно-управляемая маршрутизация	Правило вида «если этап N завершен с кодом A → уведомить исполнителя X» или код B → уведомить исполнителя Y»
Интеграционные связи	API-соединения между CRM, ERP, MES, корпоративным мессенджером и системами документооборота
Автоматическая диспетчеризация задач	Боты-распределители, направляющие запросы свободному исполнителю без участия администратора
Метрики коммуникационной плотности	Время от возникновения потребности в передаче информации до начала реакции, фиксируемое в цифровом следе
Реестр схем	Хранилище схем данных, обеспечивающее совместимость версий и предотвращающее «поломку» конвейера при изменении форматов сообщений

Процесс организации цифрового конвейера начинается с аудита коммуникационных заторов — идентификации точек в сквозном бизнес-процессе, где время ожидания превышает время полезной работы. Такой аудит позволяет выявить до 60–80% потерь, ранее не фиксировавшихся в учетных системах, поскольку они относятся не к технологическим операциям, а к межоперационным интервалам.

Для минимизации выявленных заторов используется принцип «pull-коммуникаций» вместо «pull-запросов». В традиционной модели исполнитель следующего этапа вынужден самостоятельно запрашивать статус («pull»), что порождает повторные циклы переписки. В модели цифрового конвейера информация о завершении этапа принудительно доставляется («push») тому, кому она нужна для начала действий, без предварительного запроса [1].

Инновационный потенциал предприятия часто описывают как совокупность ресурсов и компетенций, однако его практическая ценность раскрывается только через коммуникационную реализуемость. Если инновационная разработка существует, но сигнал о ее готовности к передаче в производство задерживается на дни и недели, потенциал остается нереализованным. Именно скорость коммуникаций выступает тем «узким горлом», которое определяет, превратится ли научная разработка в коммерческий продукт.

Под коммуникационной реализуемостью инновационного потенциала предприятия понимается способность организационной структуры обеспечивать передачу информации об инновационных продуктах между подразделениями (от R&D до маркетинга и сбыта) с задержкой, не превышающей технологически допустимый интервал. Основная инновация представляет собой не только технологический, но и коммуникационный процесс, так как объектом передачи является не физический образец, а информация о его характеристиках, статусе готовности и условиях внедрения [3, с. 93].

Процесс построения цифрового конвейера должен включать этапы, связанные с картированием информационных потоков, идентификацией ручных переключений, выбором интеграционных решений, внедрением событийных триггеров и обучением персонала работе в новой коммуникационной парадигме.

В настоящее время существуют три основных метода устранения коммуникационных заторов в бизнес-процессах:

1. Метод хронометража и регламентации — фиксация максимально допустимого времени ответа для каждого типа запросов (например, «на согласование заявки дается 2 часа») с последующим контролем соблюдения.
2. Метод интегрированной коммуникации — соединении информационных систем таким образом, чтобы передача данных происходила без участия человека (например, при оприходовании товара на складе автоматически создается задание на бухгалтерию).
3. Метод событийно-управляемых уведомлений — настройка корпоративного мессенджера или системы управления задачами на автоматическую рассылку уведомлений при изменении статуса процесса, с возможностью перехода к действию по кнопке или ссылке.

Также стоит рассмотреть сравнительный анализ основных методов устранения коммуникационных заторов (табл. 2).

Таблица 2

Сравнительный анализ методов устранения коммуникационных заторов

Критерий сравнения	Метод хронометража и регламентации	Метод интегрированной автоматизации	Метод событийно-управляемых уведомлений
Закрепление ответственности за передачу информации	На отправителя (обязанность уведомить в срок)	На систему (автоматическая передача данных)	На систему и на отправителя (гибридная модель)
Привлечение инвестиций	Низкие затраты (только на рабочее время аналитика)	Высокие затраты (интеграция систем, тестирование)	Средние затраты (внедрение мессенджеров, ботов)
Скорость сокращения заторов	Низкая (зависит от дисциплины персонала)	Высокая (исключает человеческий фактор)	Средняя (сохраняет контроль человека)