DOI 10.37882/2223-2966.2024.03.36

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АВТОМАТИЗАЦИИ В ПРОМЫШЛЕННОСТЬ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

INTRODUCTION OF INFORMATION TECHNOLOGIES AND AUTOMATION IN INDUSTRY: PROBLEMS AND SOLUTIONS

T. Chernyshova
E. Chernyshova
A. Titkov

Summary. The introduction of information technology and automation into industry is a key aspect of the Fourth Industrial Revolution, also known as Industry 4.0. It aims to increase efficiency, reduce costs and improve product quality. However, there are a number of problems along the way that require a comprehensive approach to solving. The article discusses the types of information technology in industry, the advantages and benefits of the introduction of information technology and automation in industry. The problems of the introduction of information technologies and automation in industrial enterprises are identified, as well as ways to solve the identified problems are proposed. The introduction of information technology in industrial enterprises is accompanied by a number of problems faced by IT specialists: uncertainty of requirements and implementation goals, resistance to change on the part of employees, integration with existing systems, data security, complexity of support and maintenance, training and development of competencies, risk assessment and management, limited budgets, scaling problems, maintenance the quality of service. Measures to solve these problems are proposed, as well as a methodology for ensuring cybersecurity of industrial enterprises in the implementation of information technologies, including the following stages: general security strategy, employee training, physical access security, network security, endpoint protection, access control, data backup, data encryption, monitoring and incident response, regular audit and testing vulnerabilities, updating and patching, sharing threat information, compliance with regulatory requirements, an incident recovery plan.

Keywords: automation, industrial automation, information technology, IT, information technology, information technology implementation, information technology in industry.

Чернышова Татьяна Владимировна
Старший преподаватель,
Московский государственный университет технологий и управления имени К.Г. Разумовского
Chernyshova.T1@yandex.ru
Чернышова Евгения Александровна
Младший научный сотрудник, ООО НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНЖЕНЕРНЫЙ ЦЕНТР «СИНТЕЗ»
harchenkoevgenia@gmail.com
Титков Александр Анатольевич
Генеральный директор ООО «ВашЭксперт»
vashexpert2016@yandex.ru

Аннотация. Внедрение информационных технологий и автоматизации в промышленность является ключевым аспектом четвертой промышленной революции, также известной как Индустрия 4.0. Оно направлено на повышение эффективности, сокращение издержек и улучшение качества продукции. Однако на этом пути возникает ряд проблем, которые требуют комплексного подхода к решению. В статье рассмотрены виды информационных технологий в промышленности, преимущества и выгоды внедрения информационных технологий и автоматизации в промышленности. Выявлены проблемы внедрения информационных технологий и автоматизации на промышленных предприятиях, а также предложены пути решения выявленных проблем. Внедрение информационных технологий на промышленных предприятиях сопровождается рядом проблем, с которыми сталкиваются ИТ-специалисты: неопределенность требований и целей внедрения, сопротивление изменениям со стороны сотрудников, интеграция с существующими системами, безопасность данных, сложность поддержки и обслуживания, обучение и развитие компетенций, оценка и управление рисками, ограниченные бюджеты, проблемы с масштабированием, поддержание качества сервиса. Предложены меры по решению данных проблем, а также методика обеспечения кибербезопасности промышленных предприятий при внедрении информационных технологий, включающая этапы: общая стратегия безопасности, обучение сотрудников, физическая безопасность доступа, сетевая безопасность, защита конечных точек, управление доступом, резервное копирование данных, шифрование данных, мониторинг и реагирование на инциденты, регулярный аудит и тестирование уязвимостей, обновление и патчинг, совместное использование информации об угрозах, соблюдение нормативных требований, план восстановления после инцидентов.

Ключевые слова: автоматизация, автоматизация промышленности, информационные технологии, ИТ, информационные технологии, внедрение информационных технологий, информационные технологии в промышленности.

Автоматизация промышленного предприятия включает в себя несколько уровней, начиная от простых автоматических механизмов и заканчивая интегрированными системами, такими как MES (Manufacturing Execution Systems) и ERP (Enterprise Resource Planning), которые позволяют управлять всеми аспектами производственной и деловой деятельности предприятия. Развитие технологий, таких как Интернет вещей (IoT), искусственный интеллект (AI), машинное обучение и робототехника, продолжает расширять возможности автоматизации, делая процессы ещё более умными и взаимосвязанными.

Растущая популярность внедрения информационных технологий и автоматизации на промышленных предприятиях обусловлена их выгодой. Автоматизация позволяет ускорить производственные процессы и увеличить количество выпускаемой продукции за единицу времени. Внедрение информационных технологий помогает минимизировать расходы на труд, энергию и сырьё за счёт оптимизации производственных процессов. Также автоматизация обеспечивает стабильное качество продукции путём постоянного контроля и устранения человеческого фактора, который может привести к ошибкам и дефектам. Вместе с тем автоматизация сокращает необходимость вовлечения работников в опасные и тяжёлые процессы, тем самым уменьшая риск производственных травм и аварий. Современные автоматизированные системы на основе информационных технологий могут быстро перенастраиваться для выпуска новых продуктов или изменения процессов, что делает производство более адаптируемым к потребностям рынка. Кроме того, автоматизация может способствовать более эффективному использованию ресурсов и снижению отходов, влияя таким образом на экологическую устойчивость производства [1, 3, 5].

Внедрение информационных технологий в промышленности является частью процесса цифровой трансформации и охватывает широкий спектр инструментов и систем (рис. 1).

Автоматизированные системы управления технологическими процессами (АСУ ТП) позволяют контролировать и управлять производственными процессами в реальном времени, повышая их эффективность и безопасность. Системы планирования ресурсов предприятия (ERP-системы) интегрируют все бизнес-процессы предприятия, от закупок и логистики до производства, продаж и отчетности. Это помогает оптимизировать ресурсы и улучшить взаимодействие между отделами компании. Интернет вещей (IoT) и промышленный интернет вещей (IIoT) — это сенсоры и устройства сбора данных, которые установлены на оборудовании и соединены между собой через интернет, обеспечивая мониторинг состояния оборудования и оптимизацию производ-

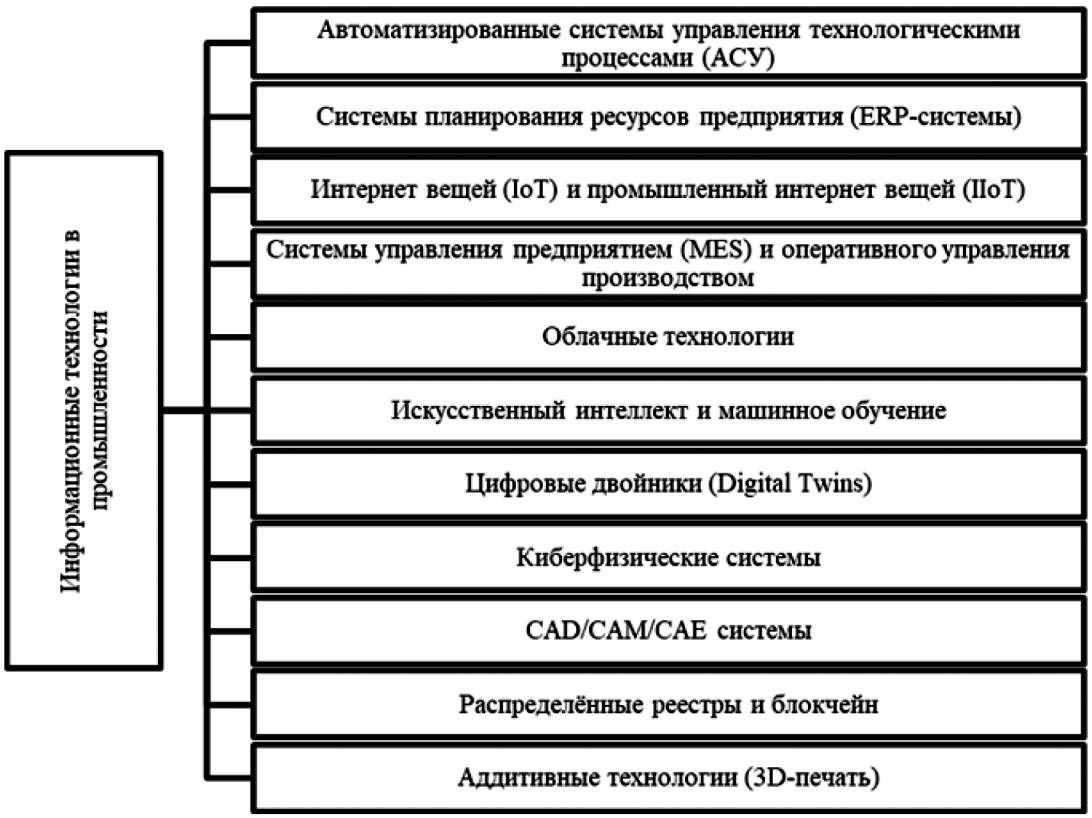

Рис. 1. Виды информационных технологий в промышленности

Источник: составлено автором

ственных процессов. Системы управления предприятием (MES) и оперативного управления производством направлены на более низкий уровень управления в сравнении с ERP и предназначены для оптимизации текущих производственных операций. Платформы и инфраструктура на базе облачных технологий обеспечивают предприятиям гибкость, масштабируемость и доступность вычислительных ресурсов и бизнес-приложений. Искусственный интеллект и машинное обучение — это алгоритмы, позволяющие производить анализ данных и совершенствовать процессы на основе предсказательной аналитики и автоматизации сложного принятия решений [3, 4, 7, 8].

Цифровые двойники (Digital Twins) представляют собой виртуальные копии реального производственного оборудования, процессов или систем, которые используются для моделирования, анализа и оптимизации. Эта технология позволяет моделировать и анализировать работу реального объекта в цифровом пространстве, что даёт возможность оптимизировать его функционирование, проводить эксперименты, прогнозировать результаты изменений и улучшать процессы без вмешательства в реальную систему. Цифровые двойники могут отображать реальное состояние оборудования и производственных процессов в реальном времени, что позволяет более эффективно отслеживать и контролировать автоматизированные системы, а также оперативно реагировать на возможные отклонения и неполадки. В целом, использование цифровых двойников в процессе автоматизации повышает эффективность управления производственными процессами, улучшает качество продукции и сокращает риски, связанные с эксплуатацией оборудования и инфраструктуры на промышленных предприятиях [2].

Киберфизические системы представляют собой такие системы, в которых физические объекты тесно связаны с компьютерными алгоритмами, сетевыми услугами и контролем данных, часто применяются в контексте умных фабрик (Industry 4.0). Системы CAD/CAM/CAE — программное обеспечение для автоматизированного проектирования, производства и инженерного анализа облегчает разработку продукции и подготовку её к производству. Распределённые реестры и блокчейн представляют собой технологии, которые могут быть использованы для улучшения цепей поставок, сертификации продукции и обеспечения прозрачности операций. Аддитивные технологии (3D-печать) — это изготовление объектов путем последовательного наращивания слоев материала, позволяющее создавать сложные детали на заказ и ускорять процесс прототипирования [9, 10].

Эти технологии позволяют улучшить качество производимой продукции, сократить время выхода продукта на рынок, повысить гибкость производства, уменьшить затраты и усилить конкурентоспособность предприятий. Они также могут помочь в управлении ресурсами, в обучении и развитии персонала, а также в соблюдении законодательства и стандартов касательно безопасности и экологии.

Внедрение информационных технологий на промышленных предприятиях сопровождается рядом проблем, с которыми сталкиваются ИТ-специалисты. Наиболее распространенной проблемой является проблема нехватки финансовых ресурсов, так как большинство информационных технологий требует больших начальных инвестиций. Так, приобретение и внедрение нового специализированного оборудования, программного обеспечения и систем управления может потребовать значительных капитальных вложений. Поэтому ИТ-отделы часто работают с ограниченными бюджетами, что затрудняет приобретение лучших решений и технологий на рынке [5, 7].

Зачастую возникает неопределенность требований и целей внедрения информационных технологий. Например, бизнес-подразделения предприятия не могут четко определить, что они хотят от новых ИТ-систем. Это приводит к неоднозначным требованиям и изменениям в процессе внедрения, что усложняет работу ИТ-специалистов и увеличивает сроки и бюджет проекта.

Другой достаточно распространенной проблемой внедрения информационных технологий информационных технологий является сопротивление изменениям со стороны сотрудников. Многие работники привыкли к определенным процессам и не хотят изучать новые системы. Работники могут сопротивляться внедрению новых технологий из-за опасений потерять работу или необходимости изучать новые навыки [9].

Еще одной проблемой при внедрении информационных технологий является сложность интеграции с существующими устаревшими ИТ-системами. Это требует от ИТ-специалистов глубоких знаний как новых, так и старых технологий, а также дополнительных затрат.

Кроме того, с каждой новой технологией увеличивается риск утечек и кибератак. По мере увеличения количества подключенных устройств растет риск кибератак, что требует вложений в меры по обеспечению безопасности. ИТ-специалисты должны обеспечить защиту данных на всех уровнях, разработать и реализовать политики и процедуры безопасности. Новые ИТ-системы требуют постоянной поддержки и обновлений. ИТ-отделам необходимо обеспечивать бесперебойную работу систем, что может быть затруднительно из-за ограниченных ресурсов. Вместе с тем для эффективного внедрения и поддержки новых технологий ИТ-специалистам необходимо постоянно повышать свою квалификацию и следить за последними тенденциями в области ИТ [6, 9].

Также необходимо отметить, что при внедрении новых ИТ-систем возникают риски, связанные с производительностью, совместимостью и надежностью систем. ИТ-специалисты должны уметь идентифицировать и минимизировать эти риски. Необходимо отметить проблемы с масштабированием информационных технологий, так как новые системы должны быть готовы к масштабированию в соответствии с ростом и изменениями бизнеса. Разработка масштабируемых решений требует глубокого понимания бизнес-процессов и перспектив развития компании. При внедрении новых ИТ-систем важно не только запустить их в эксплуатацию, но и обеспечить высокий уровень обслуживания пользователей, что требует дополнительных усилий и ресурсов [1, 5].

Внедрение ИТ и автоматизации требует комплексного подхода, включающего стратегическое планирование, инвестиции в человеческий капитал, техническое обновление и постоянное совершенствование процессов.

Для преодоления выявленных проблем ИТ-специалистам необходимо тесно сотрудничать с бизнес-подразделениями, четко понимать цели внедрения, а также обладать гибкостью и готовностью к непрерывному обучению и развитию. ИТ-специалисты должны уметь показать сотрудникам преимущества новых технологий, обеспечить поддержку и обучение.

Также необходима реализация комплексных мер безопасности для защиты от киберугроз, которые включают в себя ряд стратегий и инструментов, которые вместе образуют многоуровневую оборону против различных видов атак. Предлагается следующая методика обеспечения кибербезопасности промышленных предприятий при внедрении информационных технологий:

1. Общая стратегия безопасности. Важно начать с создания четко определенной стратегии безопасности, которая включает в себя политику безопасности, стандарты и процедуры для всех аспектов IT-системы.
2. Обучение сотрудников. Пользователи являются одной из наиболее уязвимых зон в любой системе безопасности. Регулярные тренинги и информирование сотрудников о типах киберугроз и методах предотвращения инцидентов является ключевым элементом защиты.
3. Физическая безопасность доступа. Защита физического доступа к критически важным системам и оборудованию предотвращает непосредственные попытки вмешательства или кражи данных.
4. Сетевая безопасность. Использование сетевых устройств, таких как брандмауэры (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS), а также шифрование сетевого трафика для защиты от несанкционированного доступа и перехвата данных.
5. Защита конечных точек. Включает в себя антивирусное ПО, обновление ОС и приложений, чтобы предотвратить эксплуатацию уязвимостей.
6. Управление доступом. Методы аутентификации, авторизации и учета для обеспечения того, чтобы пользователи имели доступ только к тем ресурсам, которые необходимы для их работы.
7. Резервное копирование данных. Регулярное создание резервных копий предотвращает потерю данных в случае атаки.
8. Шифрование данных. Защита чувствительных данных с помощью шифрования, как в хранилищах, так и при передаче.
9. Мониторинг и реагирование на инциденты. Непрерывный мониторинг сети и систем на предмет подозрительной активности и быстрое реагирование на инциденты.
10. Регулярный аудит и тестирование уязвимостей. Проведение плановых проверок безопасности и тестирования на проникновение, чтобы идентифицировать и устранить уязвимости.
11. Обновление и патчинг. Своевременное применение патчей к операционным системам, приложениям и оборудованию помогает закрыть известные уязвимости.
12. Совместное использование информации об угрозах. Сотрудничество с другими организациями и правительственными структурами для получения информации о последних угрозах и лучших методах защиты.
13. Соблюдение нормативных требований. Учет требований законодательства и стандартов, таких как GDPR, HIPAA, PCI DSS и других, в зависимости от сферы деятельности и местоположения организации.
14. План восстановления после инцидентов (Disaster Recovery Plan). Разработка и тестирование плана действий на случай серьёзных инцидентов для минимизации времени простоя и потери данных.

Эффективная кибербезопасность требует постоянной бдительности и адаптации к новым угрозам, так как сфера киберугроз постоянно развивается.

Таким образом, внедрение информационных технологий на промышленных предприятиях сопровождается рядом проблем, с которыми сталкиваются ИТ-специалисты: неопределенность требований и целей внедрения, сопротивление изменениям со стороны сотрудников, интеграция с существующими системами, безопасность данных, сложность поддержки и обслуживания, обучение и развитие компетенций, оценка и управление рисками, ограниченные бюджеты, проблемы с масштабированием, поддержание качества сервиса. Предложены меры по решению данных проблем, а также методика обеспечения кибербезопасности про-

мышленных предприятий при внедрении информационных технологий, включающая этапы: общая стратегия безопасности, обучение сотрудников, физическая безопасность доступа, сетевая безопасность, защита конечных точек, управление доступом, резервное копирование данных, шифрование данных, мониторинг и реагирование на инциденты, регулярный аудит и тестирование уязвимостей, обновление и патчинг, совместное использование информации об угрозах, соблюдение нормативных требований, план восстановления после инцидентов.

ЛИТЕРАТУРА

1. Алмазова, К.И. Автоматизация технологических процессов производства на промышленных предприятиях России / К.И. Алмазова, А.О. Курочкина, Р.Н. Берлизев // Тенденции социально-экономического развития в период санкционного воздействия и цифровой трансформации: материалы III Международной научно-практической конференции, Краснодар, 29 марта 2023 года, 2023. — С. 72–76.
2. Арифулин, Н.А. Технология «цифровых двойников» и ее применение в процессе автоматизации основных процессов промышленного предприятия// Научно-образовательный журнал для студентов и преподавателей «StudNet». — 2022. — №1. — URL: https://cyberleninka.ru/article/n/tehnologiya-tsifrovyh-dvoynikov-i-ee-primenenie-v-protsesse-avtomatizatsii-osnovnyh-protsessov-promyshlennogo-predpriyatiya (дата обращения: 17.02.2024).
3. Бояркин, А. Автоматизация в промышленности: технологии, виды, этапы внедрения. — URL: https://sales-generator.ru/blog/avtomatizatsiya-v-promyshlennosti/?ysclid=lsps37uo7r683827715 (дата обращения: 17.02.2024).
4. Жуков, А.О. Автоматизация и цифровая трансформация основных бизнес-процессов промышленных предприятий с помощью искусственного интеллекта / А.О. Жуков, С.В. Пономарева, Н.А. Мерзлякова // Вестник евразийской науки. — 2023. — Т. 15. — № 2. — С. 15–24.
5. Захаров, Н.А. Автоматизация процессов производства: системы автоматизации / Н. А. Захаров // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов: Сборник материалов XIX Международной научно-практической конференции, Москва, 14 апреля 2023 года, 2023. — С. 217–220.
6. Маштакова, А.В., Файзрахманова Е.В. Автоматизация бизнес-процессов на предприятии с помощью Robotic process automation // Экономика и бизнес: теория и практика. — 2021. — №1-1. — С. 205–208.
7. Мечикова, М.Н. Практика и перспективы внедрения технологий индустрии 4.0 на российских промышленных предприятиях в неблагополучных внешнеэкономических условиях / М.Н. Мечикова, Т.Д. Климачев // Вестник Сибирского института бизнеса и информационных технологий. — 2023. — Т. 12, № 2. — С. 100–106. — DOI 10.24412/2225-8264-2023-2-100-106.
8. Мотькин, И.Д. Особенности применения интернета вещей в промышленности / И.Д. Мотькин, М.И. Кондрашов // Технологии. — 2023. — № 2-2(214). — С. 5–7.
9. Романов И.Г., Трушин Н.Н. Проблемы и перспективы автоматизированного проектирования в производственных процессах // Известия Тульского государственного университета. Технические науки. — 2023. — №1. — С. 448–452.
10. Суромкин, А.С. Различные подходы к применению цифровых технологий в процессе автоматизации деятельности промышленного предприятия // Научно-образовательный журнал для студентов и преподавателей «StudNet». — 2022. — №1. — URL: https://cyberleninka.ru/article/n/razlichnye-podhody-k-primeneniyu-tsifrovyh-tehnologiy-v-protsesse-avtomatizatsii-deyatelnosti-promyshlennogo-predpriyatiya (дата обращения: 17.02.2024).

© Чернышова Татьяна Владимировна (Chernyshova.T1@yandex.ru); Чернышова Евгения Александровна (harchenkoevgenia@gmail.com);
Титков Александр Анатольевич (vashexpert2016@yandex.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»