УДК 338.2

# ИНДУСТРИЯ 4.0 КАК ВЫЗОВ ЦИФРОВОМУ СУВЕРЕНИТЕТУ РОССИИ

***Чебыкина В.А.***
*магистрант, Санкт-Петербургский государственный университет, г. Санкт-Петербург*
***Научный руководитель: Ковалевская Н.В.***
*к.пол.н., доцент, Санкт-Петербургский государственный университет, г. Санкт-Петербург*

***Аннотация**: концепция Индустрии 4.0, характеризующаяся интеграцией киберфизических систем (CPS), интернета вещей (IoT) и больших данных в производственные процессы, представляет собой значительный вызов для цифрового суверенитета России. В статье анализируются текущие тенденции и проблемы, связанные с внедрением технологий Индустрии 4.0 в российскую экономику. Особое внимание уделяется вопросам безопасности данных, зависимости от зарубежных технологий и необходимости развития национальных стандартов и инфраструктуры. Автор предлагает стратегические направления для укрепления цифрового суверенитета, включая развитие отечественных технологий, усиление законодательства и международное сотрудничество.*

***Ключевые слова**: цифровая экономика, индустрия 4.0, цифровой суверенитет, технологическая трансформация, Россия.*

# INDUSTRY 4.0 AS A CHALLENGE TO RUSSIA'S DIGITAL SOVEREIGNTY

***Chebykina V.A.***
*graduate student, St. Petersburg State University, Saint-Petersburg*
***Research supervisor: Kovalevskaya N.V.***
*Cand. Po. Sci., Associate Professor, St. Petersburg State University, Saint-Petersburg*

***Abstract**: the concept of Industry 4.0, characterized by the integration of cyber-physical systems (CPS), the Internet of Things (IoT) and Big Data into production processes, poses a significant challenge to Russia's digital sovereignty. The article analyzes current trends and issues related to the implementation of Industry 4.0 technologies in the Russian economy. Special attention is paid to the issue of data security, dependence on foreign technologies and the need for the development of national standards and infrastructure. The author proposes strategic directions for strengthening digital sovereignty, including the development of domestic technologies, strengthening legislation, and international cooperation.*

***Key words**: digital economy, Industry 4.0, digital sovereignty, technological transformation, Russia.*

Цифровая трансформация внесла качественно новые способы ведения бизнеса, хозяйства и повседневной жизни людей. Ведение бизнеса стало более гибким и мобильным благодаря возможностям удаленной работы и онлайн-продажам, что позволяет сократить затраты на аренду офисных помещений и оптимизировать рабочие процессы. В хозяйственной деятельности цифровые технологии позволяют автоматизировать процессы управления, контроля и анализа данных, что повышает эффективность производства и оптимизирует затраты на ресурсы. В повседневной жизни цифровые технологии облегчают коммуникацию, позволяют быстро получать информацию и решать задачи. Например, онлайн-платежи, онлайн-банкинг, онлайн-магазины, социальные сети и мессенджеры упрощают процессы покупки, продажи и

общения.

Таким образом, цифровая трансформация проникла во все сферы жизни общества и государства, в сфере производства она объединила передовые промышленные технологии и цифровые инновации для создания цифровых предприятий [1, с. 3]. Цитата английского экономиста Д.М. Кейнса «Спрос порождает предложение» применима к ситуации, при которой технологии Индустрии 4.0. (например, искусственный интеллект (AI), машинное обучение (ML), Интернет вещей (IoT)) выявили необходимость в обеспечении цифровой безопасности. Для начала стоит дать краткую характеристику основным элементам Индустрии 4.0, упомянутым выше. Интернет вещей (IoT) – это технология, которая позволяет устройствам взаимодействовать между собой и передавать данные посредством сети Интернет. Это могут быть датчики, умные дома, беспилотные автомобили, медицинские устройства (IoMT), и т.д. IoT, безусловно, имеет огромный потенциал для улучшения нашей повседневной жизни и работы. Например, умные дома могут автоматически регулировать температуру, освещение и другие параметры в зависимости от привычек и потребностей проживающих в нем людей. Автомобили могут быть связаны с другими устройствами, чтобы предоставлять более точную информацию о дорожной обстановке и планировать оптимальный маршрут. Медицинские устройства могут мониторить здоровье пациентов и предоставлять врачам более точную информацию для диагностики и лечения. Однако, такое взаимодействие может привести к уязвимостям и нарушениям безопасности. Например, злоумышленники могут получить доступ к вашему умному дому и начать контролировать его системы, или взломать ваш автомобиль и управлять им удаленно. Это может привести к серьезным последствиям, таким как кража личной информации, физический вред или даже угроза жизни.

Для обеспечения безопасности IoT необходимо использовать различные технологии и методы защиты. Например, шифрование данных, биометрическая аутентификация, многофакторная аутентификация, мониторинг и анализ данных для выявления угроз. Кроме того, необходимо обучать пользователей правильному использованию технологий и обеспечивать их безопасность с помощью регулярных обновлений и патчей.

Искусственный интеллект (AI) и машинное обучение (ML) также представляют новые угрозы для цифровой безопасности. Искусственный интеллект (AI) — это область компьютерных наук, которая занимается созданием компьютерных систем, способных выполнять задачи, которые обычно требуют умственного усилия человека. Интеллектуальные системы могут обрабатывать большие объемы данных, анализировать их и принимать решения на основе полученной информации. Машинное обучение (ML) — это подраздел ИИ, который занимается разработкой алгоритмов, которые позволяют компьютерным системам извлекать знания из данных. Машинное обучение использует методы статистики, математики и компьютерных наук для построения моделей, которые могут прогнозировать результаты на основе

предшествующих данных [2]. Таким образом, эти технологии используются для анализа больших объемов данных и принятия решений на основе этого анализа. Сегодня искусственный интеллект и машинное обучение широко используются в различных областях, таких как медицина, финансы, транспорт и производство. Использование этих технологий позволяет повысить эффективность работы, сократить затраты и улучшить качество жизни. Одним из наиболее известных примеров использования искусственного интеллекта является голосовой помощник Siri, который используется на устройствах Apple. Siri использует алгоритмы машинного обучения для распознавания голосовых команд и выполнения соответствующих задач. Машинное обучение широко применяется в медицине, системы которого могут анализировать медицинские изображения, чтобы помочь врачам диагностировать заболевания. Однако, несмотря на все преимущества, существуют и некоторые отрицательные аспекты использования искусственного интеллекта и машинного обучения. Один из главных недостатков — это уязвимость к кибератакам и нарушениям безопасности. Компьютерные системы, использующие ИИ и МО, могут быть скомпрометированы хакерами, что может привести к утечке конфиденциальной информации. Еще один недостаток — это потенциальная потеря рабочих мест. Использование ИИ и МО постепенно приводит к автоматизации процессов, что в конечном счете может привести к сокращению числа рабочих мест в некоторых областях. Более того, если данные, используемые для обучения алгоритмов, будут неправильными или искаженными, то это может привести к неправильным выводам и ошибкам в принятии решений. Например, AI-алгоритм, который используется в финансовой сфере для принятия решений о выдаче кредитов, может допустить ошибку, если данные о заемщике будут недостоверными. Другая угроза для цифровой безопасности связана с возможностью взлома системы и получения доступа к конфиденциальной информации. Например, злоумышленники могут взломать систему управления производством какого-либо предприятия и изменить параметры производства или получить доступ к конфиденциальной информации о продукции.

С Индустрией 4.0. также связывают риски интеллектуальной собственности, работоспособности, защиты окружающей среды, здоровью и безопасности человека [11, p. 35]. Ключевой постулат И4.0. – информационная открытость и транспарентность социально-экономических систем – вступает в конфликт с национальными государственными институтами управления, т.к., во-первых, при росте информационной прозрачности сложнее защищать национальные интересы и безопасность государства, во-вторых, мировой угрозой XXI века стал взрывной рост и масштаб хакерских структур [8, с. 33]. Таким образом, существует много рисков, связанных с внедрением современных технологий в производство, социум и бизнес.

Цифровизация и Промышленный Интернет вещей сделали производство зависимыми от глобальной сети, и, соответственно, уязвимым для кибератак. Большие объемы информации и множество каналов передачи сообщений увеличивают риски

утечки важных данных и ставят под угрозу работу предприятий. Киберпреступники все чаще используют открывшиеся возможности, атакуя промышленные структуры и требуя выкупы за простои производства. Без комплексной системы безопасности критическая информационная инфраструктура государства также находится в уязвимом положении, что порождает риски государственного масштаба. Эксперт И.А. Шеремет отмечает особое деструктивное влияние кибератак на опорные объекты инфраструктуры цифровой экономики (на элементы энергетической, транспортной, производственной, химической инфраструктур) [11, с. 8]. Например, при сбоях в системе на ГЭС (гидроэлектростанциях), в лучшем случае произойдет прекращение подачи электроэнергии, в худшем – затопление территорий. Атаки на системы управления производственными процессами могут привести к нарушению работы производственных линий и оборудования, что может вызвать серьезные последствия для производства и экономики в целом. С появлением новых умных фабрик и других реализаций И 4.0. проблема кибербезопасности на производствах будет усугубляться.

К И4.0. также относят такие понятия, как «умные фабрики», «цифровое производство», сбор данных в режиме реального времени, робототехника и т.д. Умные фабрики – это новое поколение производственных предприятий, которые используют передовые цифровые технологии для автоматизации и оптимизации производственных процессов. Они объединяют в себе технологии Интернета вещей, аналитики данных, искусственного интеллекта и автоматизации, чтобы создать более эффективные и гибкие производственные системы [6]. Одним из ключевых элементов умных фабрик является использование Интернета вещей. Это позволяет управлять производственными процессами в режиме реального времени. Например, датчики могут контролировать температуру, давление, влажность и другие параметры производства, чтобы обеспечить оптимальные условия для работы оборудования и производства продукции. Еще одним важным элементом умных фабрик является аналитика данных. Она позволяет собирать, анализировать и использовать данные для оптимизации производственных процессов. Например, данные могут использоваться для прогнозирования спроса на продукцию, оптимизации логистики и управления ресурсами. Искусственный интеллект также играет важную роль. Он может использоваться для автоматизации производственных процессов, управления качеством продукции и оптимизации эффективности производства. Например, искусственный интеллект может использоваться для определения оптимальных параметров производства или для автоматической диагностики неисправностей в оборудовании.

Таким образом, умные фабрики – это вероятно, самые ресурсоемкие предприятия, построенные в соответствии с концепцией Индустрии 4.0., чтобы они работали, нужно подключение всевозможных машин, устройств и датчиков к сетям — проводным, беспроводным, мобильным. Это открывает перед промышленниками революционные возможности, но вместе с тем создает колоссальное количество новых рисков и угроз кибербезопасности [7]. Умные фабрики имеют множество преимуществ по сравнению

с традиционными производственными предприятиями. Они позволяют увеличить производительность и качество продукции, снизить затраты на производство и улучшить условия работы для сотрудников. Кроме того, умные фабрики могут быть более экологичными.

По мнению А.А. Суворова, традиционные методы обеспечения безопасности не способны гарантировать необходимый уровень защиты в условиях развития Индустрии 4.0 [8]. Следовательно, для защиты устройств и систем требуются новые подходы. Один из современных подходов к кибербезопасности в эпоху цифровой трансформации бизнеса и перехода к Индустрии 4.0. заключается в использовании комплексных систем удаленного мониторинга, основанных на передовых технологиях сбора и анализа данных [3]. Таким образом, методы нейтрализации негативных последствий Индустрии 4.0. связаны с преимуществами технологического прогресса.

Последствием развития И4.0. стал теневой бизнес (сетевое мошенничество, кибератаки), превратившийся в целый развивающийся сектор экономики и оказывающий негативное влияние на социально-экономическое развитие государства, что в свою очередь представляет угрозу национальной безопасности государства в том числе. Эксперт А.В. Пахарев и его коллега отмечают, что не только киберпреступность влияет на экономическую безопасность страны, но и наличие в государстве цифровых валют, появляются неподконтрольные, фидуциарные денежные средства и устойчивость системы сильно ослабляется криминалом [5, с. 88]. Возможное следствие теневого бизнеса – вывод активов в теневую экономику и за рубеж – становится серьезной проблемой государства.

Индустрия 4.0. выходит за рамки производства. Практикуется внедрение цифровых технологий в сферу государственного управления, где риски связаны с материальным и информационным ущербом. Тут остро поднимается вопрос защиты персональных данных граждан и кибербезопасности в отношении информации государственного уровня (гостайны). В сфере государственного и регионального управления вопросы обеспечения цифрового суверенитета непосредственно касаются электронного предоставления государственных и муниципальных услуг, развития информационно-телекоммуникационной инфраструктуры и систем электронной демократии, подготовки цифровых кадров. Российский Единый портал государственных и муниципальных услуг представлен на июнь 2022 года 97,5 млн зарегистрированных пользователей [10], с помощью этого сервиса граждане России могут получить ряд государственных услуг в электронном виде. Портал сохраняет личные данные пользователя, в числе которых серия, номер паспорта, СНИЛС и т.д., утечка которых может иметь негативные последствия. Главная задача государства в этом направлении – обезопасить портал от киберпреступлений, следовательно, от степени цифрового суверенитета государства будет зависеть безопасность персональных данных граждан государства.

Первым шагом к обеспечению безопасности порталов предоставления

государственных услуг является регулярное обновление систем безопасности и программного обеспечения. Это поможет устранить уязвимости и предотвратить возможные атаки. Кроме того, важно внедрить многофакторную аутентификацию для защиты от несанкционированного доступа (например, посредством биометрической идентификации). Разработка строгих правил и процедур для работы с конфиденциальной информацией является еще одним важным шагом в обеспечении безопасности. Правила должны определять, какие данные считаются конфиденциальными, кто имеет доступ к ним, как они хранятся и передаются. Регулярный мониторинг и анализ безопасности систем для выявления потенциальных уязвимостей является еще одним важным шагом в обеспечении безопасности порталов предоставления государственных услуг. Это позволяет своевременно выявлять уязвимости и принимать меры для их устранения. Важным шагом можно назвать сотрудничество с другими государственными организациями и частными компаниями для обмена информацией о киберугрозах и совместных действий по их предотвращению. Разработка планов реагирования на кибератаки и проведение регулярного обучения для персонала по их выполнению является последним, но не менее важным шагом в обеспечении информационной безопасности. Планы реагирования должны определять шаги, которые необходимо предпринять в случае кибератаки, а тренинги помогут персоналу быстро и эффективно реагировать на возможные угрозы.

Таким образом, Индустрия 4.0. внесла качественные изменения в государственную систему, но при всех положительных сторонах прогресса (экономическое развитие, искусственный интеллект и автоматизация общественных процессов, преодоление бедности и т.д.) возможны риски для государства, при которых возникают угрозы цифровому суверенитету. Так, с подключением предприятий к глобальной сети Интернет, цифровизацией информации, переводом на электронное управление увеличилось количество киберпреступлений, совершенных с целью воздействия на государственные органы. Следовательно, можно констатировать наличие возможностей дестабилизирующего воздействия Индустрии 4.0. на цифровой суверенитет государства.

**Литература:**

1. Вызовы Индустрии 4.0. и необходимость новых ответов // IndustriALLglobalunion. 2018. – С. 3.

2. Кибербезопасность в индустрии 4.0: новые вызовы и решения // Железные друзья. Режим доступа: http://ironfriends.ru/kiberbezopasnost-v-industrii-4-0-novye-vyzovy-i-resheniya/ (дата обращения: 07.03.2024).

3. Моржакова М. Иностранному ПО осталось недолго жить в России / М. Моржакова // MASHNEWS. 2023. Режим доступа: https://mashnews.ru/inostrannomu-po-ostalos-nedolgo-zhit-v-rossii.html (дата обращения: 06.03.2024).

4. Пахарев, А.В. Влияние цифровизации теневой экономики на экономическую безопасность государства / А.В. Пахарев, С.Ю. Александрова // СПбГЭУ. Технико-технологические проблемы сервиса. 2022. № 2 (60). – С. 88.

5. Фонтана, К.А. «Умная фабрика» и ключевые технологии Индустрии 4.0 (обзор) / К.А. Фонтана, Б.А. Ерзнкян // Вестник ВГУ. Серия: Экономика и управление. 2022. №4. Режим доступа: https://cyberleninka.ru/article/n/umnaya-fabrika-i-klyuchevye-tehnologii-industrii-4-0-obzor (дата обращения: 19.03.2024).

6. Хантимиров Р. Индустрия 4.0: цифровые уязвимости новой промышленной революции / Р. Хантимиров //Tproger. 2021. Режим доступа: https://tproger.ru/articles/industrija-4-0-cifrovye-ujazvimosti-novoj-promyshlennoj-revoljucii/ (дата обращения: 07.03.2024).

7. Цифровизация и Индустрия 4.0. в станкостроении и металлообработке // АНК Russland. 2021. Режим доступа: https://russland.ahk.de/ru/mediacentr/novosti/detail/cifrovizacija-i-industrija-40-v-stankostroenii-i-metalloobrabotke (дата обращения: 07.03.2024).

8. Цифровой университет России: барьеры и новые траектории развития. М.Н. Дудин [и др.] //Проблемы рыночной экономики. 2021.№ 2. – С. 33.

9. Число пользователей «Госуслуг» выросло за I полугодие 2022 года до 97,5 млн //ТАСС. 2022. Режим доступа: https://tass.ru/ekonomika/15286447 (дата обращения: 09.03.2024).

10. Шеремет, И.А. Обеспечение кибербезопасности в условиях развития цифровой экономики / И.А. Шеремет // Вестн. Моск. Ун-та. Сер. 25: Международные отношения и мировая политика. 2019. № 1. – С.8.

11. Policy department A: Economic and scientific policy / Smit J. [идр.]. – EU, 2016. – P. 35.