Здражевская А.Р

Студентка 2 курса

Российская Федерация, Санкт-Петербург

Международный Банковский Институт им. Анатолия Собчака

**Аннотация.** В статье рассматриваются такие понятия как IoT и RFID: их конфигурация, принцип работы, взаимосвязь. Анализируется рынок IoT: определяются ключевые факторы развития рынка, приводятся конкретные примеры интеграции технологий IoT на базе RFID в различные секторы экономики, подкрепленные статистическими данными. Определяются выгоды, риски, проблемы IoT.

**Ключевые слова.** Интернет Вещей (IoT), RFID-технология, диджитализация, цифровая экономика, эффективность, интеграция, автоматизация, рынок, спрос.

**«ЭВОЛЮЦИЯ RFID-ТЕХНОЛОГИЙ ЭКОСИСТЕМЫ IOT КАК ДРАЙВЕР ЦИФРОВОЙ ТРАНСФОРМАЦИИ СОВРЕМЕННОЙ ЭКОНОМИКИ»**

Zdrazhevskaya A.R.

2nd year student

Russian Federation, Saint Petersburg

International Banking Institute named after Anatoly Sobchak

**Annotation.** The article considers such concepts as IoT and RFID: their configuration, principle of functioning, interrelation. The IoT market is analyzed: key factors of market growth are identified, real examples of integration of RFID-based IoT technologies into various sectors of the economy are presented, supplemented with statistical data. The benefits, risks, and challenges of IoT are determined.

**Keywords.** Internet of Things (IoT), RFID technology, digitalization, digital economy, efficiency, integration, automation, market, demand.

**«EVOLUTION OF RFID TECHNOLOGIES OF THE IOT ECOSYSTEM AS A DRIVER OF DIGITAL TRANSFORMATION OF THE MODERN ECONOMY»**

**Введение**. Очередная волна цифровизации захлестнула земной шар, унося устаревшие идеи и рудиментарные концепции на дно. На их место приходят прогрессивные технологические подходы, открывающие человечеству новую эру инноваций. В контексте разных дискуссий этот решительный переход на более высокий качественный уровень технологического развития принято называть четвертой промышленной революцией, или индустрией 4.0. Особенность в том, что отныне не создаются и развиваются отдельно взятые разработки, а формируется интерактивная среда технологической интеграции, где передовые технологии, такие как искусственный интеллект, робототехника, IoT и другие, объединяются для повышения производительности и эффективности различной экономической деятельности.

Внимание этой статьи сосредоточено на пересечении технологий и экономики с целью понять, как инновационные разработки трансформируют разные отрасли современной экономики. Речь пойдет об экосистеме IoT (Internet of Things – интернет вещей), в частности о неотъемлемой ее составной части - технологии RFID (Radio Frequency IDentification). В данной статье раскрывается сущность понятий IoT и RFID, рассматриваются их основные конфигурационные компоненты и принцип работы, анализируется рыночная ниша Интернета вещей: определяются ключевые факторы роста рынка и приводятся конкретные примеры интеграции технологий IoT (на базе RFID) в различные секторы экономики, их роль и влияние. Рассматриваются выгоды и риски, а также этическая сторона вопроса системы IoT. Статья дополнена статистическими данными и прогнозами экспертов.

**Определение IoT: сущность, компоненты и роль в экономике.**

IoT (Internet of Things – «Интернет вещей») - это сеть взаимосвязанных физических устройств (hardware), программного обеспечения (software), средств подключения (коммутаторов, сетей, датчиков и пр.), которые автоматически «собирают» данные и обмениваются ими. Таким образом, конфигурация включает 3 кластера средств. Под физическими устройствами подразумевается весьма широкий спектр приборов: от лампочек и термостатов до более сложных систем, таких как промышленное и медицинское оборудование. Программное обеспечение способствует быстрой и удобной работе с информацией и данными на физических устройствах. Что касается средств подключения, то они реализованы исполнительными механизмами (например, микроконтроллеры) и коммуникационными технологиями (Wi-Fi, Bluetooth и сотовые сети, сетевые протоколы, и др.), которые позволяют устройствам взаимодействовать друг с другом без непосредственного подключения (в том числе и через сеть Интернет).

Проект Internet of Things был разработан в 1999 году британским технологом Кевином Эштоном, который предложил идею подключения бытовых устройств к сети Интернет для более эффективного их использования; хотя сама концепция Интернета вещей восходит к началу 1980-х годов, когда были разработаны первые smart-устройства и датчики. Но прогрессировать IoT начал только после развития беспроводной связи.

Можно сказать, что рост числа интегрированных устройств -экспоненциальный, этому способствуют достижения в таких областях, как облачные вычисления, аналитика больших данных и искусственный интеллект. Сегодня миллиарды устройств подключены к сети Интернет и генерируют огромные объемы данных, сеть IoT имеет тенденцию стремительного развития: эксперты прогнозируют, что к 2025 году будет интегрировано в сеть IoT более 30 млрд. девайсов, то есть в среднем почти по 4 устройства Интернета вещей на человека, а глобальный рынок IoT к тому времени будет оцениваться в $USD 4,3 трлн.[[1]](#footnote-1) На рис.1 представлена диаграмма, отображающая тенденцию роста числа подключенных устройств за период 2010-2022гг. с прогнозом на 2023-2025 гг.

Рис.1 Количество подключенных устройств IoT (млрд.) 2010-2025гг.

За последние 12 лет количество гаджетов увеличилось в 20,5 раз, ожидается, что к 2025 году будет на 14,5 млрд. подключенных устройств больше, что в совокупности больше показателя 2022 года в 1,9 раз и больше показателя 2010 года в 39 раз.

Основными отраслевыми направлениями, в которые интегрировано на данный момент более 100 миллионов устройств IoT, являются электроэнергетика, газоснабжение, кондиционеры, водоснабжение и утилизация отходов, розничная и оптовая торговля, транспорт и хранение, а также общественные блага и др. Прогнозируется, что к 2030 году общее количество устройств Интернета вещей вырастет до более чем 8 миллиардов *в каждой из сфер*.

Ключевым фактором, стимулирующим рост IoT рынка, является растущая рыночная конкурентоспособность, ведущая к доступности экономически эффективных технологических решений. Другие микро- и макроэкономические факторы прогрессирования Интернета вещей представлены на рис.2

Рис.2 Микро- и макроэкономические факторы роста рынка IoT

Что касается отечественного рынка IoT, в России это направление тоже стремительно развивается: согласно исследованию компании ПАО «МТС», к 2026 году российский рынок Интернета вещей будет оцениваться примерно в 208,5 млрд рублей.[[2]](#footnote-2) Такой рост обусловлен инвестициями в инфраструктуру и внедрением технологий Интернета вещей в различные отрасли экономики.

**IoT в экономике.**

Для большей наглядности в таблице 1 представлены конкретные примеры интеграции технологий IoT в самые разные сферы экономики и приведены статистические сведения.

Таблица 1. Роль IoT в экономике.

|  |  |  |
| --- | --- | --- |
| Сфера | Принцип интеграции IoT: | Статистические данные: |
| Э  Н  Е  Р  Г  Е  Т  И  К  А | Внедрение IoT повышает энергоэффективность: датчики и устройства IoT могут отслеживать потребление энергии и выявлять недостатки, что позволяет оптимизировать потребление энергии.  Обеспечивается интеллектуальное управление электросетью: устройства интернета вещей помогают управлять электросетью и оптимизировать ее, сокращая потери энергии и повышая надежность. | Согласно прогнозу Marketsandmarkets, мировой рынок IoT в энергетике, вырастет с USD$20,2 млрд в 2020 году до USD$35,2 млрд. к 2025 году, а совокупный годовой темп роста составит 11,8% в течение прогнозируемого периода.[[3]](#footnote-3)  По пронозам Statista, ожидается, что к 2025 году мировой рынок интеллектуальных сетей превысит USD$50 млрд., в 2021 он составлял USD$37 млрд.[[4]](#footnote-4) |
| П  Р  О  И  З  В  О  Д  С  Т  В  О | На производстве интеграция технологий IoT способствует более эффективному контролю за состоянием оборудования: устройства Интернета вещей могут контролировать работу и состояние машин в режиме реального времени, обнаруживая потенциальные неполадки до того, как они станут серьезными, что позволит значительно сократить время простоя и затраты на техническое обслуживание. Продукты IoT повышают контроль качества, отслеживая производственные процессы и выявляя любые отклонения от установленных стандартов. | Согласно исследованию MarketsandMarkets, ожидается, что мировой объем рынка промышленного интернета вещей (IIoT) к 2026 году достигнет USD$106,1 млрд, увеличившись на 6,7% с 2023г.[[5]](#footnote-5) |
| С  Е  Л  Ь  С  К  О  Е  Х  О  З  Я  Й  С  Т  В  О | Датчики и устройства Интернета вещей могут предоставлять данные о влажности почвы, температуре и уровне питательных веществ в режиме реального времени, позволяя фермерам оптимизировать рост культур и урожайность. Фиксирующие устройства помогают контролировать здоровье и самочувствие своего скота, сокращая вспышки болезней и повышая производительность. | Эксперты MarketsandMarkets, ожидают: рынок IoT в сельском хозяйстве вырастет с USD$11,4 млрд. в 2021 году до USD$18,1 млрд. к 2026 году.[[6]](#footnote-6)  Согласно отчету Allied Market Research, объем рынка IoT в сельском хозяйстве в 2017 году оценивался в USD$16 млрд. и, по прогнозам, достигнет почти USD$49 млрд. к 2025 году, а с 2018 по 2025 год, благодаря снижению стоимости технологий, ожидается рост рынка в среднем на 14,7%.[[7]](#footnote-7) |
| Т  Р  А  Н  С  П  О  Р  Т  &  Л  О  Г  И  С  Т  И  К  А | Рост эффективности цепочки поставок: технология Интернета вещей позволяет отслеживать товары, посылки и груз в режиме реального времени по всей цепочке поставок, что оптимизирует операции, а значит снижает затраты.  Благодаря разработкам Интернета вещей, в логистике появляется опция автоматизированной маршрутизации, а в транспортном секторе –сервисы по автоматическому выявлению нарушений ПДД и различные датчики безопасности в автомобилях. Логистические и транспортные услуги становятся более доступными. | Согласно совместному исследованию DHL и Cisco, логистические решения с технологиями IoT могут повысить эффективность цепочки поставок примерно на 25%.[[8]](#footnote-8)  Эксперты издания McKinsey & Company, прогнозируют, что техническое обслуживание с технологиями IoT может сократить время простоя оборудования до 50%, а затраты на техническое обслуживание – от 10% до 40%.[[9]](#footnote-9) |
| Р  О  З  Н  И  Ч  Н  А  Я  Т  О  Р  Г  О  В  Л  Я | Эффективное управление запасами: устройства IoT отслеживают количество запасов в режиме реального времени, снижая риск дефицита или избытка товара.  Ритейлеры могут контролировать, прогнозировать спрос и оптимизировать перемещение товаров по всей цепочке поставок. IoT позволяет производить мониторинг потребления энергии в розничных точках и оптимизировать планировку магазинов - размещение товаров на основе структуры покупательского трафика. Улучшается качество обслуживания клиентов: предоставляются персонализированные предложения и рекомендации на основе анализа просмотров товаров на сайте, спроса на разные категории товаров или истории покупок. Персонализация покупок способствует росту продаж и увеличению прибыли. Повышается точность и скорость процесса оформления заказа. Например, Amazon внедрила систему оформления покупок Amazon Go на основе IoT, которая позволяет клиентам оформлять покупки, не стоя в очереди, что обеспечивает более быстрый и удобный процесс совершения покупок. | Согласно исследованию Forrester, с помощью программного обеспечения для автоматизации предприятия могут оптимизировать свои операционные расходы до 90%. В отчете Global Market Insights прогнозируется: к 2026 году рынок ПО для управления запасами ритейлеров достигнет $USD5 млрд.[[10]](#footnote-10)  Эксперты Delloite заключили, что продажи ритейлеров в области электронной коммерции возросли на 30% после внедрения IoT[[11]](#footnote-11).  Компания Walmart внедрила систему IoT, для управления системами отопления, вентиляции и кондиционирования воздуха (HVAC) в своих магазинах, что привело к экономии энергии до 15%. |
| Ф  И  Н  А  Н  С  О  В  Ы  Й  С  Е  К  Т  О  Р | Обнаружение мошенничества: устройства IoT позволяют банкам оперативно обнаруживать мошеннические транзакции, например, с помощью биометрических датчиков для аутентификации личности клиентов и предотвращения кражи личных данных. Технологии IoT предоставляют точную информацию о состоянии и производительности банкоматов, хранилищ, сейфов – своевременно анализируется эффективность и исправность оборудования.  Благодаря технологиям IoT финансовые организации предоставляют своим клиентам целевые услуги: собирается и анализируется информация о предпочтениях, действиях клиента. Яркими примерами технологий IoT в финансовом секторе: бесконтактная оплата, smart-контракты, цифровая валюта, биометрическое распознавание пользователя при входе в онлайн-банк, чат-боты в приложении банка и др. | Согласно изданию IoTForAll, В 2018 году расходы на IoT в банковской и финансовой сферах составили в среднем примерно $USD153млрд.[[12]](#footnote-12) |
| Г  О  Р  О  Д  С  К  А  Я  С  Р  Е  Д  А | Внедрение IoT технологий способствует улучшению общественных услуг: появляются такие решения, как "умный город": "умное освещение", "умная парковка" и "умное управление отходами"; оптимизирует потребление коммунальных ресурсов: датчики системы IoT отслеживают потребление энергии и воды, и управляют ими в режиме реального времени, что позволяет предотвратить чрезмерное потребление ресурсов или большую нагрузку на сети, которая может привести к аварии. «Умные города» считаются населенными пунктами с высоким уровнем жизни и комфортной городской средой. | Согласно отчету Frost & Sullivan, ожидается рост расходов на технологии для "умных городов" в среднем на 22,7%, которые достигнут USD$327 млрд. к 2025 году (в 2019 году – USD$96 млрд.)[[13]](#footnote-13) А специалисты издания MarketsandMarkets прогнозируют, что к 2026 году мировой рынок умных домов достигнет USD$138,9 млрд.[[14]](#footnote-14) |

Согласно представленным в таблице 1 сведениям, можно сделать вывод, что IoT оказал значительное влияние на различные сферы экономики: модернизируется сельскохозяйственный сектор, позволяя фермерам оперативно контролировать свои посевы, домашний скот и управлять ими, меняется энергетический сектор за счет роста энергоэффективности и рационального автоматизированного управления сетями, формируется более плодотворное производство вследствие повышения контроля качества, сокращения времени простоя оборудования, своевременного реагирования на возникающие проблемы и, соответственно, минимизации убытков, существенно преобразились транспортная и логистическая сферы, особенно с точки зрения увеличения эффективности цепочек поставок, улучшения мониторинга товаров и управления ими, а также повышения общей операционной производительности, банки предоставляют более безопасные, качественные услуги на базе предпочтений клиента, трансформируется городская среда –- с точки зрения совершенствования государственных и общественных услуг, оптимизации использования ресурсов и общего качества жизни.

Очевидно, что IoT является важным фактором, стимулирующим цифровизацию экономики и ее переход на качественно другой уровень: повышению производительности, снижению затрат, сокращению издержек, созданию новых рабочих мест и возможностей для бизнеса.

**Определение RFID: сущность, принцип работы, функции и взаимосвязь с IoT**

Краеугольный камень, с технической точки зрения, в сети IoT – это разработка RFID. Технология радиочастотной идентификации (RFID – Radio Frequency Identification) - это инновационный инструментарий, популярность которого в последние годы стремительно растет. RFID в сущности представляет собой беспроводную технологию, которая использует радиоволны для определения и контроля различных материальных объектов, состоит из трех основных компонентов: считыватель («запросчик»), программное обеспечение (ПО) и микросхемы или «метки» (транспондеры, содержащие микрочип и антенну). Метка внедряется в объект, а считыватель излучает радиоволны, микрочип хранит информацию об объекте, к которому прикреплена метка, а антенна позволяет метке взаимодействовать с RFID-считывателями. «Запросчик» считывает данные (сигналы), закодированные в микрочипе метки, которые с помощью специального ПО интерпретируются и передаются в хранилище (определенную систему, базу данных и др.).

Концепция заключается в том, что технология позволяет автоматически идентифицировать объекты (предметы, животных или людей) и отслеживать их в режиме реального времени без необходимости прямого контакта, что является фундаментальным аспектом Интернета вещей. RFID считается подмножеством IoT, поскольку это достаточно специфическая технология контроля объектов, в то время как IoT охватывает более широкий спектр средств и приложений. Взаимосвязь между RFID и IoT является симбиотической, поскольку RFID позволяет IoT отслеживать физические объекты, а IoT предоставляет инфраструктуру для управления данными, генерируемыми с помощью RFID. Иными словами, технология беспроводной радиочастотной связи является основополагающей компонентой, отвечающей за эффективную автоматизацию процесса мониторинга, сбора и передачи данных. Без инструментария RFID сеть IoT практически дисфункциональна.

Технология, несмотря на новаторство предлагаемых решений, имеет несовершенства. В таблице 2 отображены две стороны RFID.

Таблица 2. Плюсы и минусы RFID

|  |  |
| --- | --- |
| Преимущества RFID | Недостатки RFID |
| Повышенная эффективность: автоматизируются такие задачи, как интерактивное управление объектами и отслеживание. | Стоимость: первоначальное внедрение технологии RFID может быть дорогим, поскольку для этого требуется специализированное оборудование и программное обеспечение. |
| Повышенная точность: человеческий фактор сводится к минимуму. | Проблемы конфиденциальности: технология RFID может использоваться для отслеживания отдельных лиц без их ведома или согласия. |
| Оперативные данные: предоставляются данные о местоположении и статусе объектов в режиме реального времени, что позволяет принимать более эффективные решения. | Помехи и ограниченность диапазона: радиочастотным сигналам могут мешать другие беспроводные сигналы, что приводит к ошибкам или потере данных, а диапазон RFID-сигналов ограничен, что может затруднить отслеживание объектов, расположенных далеко. |

Из приведенной характеристики видно, что есть ряд недостатков RFID. Однако непрерывная модернизация технологий и признание существующих несовершенств имеют решающее значение для полного использования потенциала любой разработки. С каждым новым обновлением RFID продвигается вперед, подчеркивая важность динамической адаптации.

Несомненно, технология радиочастотной идентификации значительно модернизирует целый ряд производственных процессов, поэтому ее внедрение в различные секторы экономики становится выгодной инвестицией. Для большей наглядности, на рис.3 представлена диаграмма, которая иллюстрирует пропорциональное распределение технологии RFID как составного компонента IoT, по различным секторам экономики в процентах.

Рис.3 Пропорциональное распределение интегрированных RFID систем по секторам экономики.

Внедрение технологии RFID оказал влияние на конъюнктуру рынка труда. Радиочастотная идентификация повысила эффективность и точность в различных отраслях промышленности, что привело к структурным изменениям в сфере занятости. Происходит сокращение числа рабочих мест, связанных с ручным трудом и рутинными операциями (кассиры, фасовщики, сметчики, операторы, складские работники и т.д.), теряет востребованность некоторый административный персонал (делопроизводители, секретари и др.), вместе с тем возросла потребность в квалифицированных работниках, которые могут проектировать, разрабатывать и обслуживать RFID-устройства, а также анализировать и использовать данные, генерируемые этой технологией, для оптимизации бизнес-процессов (ннженеры-робототехники, разработчики схемотехники и микроэлектроники, сетевые и системные администраторы, аналитики и др.).

Таким образом, компаниям крайне важно адаптироваться к меняющимся условиям рынка труда, чтобы оставаться конкурентоспособными в долгосрочной перспективе.

**Проблемы RFID и IoT: способы преодоления сопутствующих рисков.**

Как уже было отмечено, технология радиочастотной идентификации приносит пользу различным отраслям экономики. Однако становление экосистемы IoT, с интегрированной в нее RFID, более доступной и широко распространенной структурой сопряжено с рисками нарушения конфиденциальности, утечкой данных и неэтического применения. Следовательно, возникает вопрос о том, перевешивают ли экономические выгоды Интернета вещей и RFID потенциальные риски, связанные с их использованием. В таблице 3 отображены ключевые возможные риски и способы их решения

Таблица 3. Проблемы, риски RFID-технологий сети IoT и пути решения.

|  |  |  |
| --- | --- | --- |
| ***Риски:*** | **Краткое описание:** | **Способы решения:** |
| *Риски нарушения*  *конфиденциальности:*  *вероятны утечки данных* | Утечка данных связана со сбором и передачей огромных массивов персональных сведений (информация о местоположении, история посещенных страниц, действия пользователя в сети и т.д.), которые могут быть использованы злоумышленниками не по назначению, что влечет серьезные последствия для частных лиц, предприятий и даже национальной безопасности. | Использование криптографии: необходимо внедрение более надёжных алгоритмов шифрования (например, Secure Sockets Layer (SSL) и Transport Layer Security (TLS)) и протоколов передачи данных (HTTPS, MQTT или CoAP), которые сокращают риск несанкционированного доступа. Важно отладить механизмы аутентификации, авторизации, валидации - сформировать многоуровневый контроль доступа (RBAC). Важно фиксировать и реагировать на попытки входа неавторизованных пользователей. Также непрерывный мониторинг активности системы может помочь обнаружить потенциальные угрозы безопасности и обеспечить своевременное реагирование. |
| *Риски кибербезопасности: подверженность уязвимостям и киберугрозам* | Устройства IoT (в том числе на основе RFID) подключены к сети Интернет, поэтому они подвержены таким уязвимостям как DDoS, DoS, фишинговые атаки, программы-вымогатели и другие вредоносные программы. Эти кибератаки представляют значительные угрозы для устройств, потенциально приводя к критическим сбоям оборудования и порче данных, финансовым потерям | Важно поддерживать актуальность программного и микропрограммного обеспечения, так как производители часто выпускают обновления с исправлениями существующих уязвимостей.  Интеграция брандмауэров и систем обнаружения вторжений (IDS) для предупреждения о подозрительной активности в сети.  Важно проводить регулярные аудиты безопасности: своевременно выявить любые уязвимости и устранить их до того, как они смогут быть использованы хакерами. |
| *Социально-этические риски* | Не менее остро стоит проблема неравного доступа к технологиям IoT, ведь не каждый человек имеет материальную или финансовую возможность для этого - это порождает социальное неравенство.  Кроме того, потенциален риск преднамеренного неэтичного применения технологий (для слежки за частной жизнью, шпионажа, несанкционированного контроля), что является прямым нарушением прав человека и гражданских свобод. | Для решения проблемы неравного доступа обществам с низким уровнем дохода государством могут быть предложены льготы, субсидии и гранты для приобретения технологий IoT. Другим эффективным решением было бы установление партнерства между государством и частными компаниями по созданию общественных центров, предоставляющих недорогой доступ к технологиям IoT. Для сокращения злонамеренного использования RFID- устройств важна коллаборация отраслевых ассоциаций, государства и экспертных сообществ для доработки нормативных актов, регулирующих риски неэтичного использования RFID и IoT и ужесточающих ответственность. Не менее важно развитие мониторинговых систем, моментально фиксирующих и пресекающих использование технологий с преступным умыслом. |
| *Возможные проблемы интероперабельности* | Ситуация отсутствия интероперабельности возникает тогда, когда различные компоненты IoT и RFID несовместимы между собой или не могут эффективно взаимодействовать друг с другом, ввиду использования разных аппаратных программных средств. Это может привести к простою системы, потере данных, снижению производительности и невозможности извлечения пользы от интеграции технологии вовсе. | Одним из решений этой проблемы является установление отраслевых стандартов функциональной совместимости и протоколов связи устройств, для обеспечения их бесшовной интеграции в существующую инфраструктуру. Это может включать создание унифицированных руководств, разработку программных и аппаратных платформ с открытым исходным кодом, а также сотрудничество между заинтересованными сторонами отрасли для установления общих нормативов и практик. |
| *Проблема финансового барьера по внедрению и сопровождению* | Внедрение IoT с радиочастотной идентификацией, в зависимости от масштабов области применения, может оказаться дорогостоящим решением, требующим значительных ресурсов и экспертных знаний. Для малого и среднего бизнеса приобретение и сопровождение этих систем оказывается финансовым препятствием. | Важна государственная поддержка - финансирование (гранты, субсидии) тех разработок RFID-устройств или продуктов IoT, которые являются самыми недорогими по сравнению со своими конкурентами (при качестве, не уступающем другим). Кроме того, дополнительные налоговые льготы для аутсорсинговых и иных компаний-разработчиков сократят их издержки, что позволит снизить стоимость конечного продукта.  С точки зрения предпринимателей, важно оценить все выгоды и потенциальные убытки, поскольку иногда целесообразнее отдать предпочтения облачным решениям (например, SaaS или PaaS) и иным, которые устраняют необходимость в дорогостоящем оборудовании и инфраструктуре. |
| *Риск нормативно-правовых дилемм* | Зачастую в отношении интегрированных технологий сбора, обработки и передачи информации отсутствует ясность в вопросах собственности данных, согласия третьих лиц на их сбор и обработку, норм контроля и безопасности IoT и RFID, что может привести к юридическим дилеммам, судебным искам со стороны конечных пользователей и разным прецедентам. | Главным решением этой проблемы является создание четких правовых рамок и нормативных стандартов, которые защищают права конечного пользователя и поощряют ответственные методы управления данными, а также составление конкретных юридических определений в контексте сбора, передачи и обработки данных (совершенствование политики конфиденциальности, согласий на обработку персональных данных и т.д.). |
| *Дефицит квалифицированных специалистов, разрабатывающих и сопровождающих эти технологии* | Системы IoT и RFID требуют специальных технических знаний для разработки, установки, обслуживания и ремонта. Их отсутствие или дефицит сказывается на качестве услуг для конечных пользователей. | Очевидно, что стимулирование обучения по разработке и сопровождению этих технологий должно быть всесторонним: необходимы государственные и частные инвестиции в учебные программы для развития необходимых навыков, поддержки аутсорсинговых фирм, интеграция в образовательный процесс опытных специалистов, которые подтверждают свои компетенции конкретными успехами в разработке. Также было бы целесообразно разрабатывать удобные интерфейсы, и обучающие программы для повышения доступности и компетентности конечного пользователя (не специалиста). |
| *Высокая степень масштабируемости и нагрузки на сети* | Масштабируемость – способность системы справляться с возросшим трафиком без ущерба для производительности. По мере увеличения количества подключенных к сети IoT устройств становится все сложнее поддерживать ее в рабочем состоянии: требуются большие вычислительные мощности для обработки увеличивающегося объема генерируемых данных. Чрезмерная нагрузка на сети может привести к сбоям, потере данных, отказу системы и сопутствующим убыткам. | Одним из очевидных решений является увеличение пропускной способности сети: добавить в сеть больше аппаратных ресурсов (серверы или маршрутизаторы), модернизировать существующее оборудование для поддержки более продвинутых протоколов, оптимизировать передачу данных путем их сжатия или сокращения частоты передачи. Также можно приоритизировать трафик данных, внедрить алгоритмы машинного обучения и искусственного интеллекта для прогнозирования нагрузки на сеть и подключить периферийные системы (например, облако). Это позволит уменьшить общий объем данных, передаваемых по сети, снижая вероятность перегрузки. |

Рис.4 Риски IoT и внедренной RFID-технологии, потенциальные решения

Таким образом, есть способы разработать комплексную стратегию безопасной интеграции, чтобы минимизировать риски, связанные с внедрением разработок Интернета вещей.

**Заключение.**

В качестве заключения можно сказать, что программные и аппаратные продукты IoT (на основе радиочастотной идентификации) являются важнейшими компонентами современной экономики, а их перманентная динамичная эволюция - фактором цифровизации. Внедрение RFID-устройств имеет как неоспоримые преимущества, так и неизбежные недостатки. С одной стороны, интеграция этих технологий в разные отрасли сопряжена со значительными рисками и вызовами, включая угрозы кибербезопасности, проблемы конфиденциальности, необходимость значительных инвестиций в инфраструктуру и переобучение персонала. С другой стороны, несмотря на эти нюансы, предприятия могут использовать разработки радиочастотной идентификации и других средств Интернета вещей для стимулирования инноваций, повышения операционной эффективности и создания новых бизнес-моделей.

Роль технологий RFID и Интернета вещей в цифровой экономике трудно переоценить. Эти технологии обладают потенциалом для преобразования разных отраслей промышленности и формированию нового бизнес-ландшафта и роста качества жизни людей. Критически важно продолжать изучать новые приложения и варианты использования этих технологий, одновременно разрабатывая стратегии для решения проблем, возникающих при их внедрении.

**Список литературы:**

1. Montazerolghaem, Ahmadreza (2021). "Software-defined Internet of Multimedia Things: Energy-efficient and Load-balanced Resource Management". IEEE Internet of Things Journal. 9 (3): 2432–2442. Doi:10.1109/JIOT.2021.3095237. ISSN 2327-4662. S2CID 237801052 (Дата обращения: 27.02.2023г.)
2. Hu, J.; Lennox, B.; Arvin, F., "Robust formation control for networked robotic systems using Negative Imaginary dynamics" Automatica, 2022. (Дата обращения: 18.02.2023)
3. Gillis, Alexander (2021). "What is internet of things (IoT)?" IOT Agenda. (Дата обращения: 19.02.2023г.)
4. "IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE STD 802.11-2020 (Revision of IEEE STD 802.11-2016): 1–4379. 26 February 2021. doi:10.1100/IEEESTD.2021.9363693. ISBN 978 -1-5044-7283-8 (Дата обращения: 22.02.2023г.)
5. Российский рынок межмашинных коммуникаций и Интернета Вещей по итогам 2019 г., прогноз до 2025 г. - Интернет вещей, IoT, M2M, платформы IoT | ИКТ Аналитика. json.tv.  (Дата обращения: 26.02.2023г.)
6. Валерия Минчичова. Россия в Индустрии 4.0. Молодой учёный — 2020. — № 24 (314). — С. 196—198. (Дата обращения: 28.02.2023г.)
7. Berdahl, Carl Thomas; Baker, Lawrence; Mann, Sean; Osoba, Osonde; Girosi, Federico (7 February 2023). "Strategies to Improve the Impact of Artificial Intelligence on Health Equity: Scoping Review". JMIR AI. 2: e42936. doi:10.2196/42936. ISSN 2817-1705. S2CID 256681439. (Дата обращения: 26.02.2023 г.)

1. Knud Lasse Lueth, “Cellular IoT & LPWA Connectivity Market Outlook 2020 – 2025”, November 2020. URL: https://iot-analytics.com/product/cellular-iot-lpwa-connectivity-market-tracker-2010-25-update-q4-20/ (Дата обращения: 15.02.2023) [↑](#footnote-ref-1)
2. # «Исследование МТС: К концу 2025 года четверть всех IoT-устройств в РФ будут подключены через eSIM», URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2022-07-05/issledovanie-mts-k-koncu-2025-goda-chetvert-vseh-iot-ustrojstv-v-rf-budut-podklyucheny-cherez-esim (Дата обращения: 20.02.2023)

   [↑](#footnote-ref-2)
3. Internet of Things (IoT) in Energy Market | Size, Share, and Industry Analysis | Global Market Forecast to 2025 | MarketsandMarkets (Дата обращения: 17.02.2023) [↑](#footnote-ref-3)
4. Smart grids worldwide - statistics & facts | Statista (Дата обращения: 18.02.2023) [↑](#footnote-ref-4)
5. Industrial IoT Market Size, Global Industry Trends Forecast, Opportunities 2030 [marketsandmarkets.com], (Дата обращения: 19.02.2023) [↑](#footnote-ref-5)
6. Agriculture IoT Market Share, Scope & Industry Analysis 2026 [marketsandmarkets.com] (Дата обращения: 17.02.2023) [↑](#footnote-ref-6)
7. Author: Aniket K. IOT in Agriculture Market Size, Share | Industry Forecast, 2025 [alliedmarketresearch.com] (Дата обращения: 17.02.2023) [↑](#footnote-ref-7)
8. https://www.dhl.com/content/dam/downloads/g0/about\_us/logistics\_insights/dhl\_trendreport\_internet\_of\_things.pdf (Дата обращения: 18.02.2023) [↑](#footnote-ref-8)
9. the-internet-of-things-mapping-the-value-beyond-the-hype.pdf [mckinsey.com] (Дата обращения: 18.02.2023) [↑](#footnote-ref-9)
10. "Inventory Management Software Market by Type (Manually Managed Inventory System, Barcode Scanning System, Advanced RFID), Application (Order Management, Asset Tracking, Service Management, Product Differentiation, Inventory Optimization), Deployment Model (On-premise, Cloud), Organization (Large Enterprise, SMEs), End-Use (Manufacturing, Medical/Healthcare, Retail, Automotive, Oil & Gas), Regional Outlook, Competitive Market Share & Forecast 2026", Global Market Insights Inc. (Дата обращения: 24.02.2023) [↑](#footnote-ref-10)
11. [↑](#footnote-ref-11)
12. How IoT Impacts The Financial Industry (iotforall.com) (Дата обращения: 26.02.2023) [↑](#footnote-ref-12)
13. https://www.frost.com/wp-content/uploads/2019/01/SmartCities.pdf (Дата обращения: 19.02.2023) [↑](#footnote-ref-13)
14. Smart Home Market Size, Share, Trends, Revenue Impact Analysis - 2031 [marketsandmarkets.com] (Дата обращения: 19.02.2023) [↑](#footnote-ref-14)