



КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

Аналитический отчет



Санкт-Петербург

2022

Настоящий аналитический отчет подготовлен Инфраструктурным центром НТИ по направлению «Технет» СПбПУ.

Отчет содержит аналитические материалы, посвященные концепции киберфизических систем. В отчете рассмотрен рынок киберфизических систем, основные барьеры и риски, а также нормативное правовое регулирование развития данного рынка, национальный и международный нормативно-технический ландшафт в области киберфизических систем. Кроме того, проанализированы ключевые игроки и проекты данного рынка, основные технологии и разработки на рынке киберфизических систем, а также показатели по компаниям «Технет» НТИ, специализирующихся на разработке решений в области развития киберфизических систем.

На обложке – изображение, созданное на основе запроса «cyber-physical system» с помощью приложения Midjourney, которое позволяет сгенерировать уникальные рисунки по фотографиям и ключевым словам с помощью нейросети.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	9
ГЛАВА 1. РЫНОК КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ.....	11
1.1 Основные сегменты рынка киберфизических систем	11
1.2 Емкость рынка/сегмента киберфизических систем	11
1.3 Темпы роста рынка/сегмента киберфизических систем.....	13
1.4 Жизненный цикл отрасли /рынка киберфизических систем, стадия зрелости	15
1.5 Тренды развития рынка киберфизических систем.....	18
ГЛАВА 2. БАРЬЕРЫ, РИСКИ И НОРМАТИВНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ РАЗВИТИЯ РЫНКА	25
2.1 Барьеры развития киберфизических систем	25
2.2 Риски развития киберфизических систем.....	27
2.3 Нормативное правовое регулирование, в том числе анализ государственных программ поддержки развития направления киберфизических систем по НИРам и НИОКРам.....	28
2.4 Национальный и международный нормативно-технический ландшафт по киберфизическим системам.....	34
ГЛАВА 3. ОСНОВНЫЕ ИГРОКИ И ПРОЕКТЫ НА РЫНКЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ НАПРАВЛЕНИЯ «ТЕХНЕТ» НТИ	41
3.1 Основные игроки направления киберфизических систем: количество, рыночные доли, описание продуктов и разработок	41
3.2 Оценка успешных бизнес-моделей и лучших практик.....	44
3.3 Инвестиции, сделки M&A, кооперация	47
3.4 Новые крупные проекты: участники, планы, суммы привлеченных инвестиций	49
3.5 Причины закрытия неудавшихся проектов.....	52
ГЛАВА 4. ОСНОВНЫЕ ТЕХНОЛОГИИ И РАЗРАБОТКИ НА РЫНКЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ НАПРАВЛЕНИЯ «ТЕХНЕТ» НТИ	54
4.1 Основные технологии, применяемые на рынке киберфизических систем.....	54
4.2 Обзор ключевых научных разработок в России и мире по результатам библиометрического и патентного анализа	66
4.3 Технологический радар рынка киберфизических систем	73
ГЛАВА 5. ПОКАЗАТЕЛИ ПО КОМПАНИЯМ «ТЕХНЕТ» НТИ, СПЕЦИАЛИЗИРУЮЩИХСЯ НА РАЗРАБОТКЕ РЕШЕНИЙ В ОБЛАСТИ РАЗВИТИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ, ВОВЛЕЧЕННЫМ В РЕАЛИЗАЦИЮ НАПРАВЛЕНИЯ НТИ	76
5.1 Количество компаний НТИ	76
5.2 Краткое описание продуктов и услуг компаний НТИ	79
5.3 Объемы выручки от продажи продуктов и услуг компаний НТИ в рамках сегментов направления НТИ	82
5.4 Количество компаний НТИ, имеющих экспортную выручку по направлению	85

5.5	Объем экспортной выручки компаний НТИ	86
5.6	Количество прав на РИД, зарегистрированных компаниями НТИ	89
5.7	Количество реализуемых проектов по отдельному направлению НТИ	90
5.8	Технологический ландшафт рынка, занимаемого компаниями НТИ	93
ЗАКЛЮЧЕНИЕ		99
ПРИЛОЖЕНИЕ		100
БИБЛИОГРАФИЯ		145

СПИСОК РИСУНКОВ

Рисунок 1. Рынок робототехники по регионам мира (%).....	11
Рисунок 2. Рынок промышленного Интернета вещей по сегментам, 2021 год (%).....	12
Рисунок 3. Рынок промышленного Интернета вещей по регионам, 2021 год.....	12
Рисунок 4. Рост рынка робототехники.....	13
Рисунок 5. Объем рынка Интернета вещей для компаний в 2019–2027 гг, млрд долларов.....	14
Рисунок 6. Рост рынка промышленного Интернета вещей, млрд долларов.....	14
Рисунок 7. Рынки цифрового проектирования в 2020 и 2027 годах.....	15
Рисунок 8. Gartner. Цикл зрелости технологий, значимых для IoT, 2017 год.....	16
Рисунок 9. Gartner. Цикл зрелости технологий, значимых для IoT, 2019 год.....	16
Рисунок 10. Внедрение различных технологий робототехники и Интернета вещей в немецкой промышленности.....	17
Рисунок 11. Статус внедрения передовых ИТ-решений в немецкой промышленности.....	17
Рисунок 12. Количество роботов на 10 000 работников по ряду стран мира, единиц.....	19
Рисунок 13. Ввод в эксплуатацию новых промышленных роботов в год по странам в 2021 году, тысяч единиц.....	19
Рисунок 14. Актуальные тенденции в сфере CAD/CAE.....	22
Рисунок 15. Распределение технологических трендов в CAD по важности и используемости.....	23
Рисунок 16. Барьеры внедрения CAD/CAE в организациях (%).....	27
Рисунок 17. Обзор стандартов ISO, IEC, GB в области киберфизических систем.....	37
Рисунок 18. Основные игроки на рынке киберфизических систем по количеству патентов (ед.).....	41
Рисунок 19. Количество научных публикаций в сфере КФС по годам (единиц, 2006–2023 годы).....	67
Рисунок 20. Количество научных публикаций в сфере КФС по странам (единиц, 2006–2023 годы).....	67
Рисунок 21. Количество научных публикаций в сфере КФС по аффилиации (единиц, 2006–2023 годы).....	68
Рисунок 22. Количество научных публикаций в сфере КФС по аффилиации по России (единиц, 2007–2023 годы).....	68
Рисунок 23. Количество научных публикаций по предметной области по миру (% , 2006–2023 годы).....	69
Рисунок 24. Количество научных публикаций по предметной области по России (% , 2007–2023 годы).....	69
Рисунок 25. Количество поданных заявок на защиту патентов в сфере КФС по годам (единиц, 2006–2022 годы).....	70
Рисунок 26. Количество патентов в сфере КФС по патентным агентствам стран (единиц, 2006–2022 годы).....	71
Рисунок 27. Анализ временной динамики по миру (единиц, 2006–2022 годы).....	71
Рисунок 28. Анализ временной динамики по России (единиц, 2013–2022 годы).....	72
Рисунок 29. Количество патентов по предметной области по миру (% , 2006–2022 годы).....	72
Рисунок 30. Количество патентов по предметной области по России (% , 2013–2022 годы).....	73
Рисунок 31. Технологический радар отечественного рынка КФС.....	75
Рисунок 32. Общая выручка компаний в рамках технологий (млн руб., 2021 год).....	77

Рисунок 33. Средняя выручка компаний в рамках технологических типов (млн руб., 2017–2021 годы).....	77
Рисунок 34. Средняя выручка по субъекту Российской Федерации (млн руб., 2017–2021 годы)	79
Рисунок 35. Динамика общей выручки компаний по технологиям (млн руб., 2017–2021 годы).....	83
Рисунок 36. Динамика общей выручки компаний (млн руб., 2017–2021 годы)	84
Рисунок 37. Динамика средней выручки компаний по технологиям (млн руб., 2017–2021 годы).....	84
Рисунок 38. Динамика средней выручки компаний (млн руб., 2017–2021 годы)	85
Рисунок 39. Доля компаний с экспортной выручкой в общем числе компаний технологии (единиц, 2019 год)...	86
Рисунок 40. Сравнение общей выручки компаний, осуществляющих экспорт, и их экспортной выручки по технологиям (млн руб., 2019 год).....	87
Рисунок 41. Динамика общей экспортной выручки компаний (млн руб., 2017–2019 годы).....	88
Рисунок 42. Сравнение средней экспортной выручки компаний и их средней общей выручки по технологиям (млн руб., 2019 год)	88
Рисунок 43. Динамика средней экспортной выручки компаний (млн руб., 2017–2019 годы).....	89
Рисунок 44. Карточка технологического ландшафта «Робототехническое оборудование и устройства»	94
Рисунок 45. Карточка технологического ландшафта «Средства сбора и / или обработки информации из внешней среды»	95
Рисунок 46. Карточка технологического ландшафта «Технологии проектирования и моделирования».....	95
Рисунок 47. Карточка технологического ландшафта «Интернет вещей».....	96
Рисунок 48. Карточка технологического ландшафта «Облачные вычисления».....	97
Рисунок 49. Карточка технологического ландшафта «Большие данные»	98
Рисунок 50. Доля продуктов / проектов в составе технологии с опережением, паритетом или отставанием относительно зарубежных аналогов	98

СПИСОК ТАБЛИЦ

Таблица 1. Уровень роботизации по различным странам и отраслям промышленности	20
Таблица 2. Факторы, влияющие на развитие рынка Интернета вещей	20
Таблица 3. Основные игроки на рынке киберфизических систем.....	41
Таблица 4. Робототехническое оборудование и устройства.....	55
Таблица 5. Средства сбора и/ или обработки информации из внешней среды.....	56
Таблица 6. Технологии проектирования и моделирования	58
Таблица 7. Интернет вещей	60
Таблица 8. Облачные вычисления	62
Таблица 9. Большие данные	64
Таблица 10. Технологии и субтехнологии КФС	73
Таблица 11. Распределение компаний по технологиям производимой продукции (единицы).....	76
Таблица 12. Распределение компаний по регионам (единицы).....	78
Таблица 13. Средняя выручка по субъекту Российской Федерации (млн руб., 2017–2021 годы)	78
Таблица 14. Ранжированный объем выручки от продажи продуктов компаний НТИ (2021 год)	82
Таблица 15. Перечень компаний НТИ, имеющих экспортную выручку (2019 год)	85
Таблица 16. Ранжированный объем выручки от продажи продуктов компаний НТИ.....	87
Таблица 17. Количество зарегистрированных РИД компаниями НТИ с разделением по технологиям.....	89
Таблица 18. Перечень нормативно-технической документации, разрабатываемой международными организациями в области киберфизических систем	103
Таблица 19. Перспективный план стандартизации в области передовых производственных технологий на 2018–2025 годы (с изменениями №1, №2) в области киберфизических систем	110
Таблица 20. Самые успешные стартапы в сфере киберфизических систем на 2021 год	116
Таблица 21. Новые материалы	118
Таблица 22. Аддитивные технологии	120
Таблица 23. Результаты библиометрического анализа. Публикации с наибольшим количеством цитирований (2006–2023 годы).....	122
Таблица 24. Результаты патентного анализа. Наиболее релевантные опубликованные патенты в сфере КФС (2006–2022 годы)	124
Таблица 25. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части робототехнического оборудования и устройств.....	129
Таблица 26. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части средств сбора и / или обработки информации из внешней среды.....	130
Таблица 27. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части технологий проектирования и моделирования	131
Таблица 28. Перечень и описание продукции компаний НТИ в части систем Интернета вещей.....	133
Таблица 29. Перечень и описание продукции компаний НТИ в части облачных вычислений.....	134

Таблица 30. Перечень и описание продукции компаний НТИ в части Больших данных.....	136
Таблица 31. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части робототехнического оборудования и устройств	138
Таблица 32. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части средств сбора и / или обработки информации из внешней среды	139
Таблица 33. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части технологий проектирования и моделирования	140
Таблица 34. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части систем Интернета вещей.....	142
Таблица 35. Описание проекта компании НТИ в части облачных вычислений	143
Таблица 36. Описание проекта компании НТИ в части Больших данных	144

ВВЕДЕНИЕ

Киберфизические системы – достаточно устоявшаяся тематика в современной научной литературе. Общий поиск научных публикаций в системе Scopus по запросу cyber AND physical AND system выявляет более 30 тысяч публикаций [1].

Наиболее простое объяснение сущности киберфизических систем – интеграция вычислительных мощностей с физическими объектами, сочетание вычислений и физических процессов [2]. Киберфизические системы часто встроены в физический мир и могут взаимодействовать с ним в режиме реального времени. Примеры киберфизических систем включают роботизированные линии, беспилотные автомобили, интеллектуальные электрические сети и медицинские устройства, которые контролируют и диагностируют пациентов. Эти системы используют датчики, приводы и другие устройства для сбора данных из физического мира и используют эти данные для управления поведением системы.

Цель КФС – обеспечить бесшовную интеграцию физического и цифрового миров для создания более эффективных, надежных и быстродействующих систем [3].

Ключевая проблематика концепции киберфизических систем связана с максимально широким толкованием термина в научной литературе, а также участниками рынка. В настоящее время отсутствует общепринятое определение термина «киберфизическая система». Зачастую это приводит к синонимическому использованию понятий КФС и «Интернет вещей».

Национальный институт стандартов и технологий США (NIST) определяет киберфизические системы как **совокупность взаимодействующих и интегрированных друг с другом цифровых, аналоговых, физических компонентов и человека** [4].

Согласно NIST [5], как Интернет вещей, так и киберфизические системы включают взаимодействующие логические, физические, преобразовательные и человеческие компоненты, спроектированные для функционирования посредством интегрированных схем логического и физического взаимодействия. *«Понятия «киберфизические системы», или «CPS», и «Интернет вещей», или «IoT», имеют разное происхождение, но при этом перекрывающиеся определения. Оба понятия апеллируют к тенденциям интеграции цифровых возможностей – возможности подключения устройств в единую сеть и использования вычислительных мощностей – с физическими устройствами и системами. Примеры КФС / «Интернета вещей» варьируются от интеллектуальных транспортных средств до передовых производственных систем в таких разнообразных отраслях как энергетика, сельское хозяйство, умные города и т.д.»*. Совпадение терминов можно объяснить их происхождением из различных технологических сообществ, в какой-то момент пришедших к единому предмету деятельности [5].

В статье The 12 Flavors of Cyberphysical Systems (IEEE Journals & Magazine) авторы приводят обзор двенадцати альтернативных определений киберфизических систем и отмечают сложность выявления связей между понятиями КФС и Интернет вещей до появления четких и непротиворечивых определений обоих терминов [6].

Также для оценки ключевой терминологии КФС был выполнен автоматизированный анализ аннотаций научных публикаций, выгруженных из системы научного цитирования Scopus (на массиве более 7656 публикаций). Исследование было выполнено с помощью метода тематического моделирования BERTopic, основанного на технологиях кластеризации семантических векторов [7]. Алгоритм исключил из анализа 3550 статей на основании того, что эти публикации затруднительно отнести к какой-либо определенной тематике. Таким образом, в выборку попало 4106 статей, по результатам анализа которых BERTopic выявил 108 тем. То есть на одну тему в среднем приходится 38 статей.

К наиболее популярным темам публикаций относятся тематики: дорожное движение_автомобили_автомобиль_транспортировка (traffic_vehicles_vehicle_transportation, 151 публикаций), обнаружение_обучение_глубинное_атаки (detection_learning_deep_attacks, 142 публикации), цифровой_двойник_цд_двойники (digital_twin_dt_twins, 136 публикаций), системы_мир_физический_кфс (systems_world_physical_cps, 131 публикаций), верификация_гибрид_формальный_модель (verification_hybrid_formal_model, 125 публикаций). Всего на

лидирующие 10 тематик приходится 1117 публикаций.

Наряду с другими сферами применения и реализации киберфизические системы активно используются в промышленности. Результаты тематического моделирования показали, что исследования также ведутся в рамках многих направлений в промышленной сфере. Так, выше уже упоминались тематики кибербезопасности (142 статьи), цифровые двойники (136 статей), верификация моделей (125 публикаций). Также этот перечень можно дополнить следующими тематиками: моделирование_комоделирование_модели (simulation_cosimulation_models, 104 публикации), техническое обслуживание_машина_данные_производство (maintenance_machine_data_manufacturing, 82 публикации), а также тематика, связанная с Четвертой промышленной революцией: Индустрия_4.0_производство_промышленный (industry_40_manufacturing_industrial, 79 статей).

Иногда КФС и передовые производственные технологии (в некоторых случаях «умная фабрика») используются как тождественные термины. Тем не менее, существует ряд различий. Киберфизическая система – любая система, сочетающая вычисления и физические процессы, а умная фабрика – это объект, в рамках которого киберфизические системы используются для автоматизации и оптимизации операций. Другими словами, умная фабрика – это особый тип киберфизической системы, который используется в производстве [3].

В Российской Федерации в течение 7 лет развивается направление «Технет» Национальной технологической инициативы по поддержке и развитию передовых производственных технологий. В рамках этого направления осуществляется интеграция существующих компетенций для формирования базиса национальной конкурентоспособности по развитию «фабрик будущего». Базовые принципы развития направления «Технет» преодолевают противоречие, заложенное широким трактованием термина «киберфизических систем».

В основе направления «Технет» – «Фабрики будущего», – системы комплексных технологических решений, в рамках которых обеспечиваются сокращение сроков проектирования, производства и вывода конкурентоспособной продукции. В рамках этого направления выделяются три типа в соответствии с этапом производственного процесса: «Цифровые» фабрики (проектирование продукции) – «Умные» фабрики (производство продукции) – «Виртуальные фабрики» (сбыт, сервисное обслуживание, логистика продукции) [8].

Из всех выделяемых типов «Умные» фабрики в наибольшей степени соответствуют и близки концепции применения киберфизических систем в современных промышленных производствах. К ключевым технологиям этого типа фабрик относятся такие сквозные технологии направления «Технет», как промышленная робототехника, сенсорика, технологии беспроводной связи, промышленного Интернета вещей и больших данных. В то же время к киберфизическим системам могут быть отнесены и технологии, которые применяются на других этапах цепочки добавленной стоимости в производстве. В рамках направления «Технет» НТИ – это цифровое проектирование и моделирование, новые материалы и аддитивные технологии.

Важно отметить, что в рамках направления «Технет» НТИ технология цифровых двойников (далее – ЦД) является технологией–интегратором практически всех «сквозных» цифровых технологий и субтехнологий, позволяет высокотехнологичным компаниям переходить на новый уровень технологического и устойчивого развития на пути к промышленному лидерству на глобальных рынках [8]. ЦД как технология близка КФС и используется для киберфизической интеграции умного производства.

Благодаря обратной связи, с помощью которой физические процессы влияют на виртуальный объект и наоборот, КФС и ЦД могут повысить эффективность и устойчивость производственной системы. При этом используются одни и те же основные концепции киберфизического соединения, взаимодействия в реальном времени, организационной интеграции и углубленного взаимодействия. В то же время КФС и ЦД не идентичны со многих точек зрения, включая процесс разработки, инженерные методы и основные элементы [9].

Для целей этого обзора, с учетом выводов по анализу понятия под рынками киберфизических систем понимаются непосредственно рынок КФС, а в качестве сегментов – элементы физической (промышленная робототехника, сенсорика и рынок промышленного Интернета вещей) и программной/цифровой/виртуальной среды (рынок цифрового проектирования и моделирования, больших данных).

ГЛАВА 1. РЫНОК КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ

В главе рассмотрены основные сегменты рынка киберфизических систем, приведены оценки емкости и темпов роста рынка, а также представлен анализ жизненного цикла отрасли и тренды развития рынка киберфизических систем.

1.1 Основные сегменты рынка киберфизических систем

Рынок киберфизических систем можно определить некоторыми технологическими направлениями или сегментами – элементами физической и программной среды. В соответствии с этим в рамках аналитического обзора были выделены следующие технологические сегменты рынка киберфизических систем:

1. Элементы физической среды:
 - Рынок промышленной робототехники (industrial robotics);
 - Смежные рынки промышленной сенсорики (industrial sensors) и промышленного Интернета вещей (industrial internet of things market) в его аппаратном компоненте.
2. Элементы программной/цифровой/виртуальной среды:
 - Рынок цифрового проектирования и моделирования (CAD/CAE);
 - Рынок больших данных (Big data).

В большинстве случаев маркетинговые обзоры и профильные исследования, содержащие обзорные данные по рынку Интернета вещей, практически полностью совпадают с рынком киберфизических систем. Необходимо отметить, что маркетинговые и консалтинговые агентства в своих документах чаще используют термин «Интернет вещей» как более «популярный».

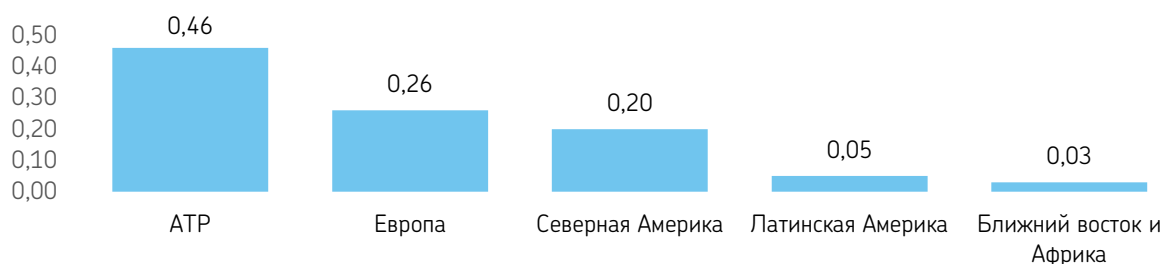
1.2 Емкость рынка/сегмента киберфизических систем

Ряд маркетинговых агентств приводит оценку рынка киберфизических систем в целом. Так, в 2018 году агентство Credence Research оценивало емкость рынка КФС в размере 60,5 млрд долл., в 2020 году агентство Research and Markets оценило емкость рынка КФС в 2020 году в размере 71,75 млрд долл., а в 2022 году Агентство Future market insights оценивает мировой рынок КФС в размере 86,9 млрд долл. [10; 11]. Тем не менее, большая часть сегментов рынка КФС оценивается в рамках более узких технологических рынков.

Робототехника

По оценкам Precedence Research в 2021 году размер мирового рынка робототехники достиг 79,5 млрд долл. и, как ожидается, превысит 225,6 млрд долл. к 2030 году. Среднегодовой темп роста в 2022–2030 гг. составит 12,29% [13].

Рисунок 1. Рынок робототехники по регионам мира (%)



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Precedence Research

На промышленных роботов в 2021 г. пришлось 52% выручки рынка робототехники – 42,3 млрд долл., при этом на отрасль обрабатывающей промышленности пришлось 68%.

Агентство Fortune Business Insights приводит несколько иные оценки: рынок промышленной робототехники оценивался в 15,6 млрд долл. в 2021 году. Агентство прогнозирует рост рынка до 34,68 млрд долл. к 2029 году со среднегодовым темпом роста рынка в размере 11,4% [12].

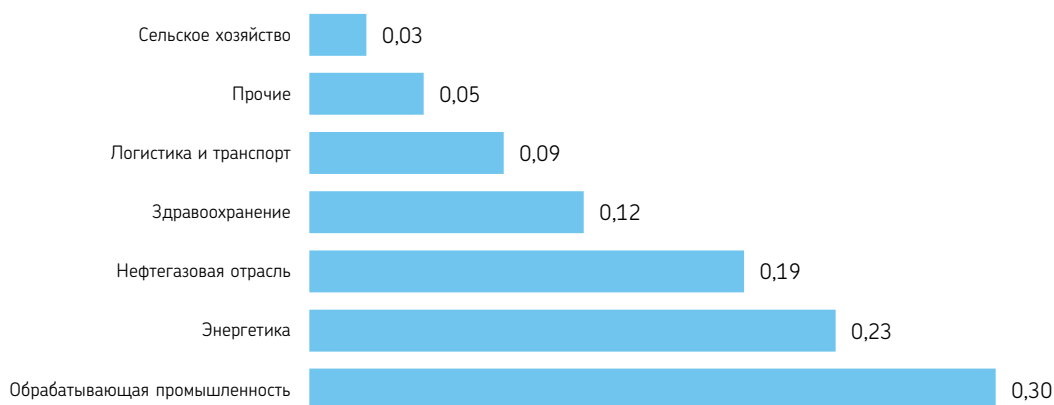
В свою очередь исследователи Allied Markets Research оценили объем мирового рынка промышленной робототехники 2020 года в размере 37,8 млрд долл., и отметили, что к 2030 году он достигнет 116,848 млрд долл. [13].

Промышленный Интернет вещей

Размер рынка промышленных датчиков оценивается агентством Markets and Markets в 20,6 млрд долл. в 2021 году. Как ожидается, рынок достигнет 31,9 млрд долл. к 2026 году при среднегодовом темпе роста 9,1% в период с 2021 по 2026 год [14].

Размер мирового рынка промышленного Интернета вещей в 2021 году агентство Precedence Research оценивает в 326,1 млрд долл. [15]. По оценкам агентства, к 2030 году рынок достигнет объема 1742,8 млрд долл. с зарегистрированным среднегодовым темпом роста рынка 20,47% в течение прогнозируемого периода с 2022 по 2030 год. В 2021 году на рынке промышленного Интернета вещей доминировал сегмент обрабатывающей промышленности, на который пришлось 30% рынка.

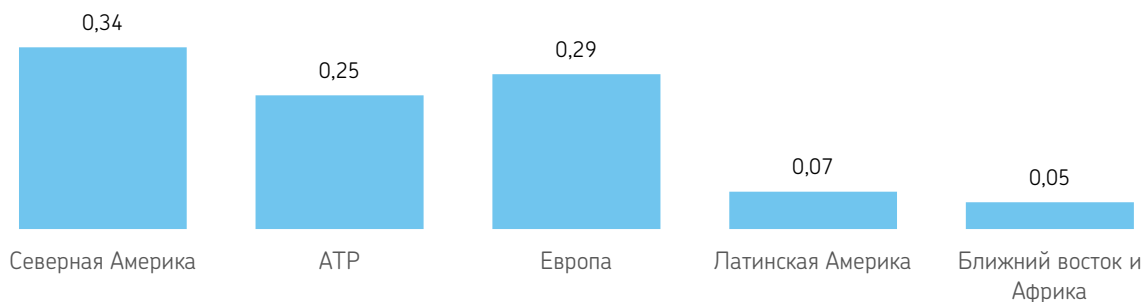
Рисунок 2. Рынок промышленного Интернета вещей по сегментам, 2021 год (%)



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Precedence Research

В географическом разрезе на рынке доминируют рынки Северной Америки и Европы.

Рисунок 3. Рынок промышленного Интернета вещей по регионам, 2021 год



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Precedence Research

Цифровое проектирование и моделирование (CAD/CAE)

Размер мирового рынка цифрового проектирования и моделирования (CAE) оценивался компанией Grand View Research в размере 8,9 млрд долл. в 2021 году [18]. Ожидается, что в период с 2022 по 2030 год рынок будет расти в среднем на 8,8% в год в связи с увеличением спроса на аутсорсинг производственных процессов в странах с развивающейся экономикой, таких как Китай, Индия и Россия [18].

Иным образом оценивает рынок цифрового проектирования и моделирования (CAE) агентство Research and Markets. По оценкам агентства, в 2020 году в условиях пандемии мировой рынок CAE достиг отметки в 5,2 млрд долл., а к 2027 году он достигнет 9,6 млрд долл. Американский рынок цифрового проектирования и моделирования оценивался агентством в размере 1,6 млрд долл. в 2020 году. Наиболее быстро развивающимся рынком цифрового проектирования и моделирования является рынок Китая, который, согласно прогнозам, достигнет размера рынка в 1,3 млрд долл. к 2027 году [5].

По оценкам Researchandmarkets прогнозируется, что мировой рынок программного обеспечения для автоматизированного проектирования (CAD) достигнет стоимости 18,7 млрд долл. в 2030 году, увеличившись с 9,3 млрд долл. в 2019 году, и будет расти на 6,6% в течение прогнозируемого периода с 2020 по 2030 год [16]. Аналитики агентства считают, что движущей силой рынка будет выступать растущее использование программного обеспечения систем автоматизированного проектирования в производстве упаковки и растущее внедрение технологий в автомобильной промышленности.

Большие данные (big data)

Размер рынка больших данных оценено агентством Markets and Markets в 162,6 млрд долл. в 2021 году. По прогнозам рынок вырастет до 273,4 млрд долл. к 2026 году при совокупном годовом темпе роста 11,0% в течение прогнозируемого периода с 2021 по 2026 год [19].

Ожидается, что резкое снижение стоимости технологий, разработка платформ для работы с большими данными на основе открытого исходного кода, хранение и обмен данными в гибридных и многооблачных средах, а также реализация стратегий цифровой трансформации компаний будут стимулировать внедрение решений и услуг на основе больших данных.

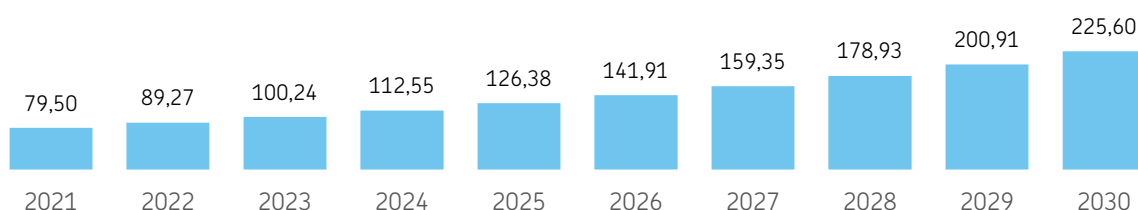
1.3 Темпы роста рынка/сегмента киберфизических систем

По оценке агентства Researchandmarkets, в глобальном масштабе рынок киберфизических систем достиг в 2020 году рыночной стоимости в размере 71,75 млрд долл., при этом ожидается, что с 2021 по 2029 год рынок будет расти со среднегодовым темпом роста 9,3%. По оценкам агентства Dataintel [20], размер мирового рынка киберфизических систем будет расти в среднем на 9% до 2030 года.

Робототехника

Среднегодовой темп роста рынка робототехники, по оценкам Precedence Research, в 2022-2030 составит 12,29% [17].

Рисунок 4. Рост рынка робототехники



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Precedence Research

По оценкам агентства Allied Markets Research среднегодовой темп роста рынка робототехники в период с 2021 по 2030 год составит 11,7% [15].

Как отмечают специалисты Массачусетского технологического института (Massachusetts Institute of Technology), Азия остается крупнейшим в мире рынком промышленных роботов. 70% всех новых роботов, введенных в эксплуатацию в 2020 г., были установлены в Азии, в 2021 году – 74% роботов. Ввод роботов в эксплуатацию для крупнейшего в регионе потребителя, Китая, выросли на 51% – фактически каждый второй робот в мире устанавливается в Китае. Китайский парк роботов превысил отметку в 1 млн единиц, увеличившись на 27%. Япония является вторым после Китая крупнейшим рынком промышленных роботов: в 2021 году введение новых роботов в эксплуатацию в Японии выросло на 22%, до 47 тысяч единиц [21].

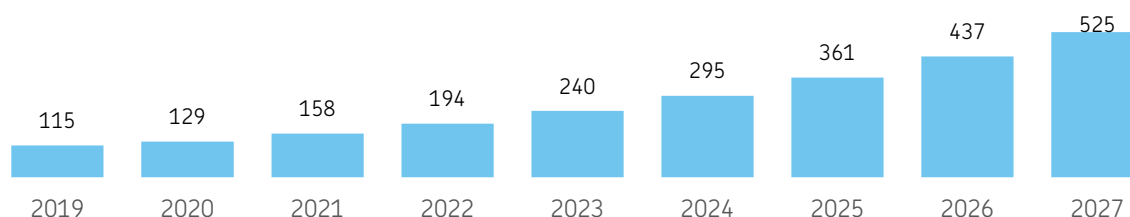
Промышленная сенсорика

Как ожидается, рынок промышленной сенсорики достигнет 31,9 млрд долл. к 2026 году при среднегодовом темпе роста 9,1% в период с 2021 по 2026 год [16]. В качестве одного из ключевых драйверов развития рынка промышленной сенсорики называется прогресс в производстве микроэлектромеханических систем (МЭМС), используемых в промышленных датчиках. В большинстве случаев микросенсоры на основе МЭМС могут достигать значительно более высоких скоростей и чувствительности по сравнению с макроскопическими сенсорами.

Промышленный Интернет Вещей

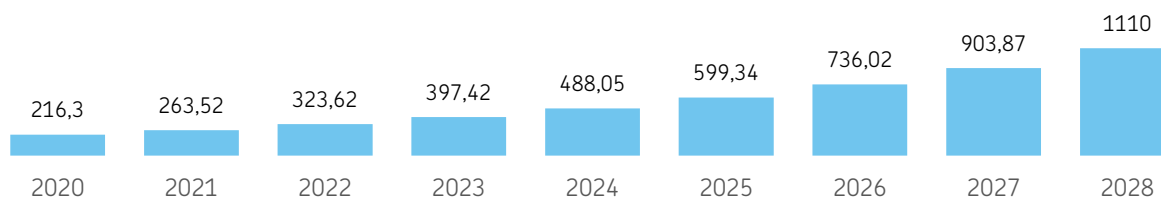
По оценкам агентства IoT Analytics размер рынка Интернета вещей вырастет в среднем на 22% до 525 млрд долл. в период с 2022 по 2027 год. Опубликованные в более раннем отчете агентства прогнозные значения были выше, чем значения из отчета 2021 года, так как ряд факторов, препятствующих росту, оказал гораздо более сильное влияние, чем предполагалось ранее. Развитию рынка препятствуют разрывы производственных цепочек, дефицит чипов и нехватка квалифицированной рабочей силы, особенно в сфере разработки программного обеспечения. Несмотря на снижение темпов роста, Интернет вещей остается актуальным технологическим направлением. Многие проекты по направлению Интернета вещей переходят в стадию внедрения – ожидается, что к концу 2022 года количество подключенных IoT-устройств во всем мире достигнет 14,5 млрд единиц.

Рисунок 5. Объем рынка Интернета вещей для компаний в 2019–2027 гг, млрд долларов



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам IoT Analytics

Рисунок 6. Рост рынка промышленного Интернета вещей, млрд долларов



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Statista [20]

По ожиданиям аналитиков Precedence Research, мировой рынок промышленного Интернета вещей в период с 2022 по 2030 года будет расти со среднегодовыми темпами роста в размере 20,47% и достигнет 1742,8 млрд

долл.

Как отмечают аналитики агентства, самым быстрорастущим сегментом рынка промышленного Интернета вещей является отрасль логистики и транспорта. В период до 2030 года совокупный темп роста отрасли логистики и транспорта ожидается в размере 25,6%. Это можно объяснить вниманием, которое компании-поставщики логистических и транспортных услуг уделяют внедрению интеллектуальных систем по управлению перевозками и активами. Кроме того, использование подключенных к Интернету вещей трекеров в дополнение к RFID-меткам в логистической отрасли еще больше поддерживает рост отрасли. Самым быстрорастущим географическим рынком промышленного Интернета вещей до 2030 года будет являться Азиатско-Тихоокеанский регион со среднегодовым темпом роста рынка в размере 26,7% [15].

Цифровое проектирование и моделирование (CAD/CAE)

По оценкам агентства Research and Markets рынок цифрового проектирования (CAE) в период 2022–2027 годов будет расти со среднегодовым темпом роста в 9,1% и достигнет 9,6 млрд долл. [18]. Рынок цифрового моделирования по оценкам агентства будет расти на 6,6% в течение прогнозируемого периода с 2020 по 2030 год [16].

Рисунок 7. Рынки цифрового проектирования в 2020 и 2027 годах



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Research and Markets

Большие данные (big data)

По оценкам агентства Markets and Markets рынок больших данных вырастет до 273,4 млрд долл. к 2026 году при совокупном годовом темпе роста рынка 11% с 2021 по 2026 год. Ключевым фактором, влияющим на высокие темпы роста рынка больших данных, является нарастающее увеличение количества данных, релевантных для ведения бизнеса и собираемых организациями – в особенности слабоструктурированных данных в социальных сетях.

Растущий объем бизнес-данных, быстрые технологические изменения и снижение средней цены продажи интеллектуальных устройств в конечном итоге способствуют созданию огромного количества структурированных и неструктурированных данных. При этом многие организации сталкиваются со значительными сложностями при управлении этим потоком данных.

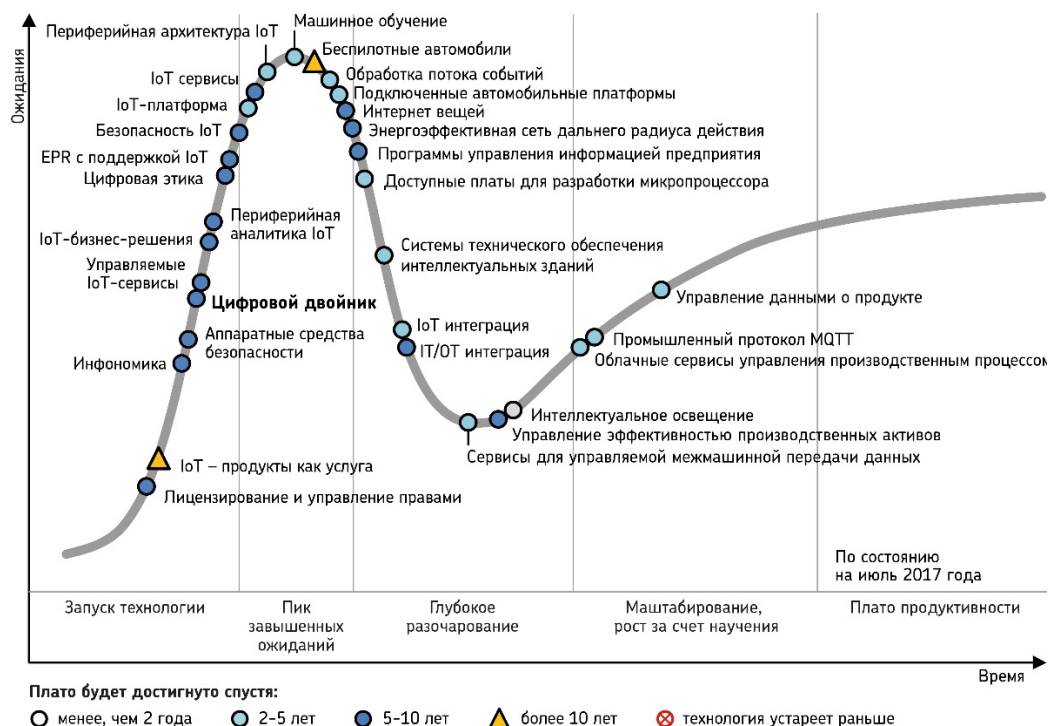
Увеличение числа стартапов и растущие государственные инвестиции в технологии больших данных и инфраструктуру в Китае, Индии и Японии станут главным фактором роста рынка больших данных в Азиатско-тихоокеанском регионе. При этом большая часть рынка больших данных в период до 2026 года будет приходиться на Северную Америку [19].

1.4 Жизненный цикл отрасли /рынка киберфизических систем, стадия зрелости

Киберфизические системы, как было отмечено ранее, определяются отдельными технологическими направлениями. Различные сегменты киберфизических систем значительно отличаются между собой по времени распространения в промышленности и общей зрелости.

Так, в 2017 году аналитики Gartner привели кривую зрелости технологий, связанных с Интернетом вещей, на которой обозначили значительное количество развивающихся технологий, подключенных к устройствам Интернета вещей.

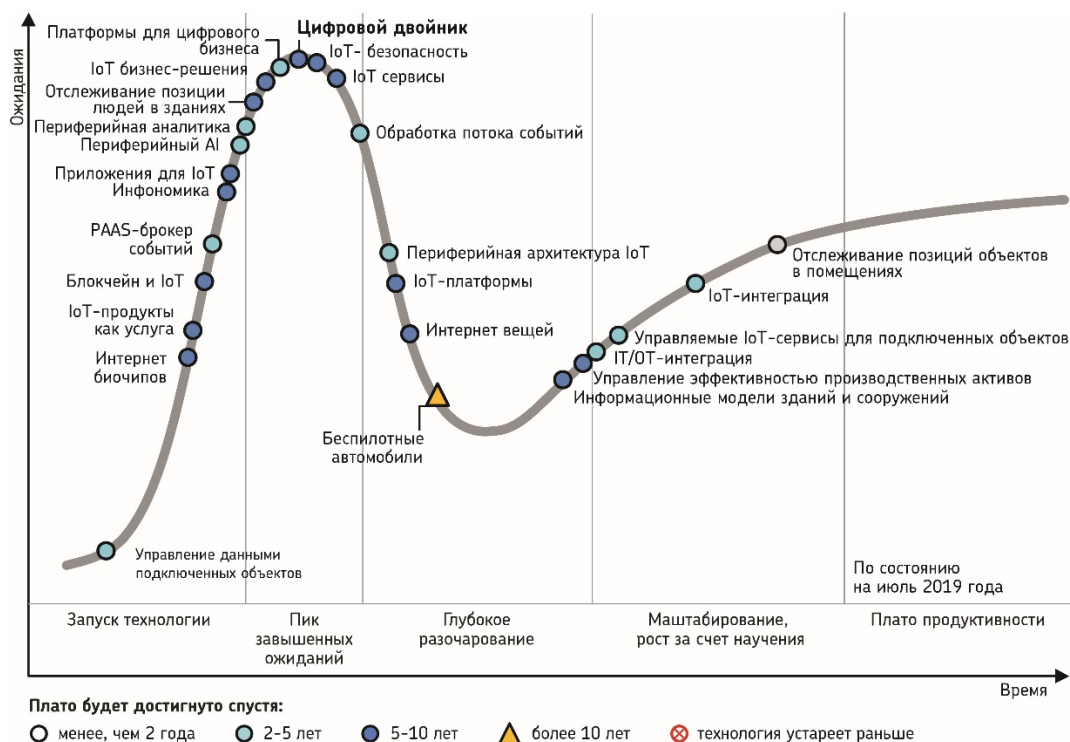
Рисунок 8. Gartner. Цикл зрелости технологий, значимых для IoT, 2017 год



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Gartner, 2017 [19]

Уже в 2019 году на цикле значимости технологий Интернета вещей большая часть технологий из стадии запуска технологий и пика завышенных ожиданий перенесены на стадию масштабирования и роста за счет научения, приближаясь к стадии продуктивности.

Рисунок 9. Gartner. Цикл зрелости технологий, значимых для IoT, 2019 год

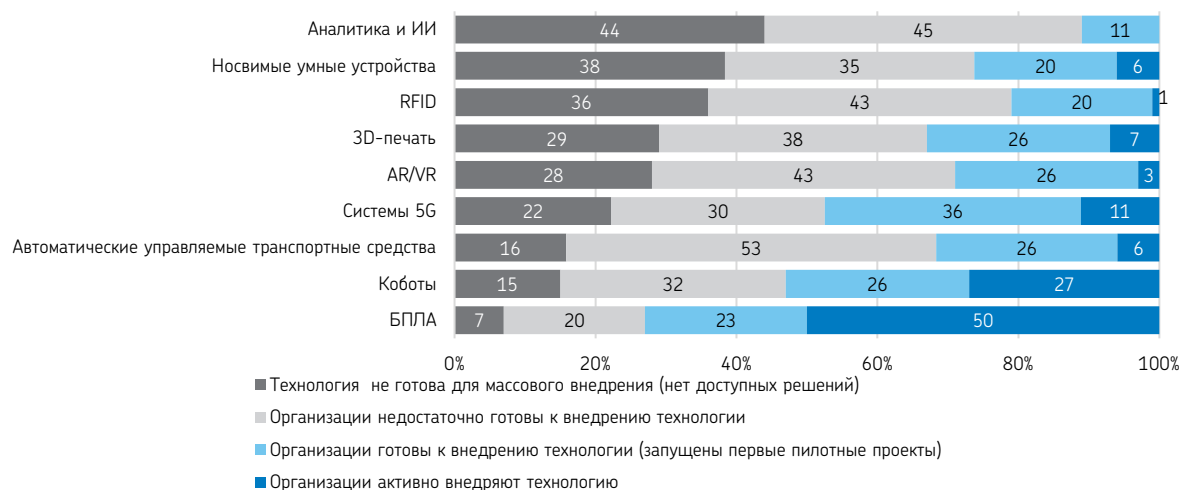


Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Gartner, 2019 [20]

Наиболее зрелый сегмент киберфизических систем – промышленная робототехника. Масштабное внедрение роботов в промышленность началось еще с 1970-х годов. В настоящее время роботами насыщены наиболее технологичные отрасли промышленности – автомобилестроение, производство электроники и пластика и др. Перспективными направлениями выступают распространение складских логистических роботов и проникновение роботов в сельское хозяйство.

Некоторые технологии, которые обычно относят к промышленному Интернету вещей, в настоящее время находятся на достаточно ранней стадии внедрения в промышленность. Согласно опросу, проведенному консалтинговой компанией PriceWaterhouseCoopers среди немецких промышленных компаний, 31% опрошенных компаний уже внедрили решения промышленного Интернета вещей, а 41% находятся на этапе развертывания [21]. Компании в настоящее время выбирают два основных пути внедрения систем промышленного Интернета вещей: приобретение платформы у крупных вендоров или собственная разработка платформы, что является более дорогостоящим, но потенциально более гибким решением.

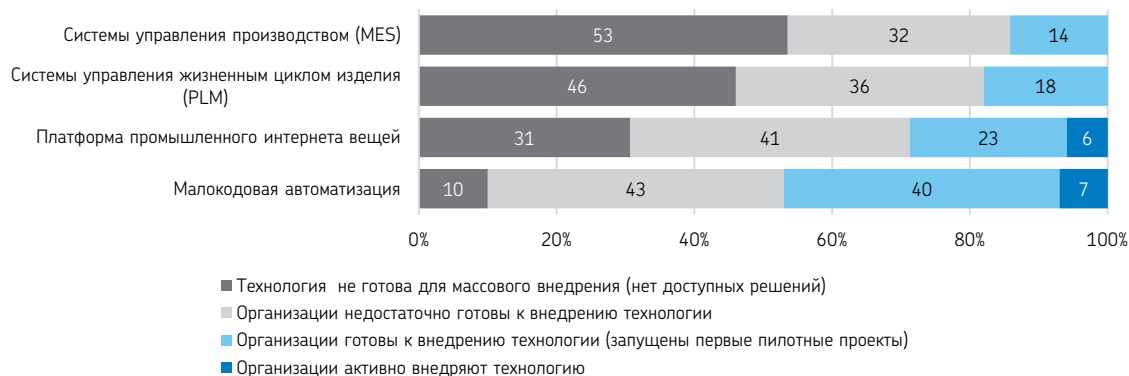
Рисунок 10. Внедрение различных технологий робототехники и Интернета вещей в немецкой промышленности



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам PWC

Следует отметить, что распространение в высокотехнологичной промышленности «коллаборативных роботов» – коботов – находится на ранней стадии, и в настоящее время определяется реальная эффективность и окупаемость устройств этого направления.

Рисунок 11. Статус внедрения передовых ИТ-решений в немецкой промышленности



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам PWC

Согласно данным опроса PWC, большая часть компаний, внедривших решения на основе платформ промышленного Интернета вещей, оценивает окупаемость таких решений не ранее, чем через 3 года.

Решения в сфере цифрового проектирования и моделирования (CAD/CAE) достаточно давно распространены в промышленности и находятся на зрелой стадии развития. Первые решения в сфере CAD/CAE были внедрены в промышленность около 60 лет назад. В то же время внедрение цифрового проектирования, в особенности в его передовых формах, остается важным направлением развития для российских компаний, зачастую внедряющих передовые технологии с определенным опозданием.

Использование больших данных в настоящее время достаточно неравномерно распространено по разным сферам экономической деятельности. Если в высокотехнологичных отраслях услуг, таких как финансы или страхование, использование больших данных уже фактически является обязательным, то в более традиционных и капиталоемких отраслях использование больших данных может находиться на самой ранней стадии.

1.5 Тренды развития рынка киберфизических систем

В исследовательской литературе вопросы трендов развития киберфизических систем рассматриваются преимущественно на уровне технологий, входящих в КФС – робототехники, Интернета вещей, больших данных и технологий цифрового проектирования и моделирования.

Робототехника

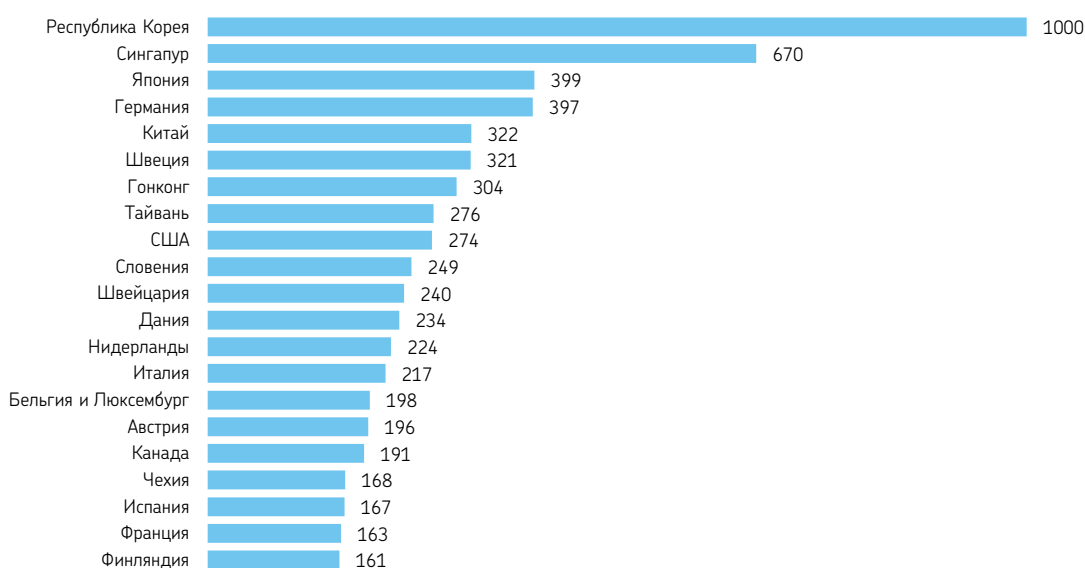
Исследователи Массачусетского технологического института в 2020 году обозначили ряд ключевых направлений развития промышленной робототехники:

- **Технологии восприятия.** На сегодняшний день ключевое ограничение надежности существующих робототехнических систем связано с недостаточным качеством как зрительного, так и осязательного восприятия роботов. Для того, чтобы роботы смогли работать в менее предсказуемых средах и в меняющихся условиях (например, с изменяемой освещенностью), необходимо развитие технологий машинного обучения для улучшения методов восприятия.
- **Технологии интеллектуального захвата.** Способность выбирать и перемещать объекты – важная задача роботов. Для маневрирования объектами в малоопределенных производственных условиях или работы с деталями разного размера и формы требуется высокий уровень искусственного интеллекта у роботов. Несовершенство методов захвата объектов остается одним из наиболее важных ограничивающих факторов роботизации производств.
- **Безопасные коллаборативные роботы.** Для общего увеличения безопасности и обеспечения совместной работы необходимы решения, интегрирующие функции прогнозирования поведения человека в планирование маршрута робота и отслеживание ситуации в динамических рабочих областях.
- **Более совершенная навигация для автоматически управляемых транспортных средств.** Для совершенствования работы автономных роботов необходимо совершенствование и распространение методов одновременной локализации и картирования в навигации. В настоящий момент технологии находятся на ранней стадии развития, в связи с чем трудно оценить масштаб ее реального воздействия на производство.
- **Упрощенные интерфейсы и техники программирования.** Программирование роботов – сложная и дорогостоящая задача, требующая времени и опыта. Необходимо развитие технологий упрощенного программирования роботов, не требующих высоких навыков в программировании.
- **Моделирование.** Необходимо совершенствование методов цифрового моделирования для снижения затрат на запуск и перенастройку производственных линий.
- **Дизайн, ориентированный на работников.** Необходимы дополнительные исследования того, как непосредственная деятельность работников учитывается в процессе проектирования робототехники и как учет человеческого фактора влияет на общую производительность.
- **Облачные системы.** Облачные системы создают возможность объединять и контролировать

операции на заводе с помощью данных. Однако такая возможность слабо реализована на практике, затраты на подобные решения высоки, а степень полезности получаемых данных не до конца ясна, в связи с чем необходимо обеспечить получение значимой информации.

При этом стоит учитывать региональную и отраслевую зависимость тенденций развития рынка робототехники. Распределение промышленных роботов по регионам и странам напрямую связано с интенсивностью их использования в различных отраслях промышленности. Наибольшая концентрация роботов отмечена в странах, лидирующих в производстве автомобилей и электронных устройств. К их числу относятся Сингапур, Республика Корея, Япония и Германия.

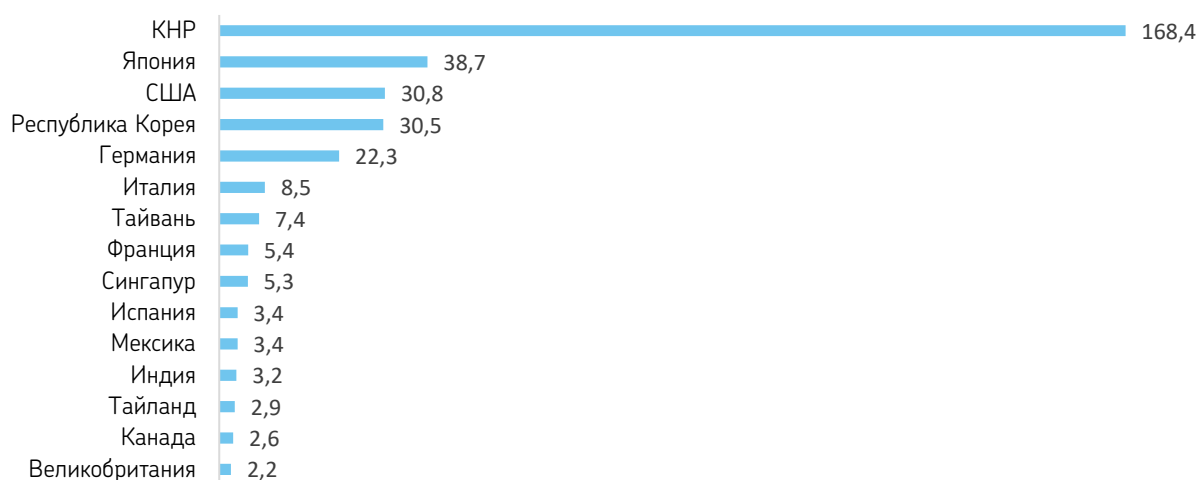
Рисунок 12. Количество роботов на 10 000 работников по ряду стран мира, единиц.



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам IFR

По общему числу установок промышленных роботов лидирует Китайская Народная Республика.

Рисунок 13. Ввод в эксплуатацию новых промышленных роботов в год по странам в 2021 году, тысяч единиц



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам IFR

Уровень роботизации также тесно связан с производимой номенклатурой устройств в разных отраслях – так, уровень роботизации в производстве электрооборудования в Республике Корея и Германии различается на порядок.

Таблица 1. Уровень роботизации по различным странам и отраслям промышленности

Страна	Уровень по отраслям							Уровень по отраслям обрабатывающей промышленности							
	Все отрасли	Сельское хозяйство	Строительство	Образование	Энергетика	Горная промышленность	Обрабатывающая промышленность	Автомобилестроение	Электротехническая промышленность	Производство пластиков	Металлургия	Пищевая промышленность	Производство стекла	Целлюлозно-бумажная промышленность	Текстильная промышленность
Корея	10,1	0,2	0	0,2	0,1	1,6	47	192,6	112,8	21	6	3	3	0	0
Япония	5,5	0,4	0,2	0,2	0,2	0,1	33	140	52,8	29	12	4	4	2	0
Тайвань	5,2	–	–	0,1	0,5	0,3	9,4	25,6	23,3	6	2	1	0	0	1
Германия	4,6	0,2	0,1	0,8	0,1	0,1	21	108,7	9,5	20	10	8	–	2	2
Италия	3,3	0,1	0,2	0,1	0,1	0	15	106,3	5,8	25	14	13	7	2	1
Швеция	2,4	1,6	0,5	0,4	–	–	8,9	58,2	4,5	10	5	5	2	0	0
США	1,5	0,1	0	0,1	0	0	14	116,3	21,7	10	6	5	1	0	0
Канада	0,5	0	0	0,1	0	0	4	38,5	2	2	1	3	0	0	–
Мексика	0,4	–	0	0	–	0	2,2	14,9	0,8	3	1	0	0	0	–

Источник: Инфраструктурный центр «Технет» СПбПУ по материалам МВФ [22]

Интернет Вещей

Исследователи IOT Analytics выделяют 16 макрофакторов, которые будут влиять на развитие рынка Интернета Вещей в 2022–2027 годах.

Таблица 2. Факторы, влияющие на развитие рынка Интернета вещей

Фактор	Влияние
Экономические факторы	
Снижение темпов экономического роста	Негативное
Рост цен на факторы производства	Негативное
Снижение ожиданий от эффектов внедрения прорывных технологий	Умеренно негативное
Нестабильность цепочек поставок	Умеренно позитивное
Политические факторы	
Возвращение производств в развитые страны	Позитивное
Нехватка рабочей силы	Негативное
Европейский закон о данных	Умеренно негативное
Экологические факторы	
Следование целям устойчивого развития	Позитивное
Сокращение использования ископаемого топлива	Позитивное
Эпидемиологическая ситуация	Позитивное
Технологические факторы	
Развитие технологий искусственного интеллекта	Позитивное
Облачные решения для Интернета вещей	Позитивное

Развитие технологий связи для Интернета вещей	Позитивное
Увеличение числа инцидентов, связанных с кибербезопасностью	Негативное
Нехватка чипов	Негативное

Источник: Инфраструктурный центр «Технет» СПбПУ по материалам IoT Analytics

Также агентство IOT Analytics выделило 10 главных трендов в сфере Интернета вещей в 2022 году [23]:

1. **Интернет вещей как технология устойчивого развития.** Возможности интеллектуальных подключенных устройств для задач мониторинга окружающей среды, территориального управления и оптимизации энергопотребления известны достаточно давно. Но коммерческая ценность этих приложений была ограничена и до сих пор отодвигалась на второй план большинством крупных игроков в сфере Интернета вещей. Учитывая растущее внимание к формированию «зеленой» экономики и смягчению последствий изменения климата, технологии Интернета вещей могут занять важное место среди «зеленых» решений для компаний и государственных органов.
2. **От облачных вычислений к периферийным.** В настоящее время определяется архитектура будущего рынка, в котором компании могут привязывать решение в области периферийных вычислений к оборудованию конкретных поставщиков, а также развивать решения в сфере периферийных вычислений, независимых от вендоров аппаратного обеспечения.
3. **Инициативы промышленного Интернета вещей трансформируют производство.** Промышленный Интернет вещей позволяет выйти за рамки систем по сбору данных для машинных операций за счет оперативного предоставления данных об оборудовании, необходимых для своевременного технического обслуживания, а также данных для решения конкретной бизнес-задачи.
4. **Приложения cloud-native.** Компании, вложившиеся в облачную цифровую инфраструктуру, ищут новые способы повышения ее эффективности и увеличения функционала. Поскольку облачные решения становятся нормой для многих компаний на уровне инфраструктуры, платформы или программного обеспечения, в отрасли формируется новая группа приложений, разработанных и оптимизированных для облачного масштаба и производительности, что повысит надежность облачных решений и сократит время их выхода на рынок.
5. **Гиперавтоматизация.** Пандемия коронавирусной инфекции, вопросы обеспечения безопасности работников и разрастающаяся нехватка рабочей силы усиливают тенденции гиперавтоматизации – внедрение решений на основе искусственного интеллекта и роботизированная автоматизация процессов для увеличения эффективности предприятий.
6. **Распространение архитектуры граничных периферийных вычислений для искусственного интеллекта.** Перед компаниями встает вопрос – где проводить вычисления в сфере искусственного интеллекта, в облаке или на периферийных устройствах. До сих пор периферийные приложения с использованием искусственного интеллекта работали на вычислительно- и энергоемких периферийных устройствах, таких как промышленные компьютеры и пограничные маршрутизаторы. Постепенно развивается переход к архитектуре граничных вычислений. Благодаря удешевлению периферийных микроконтроллеров и общему увеличению эффективности алгоритмов искусственного интеллекта становится возможным осуществлять распределенные граничные вычисления.
7. **Внедрение «невидимого искусственного интеллекта».** Благодаря прогрессу в сфере увеличения вычислительной мощности и удешевления вычислительных устройств, развития Интернета, доступности сенсоров, улучшению сложных алгоритмов и моделей машинного обучения, технологии искусственного интеллекта начинают внедрять практически во все отрасли. Искусственный интеллект универсален – он охватывает все отрасли и влияет практически на все рабочие звенья – от рядового сотрудника до генерального директора.
8. **Виртуальная и дополненная реальность.** Развитие удаленного управления операциями способствовало интеграции IoT с технологиями виртуальной и дополненной реальности и технологиями имитации окружающей среды.
9. **Готовность к использованию 5G для Интернета вещей.** Сети 5G для промышленных и

коммерческих целей применяются в частных сетях промышленных компаний. Примерами таких сетей можно назвать беспроводную сеть 5G для Volkswagen, созданную компанией Nokia на главном заводе автопроизводителя в Вольфсбурге.

10. **Безопасный удаленный доступ к активам.** Компании, предоставляющие удаленный доступ к своему оборудованию, могут получить ряд преимуществ, в том числе поддержку со стороны поставщиков оборудования, которые могут удаленно устранять неполадки и анализировать данные об устройствах в режиме реального времени. Дополнительным преимуществом может стать доступ к более дешевой удаленной рабочей силе из стран с более низкой заработной платой. Но с расширением доступа увеличивается количество кибератак, поэтому компании увеличивают свои расходы на кибербезопасность. Три тенденции в области кибербезопасности в 2022 году — это распространение технологий отслеживания активов (Asset Visibility), технологии глубокой проверки активов и «архитектуры нулевого доверия».

Цифровое проектирование и моделирование

В 2022 году компания Business Advantage Group провела опрос среди машиностроительных компаний, посвященный определению основных тенденций в сфере цифрового проектирования и моделирования [24]. Исследователи компании выделили 20 основных технологических направлений, развитие которых является важным для отрасли, четыре из которых были включены в отчет впервые.

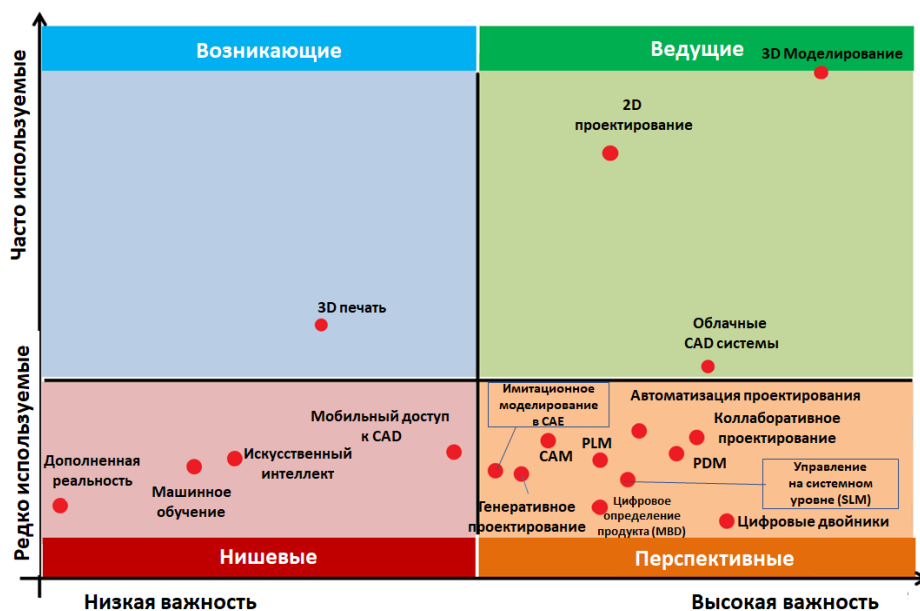
Рисунок 14. Актуальные тенденции в сфере CAD/CAE



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Business Advantage Group

По результатам опроса аналитики Business Advantage Group сгруппировали тенденции по критериям использования и важности для развития рынка. К числу перспективных, но еще относительно малоиспользуемых технологий были отнесены технологии генеративного проектирования, коллаборативного проектирования, автоматизации проектирования, цифровые двойники и ряд иных.

Рисунок 15. Распределение технологических трендов в CAD по важности и используемости.



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Business Advantage Group

Большие данные

В исследовании Financesonline выделено 11 тенденций в сфере больших данных на 2022–2023 годы [25]:

1. **Технологии больших данных становятся ключевыми для процесса цифровой трансформации компаний.** Распространение технологий Интернета вещей, моделей инфраструктуры-как-услуги и искусственного интеллекта формирует массивы больших данных, нуждающихся в обработке. Предприятиям предстоит проделать большой объем работы по оптимизации использования больших данных на своих серверах. Так, американские компании теряют до 3,1 триллиона долл. в год из-за низкого качества накопленных больших данных.
2. **Большие данные будут активно использоваться для исследований изменения климата.** Накопленные данные, свободные от предвзятой интерпретации, будут иметь решающее значение для оценки изменения климата. Большие данные планируется генерировать разрозненными исследовательскими центрами с разной специализацией по всему миру.
3. **Аналитика данных будет чаще использоваться в режиме реального времени.** Организации, специализирующиеся на природных катаклизмах, а также финансовые организации будут больше применять большие данные совместно с искусственным интеллектом, роботизированной автоматизацией процессов и машинным обучением для прогнозирования изменений в режиме реального времени.
4. **Большие данные будут чаще использоваться в рамках модели «Данные-как-услуга», в том числе малыми предприятиями.** Большие данные станут доступны для любых клиентов и с любого устройства из любой точки мира за невысокую стоимость.
5. **Использование больших данных позволит находить новые точки роста.** Аспекты ведения бизнеса, такие как реклама и социальные сети, управление цепочками поставок и техническая поддержка будут интегрированы друг с другом за счет больших данных.
6. **Увеличение значимости технологий больших данных для поиска новых медицинских препаратов.** Доступ к обширным библиотекам больших данных, включающих в себя информацию о ДНК, медицинские данные пациентов, научные исследования и данные по другим смежным областям позволит искусственному интеллекту выделять новые закономерности для создания новых лекарств.

7. **Технологии беспилотных автомобилей будут развиваться за счет использования больших данных.** С помощью аналитических инструментов массивы больших данных о трафике будут способствовать планированию маршрутов и управлению транспортной системой.
8. **Сферы использования больших данных будут расширяться от моделирования нефтяных месторождений до исследований в сфере квантовой физики.**
9. **В сфере технологий обработки естественного языка будет достигнут значительный прогресс.** Технологии обработки естественного языка позволят взаимодействовать с интеллектуальными системами, при этом компании смогут получить доступ к качественному анализу настроений пользователей.
10. **Демократизация в сфере управления данными.** Законы, аналогичные Общему регламенту по защите данных (GDPR), расширят возможности потребителей и защитят права персональных данных, а также предоставят преимущества компаниям, ведущим открытую и честную политику работы с данными клиентов.
11. **Вопросы обеспечения кибербезопасности останутся острыми.** Проблемы кибербезопасности будут увеличиваться соразмерно объему и сложности используемых данных.

ГЛАВА 2. БАРЬЕРЫ, РИСКИ И НОРМАТИВНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ РАЗВИТИЯ РЫНКА

В рамках данной главы рассмотрены барьеры и риски развития сегментов киберфизических систем (элементы физической и программной среды). Также представлены результаты анализа нормативного правового регулирования, в том числе государственных программ поддержки развития направления киберфизических систем по НИРам и НИОКРам и текущих достижений в области национальной и международной стандартизации.

2.1 Барьеры развития киберфизических систем

В данном разделе рассмотрены барьеры для технологий, являющихся элементами физической и программной среды киберфизических систем с учетом их особенностей.

Барьеры развития робототехники

Исследователи MIT в аналитическом докладе «Состояние промышленной робототехники» [26] выделили основные вызовы, стоящие на пути развития промышленной робототехники:

- **Высокая стоимость интеграции.** Несмотря на то, что оборудование робота стало дешевле, стоимость робота составляет небольшую часть общей стоимости внедрения автоматизации на производственной линии. По словам представителя крупной фирмы-интегратора: «Роботы сейчас недороги, а интеграция – нет». Долгим, трудным и дорогостоящим является не только начальный процесс интеграции. Даже небольшие изменения в производственной линии часто требуют привлечения интегратора для перепроектирования и перепрофилирования рабочих элементов роботов в соответствии со спецификациями новых задач.
- **Отсутствие стандартов.** Отсутствие стандартизации во многих аспектах робототехники мешает некоторым компаниям полностью использовать потенциал перспективных технологий или включать новые типы роботов в производственные линии. Некоторые компании в течение многих лет разрабатывали собственные системы, которые они предпочли бы использовать и дальше. Другие, часто небольшие компании, проектируют производственные линии или закупают новые технологии с нуля. Для каждого типа роботов может потребоваться знание разных языков программирования, интерфейсов или протоколов связи.
- **Недостаточная гибкость.** Современные робототехнические технологии не всегда могут быть быстро перепрофилированы, что ограничивает потенциал использования роботов.
- **Лучший баланс скорости и безопасности.** Роботы для совместной работы по своей сути более безопасны, но во многих ситуациях их использование остается ограниченным. Крупные компании предпочитают скорость операций использованию коллаборативных роботов тем более, что «коботы» не являются оптимальным решением для широкого спектра задач.
- **Необходимость усовершенствования технологий, лежащих в основе робототехники.** Для инвестиций и массового внедрения автоматизированных промышленных операций имеют решающее значение высокая надежность, быстрая интеграция и устранение технологических узких мест, связанных с сенсорами, технологиями восприятия и захвата объектов.

В качестве ключевых барьеров развития промышленной робототехники в России можно определить общую дороговизну кредитов для промышленности, сдерживающей технологическое перевооружение предприятий, большое значение государственных предприятий, не испытывающих жесткого конкурентного давления и дефицит инженерных компетенций по внедрению робототехнического оборудования. Также по экспертным оценкам в последние годы возрастают риски, связанные с поставками относительно дешевого китайского оборудования, не самого высокого качества, что приводит к некачественным решениям и «историям провала» [27]. В 2022 году официальные поставки роботов со стороны большинства зарубежных производителей стали для российских предприятий практически невозможными.

Барьеры развития промышленной сенсорики промышленного Интернета вещей

Аналитики Marketsandmarkets в качестве барьера для развития промышленной сенсорики выделяют [14] два основных фактора:

- Во-первых, **установка сенсорных сетей все еще остается дорогостоящей**. Хотя стоимость сенсорных систем снижается, она все еще достаточно высока, чтобы влиять на скорость внедрения в промышленности. Устройства и сеть проводов должны устанавливаться профессионально и соответствовать отраслевым стандартам и практикам владельцев и операторов.
- Во-вторых, к **точности работы продвинутых датчиков в различных отраслях промышленности применяются различные требования**. Например, параметры измерения температуры, давления, расхода и положения в автомобильной промышленности отличаются от параметров в нефтегазовой отрасли; поэтому требования к производительности датчиков становятся критически важными для сложных приложений.

Консалтинговая компания Mckinsey в исследовании 2021 года, посвященном развитию Интернета вещей, выделяет ряд барьеров на пути более масштабного использования Интернета вещей и его влияния на организации:

- **Проблемы в управлении изменениями.** Компании и государственные органы зачастую рассматривают внедрение IoT как технологический проект, а не как трансформацию операционной модели. В таких условиях внедрение IoT может осуществляться под руководством ИТ-отдела без учета необходимых изменений в процессах стратегического управления, управления персоналом и управлении производительностью. Это может приводить к разочаровывающим результатам, особенно в сочетании с фрагментарной покупкой решений IoT, даже в рамках одной компании или государственного ведомства. Для того, чтобы внедрение Интернета вещей принесло пользу, необходимо чтобы участники из различных департаментов сотрудничали между собой для изменения принятых бизнес-процессов и рабочей культуры организации.
- **Функциональная совместимость (интероперабельность).** Несмотря на прогресс в области Интернета вещей, решения в этой сфере чаще всего состоят из множества закрытых экосистем от различных производителей, слабо интегрируемых между собой. Дополнительную сложность представляет интеграция между собой устаревших ИТ-систем, различных архитектур данных и многочисленных датчиков, которые используют различные языки программирования.
- **Установка.** Многие потребители, корпоративные заказчики и государственные органы указывают на установку оборудования в качестве самого затратного компонента развертывания решений IoT. Из-за проблем с функциональной совместимостью почти каждая крупномасштабная установка требует настройки, а в некоторых случаях даже разработку полностью индивидуального решения. В случае проектов «браунфилд», в которых реализуется от 80 до 90 процентов развертываний, ситуация обычно еще более сложная. Такие кажущиеся простыми задачи, как установка безопасного подключения (без создания помех), модернизация старых устройств (без отключения их от сети на слишком долгое время) или подключение к существующим системам (без необходимости перестраивать с нуля) увеличивают время, сложность и стоимость, которые препятствуют масштабному развертыванию.
- **Кибербезопасность.** Потребители, корпоративные клиенты и правительства все больше беспокоятся о кибербезопасности IoT, поскольку растущее число подключенных устройств увеличивает число уязвимых точек для использования хакерами. Чтобы решить эту проблему, система безопасности должна быть построена с нуля на каждом уровне системы.

Барьеры развития цифрового проектирования и моделирования

По итогам опроса машиностроительных компаний в 2022 году (Business Advantage Group) [20] был выделен ряд барьеров для внедрения передовых технологий цифрового проектирования и моделирования. Лидирующими барьерами являются нехватка технических компетенций, вопросы безопасности и высокая стоимость решений в сфере цифрового проектирования и моделирования.

Рисунок 16. Барьеры внедрения CAD/CAE в организациях (%)



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Business Advantage Group

Барьеры развития больших данных

Аналитики Marketsandmarkets выделяют[28] два ключевых барьера для развития больших данных:

- **Обособленные базы данных.** Проблема с любыми данными заключается в том, что в любой организации они хранятся в разных местах и в разных форматах. С большими данными проблема разрозненности становится еще более серьезной. Это связано не только с огромным объемом данных, но и с разнообразием их внутренних и внешних источников, а также с различными применимыми требованиями безопасности и конфиденциальности. Устаревшие системы также оказывают влияние, затрудняя или даже делая невозможной консолидацию данных таким образом, чтобы это было полезно для аналитики.
- **Низкое качество данных.** Еще одна серьезная проблема с большими данными заключается в том, что они не могут быть полностью непротиворечивыми. Данные подвержены ошибкам. Аналитические алгоритмы и приложения ИИ, основанные на больших данных, могут давать плохие результаты, когда проблемы с качеством данных проникают в системы больших данных. Такие проблемы могут стать еще более значительными по мере того, как специалисты по управлению данным и аналитике будут подключать все большее число разнообразных данных.

2.2 Риски развития киберфизических систем

На основании проведенного анализа опубликованных материалов можно отметить, что большинство исследователей в качестве наиболее крупной проблемы киберфизических систем и родственного концепта Интернета вещей выделяют вопросы обеспечения безопасности.

Как указывают авторы доклада NIST [5], обеспечение кибербезопасности в киберфизических системах отличается от безопасности в обычных ИТ-системах, как минимум в трех вопросах: сложности «ландшафтов» развертывания кибербезопасности, возможности кибератак на физические системы, а также возможность физических атак на КФС.

Во-первых, количество и разнообразие компонентов в киберфизических системах создает серьезные проблемы. Добавление сетевого подключения к повседневным объектам увеличивает количество точек атаки, нуждающихся в защите. Различия в вычислительной мощности, системной памяти, пропускной способности сети, физической доступности, возможности обновления и других факторах среди разнородных подключенных элементов КФС требуют применения индивидуальных подходов к безопасности.

Во-вторых, интеграция цифровых и физических компонентов означает, что атака на ИТ-системы может быть использована для получения контроля над важными физическими системами для медицины, критически важной инфраструктуры, безопасности жизни и других функций с возможностью причинения ущерба, в том числе – смертельного. Применительно к техническому проектированию это также означает, что положения о цифровой кибербезопасности и конфиденциальности нельзя рассматривать независимо от положений о физической безопасности,

отказоустойчивости и надежности системы. Они должны рассматриваться как взаимозависимые, с учетом компромиссов и взаимодействий, оцениваемых в любом комплексном процессе проектирования и страхования киберфизических систем.

В-третьих, физические компоненты сетевых систем CPS/IoT обеспечивают как новые векторы угроз, так и новые средства борьбы с угрозами. Примеры новых векторов угроз включают использование фонового шума или ультразвука для атаки на аудиоинтерфейсы интеллектуальных систем или скрытые функции для бэкдор-атак на распознавание изображений. Примеры новых средств борьбы с угрозами включают в себя использование информации о физических свойствах киберфизической системы для получения сведений о том, было ли логическое состояние скомпрометировано в результате сбоя или атаки.

Отдельным вопросом является дальнейшее развитие законодательства о критической информационной инфраструктуре. Данный вопрос актуален для всех стран. В России компании оказываются в ситуации двойного давления: из-за ужесточения международных санкций закупки иностранного ПО и элементной базы зачастую стали невозможны, при этом ужесточается государственный контроль за закупками ПО для объектов критической инфраструктуры и ее переводом на отечественное программное обеспечение.

Проблема возможного лишения доступа к необходимому программному обеспечению, оборудованию, запасным частям и техническому обслуживанию предполагает коммерческие риски, а в случае с государственными организациями, в особенности участвующими в обеспечении обороноспособности страны, вопрос надежности доступа к компонентам киберфизических систем может стать ключевым.

Вероятно, необходимость развития КФС в какой-то момент потребует изменения нормативной базы и вынесения закупок устройств из дружественных стран в отдельную категорию, и/или создания нормативной базы для закупок технологических компонентов в рамках параллельного импорта, но на сегодняшний день ситуация неопределенная.

2.3 Нормативное правовое регулирование, в том числе анализ государственных программ поддержки развития направления киберфизических систем по НИРам и НИОКРам

В рамках текущего раздела представлены результаты анализа нормативного правового регулирования и государственной политики в области поддержки развития направления киберфизических систем по НИРам и НИОКРам.

Основной фокус мер государственного регулирования в настоящее время сосредоточен на создании или усилении конкурентных преимуществ с использованием технологий киберфизических систем, а также обеспечении кибербезопасности государственного сектора, объектов инфраструктуры и промышленности. Инициативы в области киберфизических систем и смежных технологий реализуются во всем мире. Сразу несколько таких программ существуют в США, странах Европы и крупнейших государствах Азиатско-Тихоокеанского региона. В рамках обзора нормативно правового регулирования в области киберфизических систем были рассмотрены программы и инициативы таких стран как США, Европейский Союз, Великобритания, Германия, КНР и Российская Федерация.

В рамках государственной политики США, направленной на поддержку и развитие киберфизических систем, реализуется исследовательская программа «Киберфизические системы» (The Cyber-Physical Systems research program, CPS) [29], инициированная Национальным научным фондом (The National Science Foundation, NSF). Программа направлена на поддержку исследований инженерных систем с бесшовной интеграцией кибер- и физических компонентов, таких как вычисления, системы управления, сетевого взаимодействия, обучения, автономности, безопасности, конфиденциальности и проверки, применимых в различных областях. Эта программа также способствует формированию исследовательского сообщества (Cyber-Physical Systems Virtual Organization, CPS-VO), которое стремится к развитию образования и просветительской деятельности в области киберфизических систем, а также ускорению перехода от исследований в данной области к реальному внедрению технологий [30]. В настоящее время в рамках Программы осуществляется ежегодная грантовая поддержка для реализации от 20 до 30 проектов на общую сумму 32,4 млн долл. [31]. Суммы финансирования варьируются для малых проектов (приблизительно 15 малых проектов с финансированием до 500 000 долл., на срок до 3 лет), средних проектов

(приблизительно 15 средних проектов с финансированием от 500 001 до 1 200 000 долл., на срок до 3 лет) и 1 передовой проект (общая сумма от 1 200 001 до 7 000 000 долл., на срок от 4 до 5 лет).

Поддержка проектов осуществляется в рамках сотрудничества с несколькими агентствами Правительства США, включая Управление науки и технологий Министерства внутренней безопасности США (DHS Science and Technology Directorate, DHS S&T) [32; 33]; Федеральное управление автомобильных дорог Министерства транспорта США (Federal Highway Administration, FHWA; United States Department of Transportation, DOT) [34], несколько Национальных институтов здравоохранения (National Institutes of Health, NIH) [35], включая Национальный институт биомедицинской визуализации и биоинженерии (National Institute of Biomedical Imaging and Bioengineering, NIBIB) [36], Национальный институт онкологии (National Cancer Institute, NCI) [37], Управление исследований поведенческих и социальных наук (Office of Behavioral and Social Sciences Research, OBSSR) [38] и Национальный центр развития трансляционных наук (National Center for Advancing Translational Sciences, NCATS) [39], Национальный институт продовольствия и сельского хозяйства Министерства сельского хозяйства США (The U.S. Department of Agriculture, National Institute of Food and Agriculture, USDA NIFA) [40].

Так, например, в рамках сотрудничества с управлением науки и технологий Министерства внутренней безопасности США (DHS S&T) реализуется проект в области безопасности киберфизических систем (The Cyber Physical Systems Security project (CPSSEC)) [33]. В рамках проекта осуществляется совместная поддержка исследований и разработок направленных на решение фундаментальных и сквозных проблем. В настоящее время проект CPSSEC сосредоточен на решениях в области безопасности для таких направлений как автомобилестроение, медицинские устройства, системы управления зданиями, а также безопасность Интернета вещей.

В *Европейском Союзе* на сегодняшний момент реализуется рамочная программа «Горизонт Европа» (Horizon Europe) 2021-2027 гг., являющаяся продолжением ранее существовавшей рамочной программы по научным исследованиям и инновациям «Горизонт 2020» (Horizon 2020). Бюджет программы на весь период составляет 95,5 млрд евро, что на ~20 млрд евро больше, чем бюджет предыдущей программы [41]. В рамках программ реализуется ряд проектов по направлению киберфизических систем (некоторые проекты, начатые в рамках программы Horizon 2020 еще продолжаются).

Один из проектов – Центры цифровых инноваций и совместная платформа для киберфизических систем (Digital innovation hubs and collaborative platform for cyber-physical systems (HUBCAP)) – направлен на повышение доступности для малого и среднего бизнеса цифровых инноваций с использованием модельно-ориентированного проектирования (model-based design, MBD) для киберфизических систем. В рамках проекта объединены семь центров цифровых инноваций (Digital Innovation Hubs (DIHs)), расположенные в семи европейских странах, каждый из которых встроен в свою региональную инновационную экосистему. На базе HUBCAP малый и средний бизнес может получить доступ к экспериментальной базе, обучению в различных областях применения киберфизических систем, получить возможность поиска инвестиций, а также установления новых деловых связей. Это обеспечивается облачной открытой платформой для совместной работы с возможностью «песочницы», которая помогает пользователям опробовать новые технологии. Финансирование проекта составляет 8 383 587,50 евро (2020-2022 гг.) [42].

Еще один проект в данной области направлен на обеспечение возможности создания продуктов киберфизических систем, а также их использование во всех отраслях промышленности – Киберфизические системы для Европейского Союза (Cyber Physical Systems for European Union (CPS4EU)) [43]. В рамках проекта реализуется обмен знаниями и формирование инноваций в ключевых секторах экономики за счет объединения исследовательских центров мирового класса, малых и средних предприятий (FHG, CEA, DLR, INRIA, KIT, CNRS) и крупных компаний (BMW, VALEO, THALES, TRUMPF, RTE, ABENGOA, LEONARDO, SCHNEIDER ELECTRIC). Финансирование проекта составляет 52,4 млн евро (2019-2022 гг.) [44]. По итогам реализации проекта представлены 15 демонстраторов разработок, охватывающих автомобилестроение, промышленную автоматизацию и другие ключевые отрасли промышленности.

Отчасти область киберфизических систем рассматривается и поддерживается в рамках совместной инициативы «Ключевые цифровые технологии» (The Key Digital Technologies Joint Undertaking, KDT JU) [45]. Инициатива реализуется в продолжение ранее существовавшей программы Электронные компоненты и системы для

европейского лидерства (Electronic Components and Systems for European Leadership Joint Undertaking, ECSEL JU) [46], и существует в форме государственно-частного партнерства с целью развития исследований, разработок и инноваций. В рамках инициативы финансируются проекты, направленные на обеспечение экспертных знаний мирового уровня в ключевых передовых технологиях, необходимых для конкурентоспособного лидерства Европы в эпоху цифровой экономики. Инициатива поддержана ассоциациями: The European Technology Platform on Smart Systems Integration (EPoSS) [47], Advanced European Network of E-infrastructures for Astronomy with the SKA (AE-NEAS) [48] и Inside Industry Association [49], представляющими участников из областей микро- и нанoeлектроники, интеллектуальных интегрированных систем и встроенных/киберфизических систем. Подготовленная данными ассоциациями Стратегическая программа исследований и инноваций для электронных компонентов и систем (The Electronic Components and Systems (ECS) Strategic Research and Innovation Agenda (SRIA)) [50] стала основой для формирования предложений на конкурсы KDT JU [51]. Также инициатива KDT JU реализуется при поддержке Европейской комиссии и государств-участников программы Horizon Europe [52]. Общий объем проектов НИОКР должен составить более 7 млрд евро, до 1,8 млрд евро, поступят от государств-участников. Основными темами поддержки проектов в 2022 году стали: промышленная цепочка поставок для кремниевой фотоники, разработка настраиваемых и специализированных процессоров с открытым исходным кодом RISC-V и интеллектуальные электронные системы, поддерживающие цели Green Deal (Зеленый пакт для Европы).

В 2021 году, в год принятия программы Horizon Europe, была принята программа «Цифровая Европа» (The Digital Europe Programme, DIGITAL) 2021–2027 гг., предназначенная для преодоления разрыва между исследованиями в области цифровых технологий и внедрением их на рынок. Общий бюджет программы составляет 7,5 млрд евро [53]. Обе эти программы согласованы между собой: программа Horizon Europe предполагает инвестирование в исследования и инновации, а программа Digital Europe, опираясь на полученные результаты, направлена на создание необходимой цифровой инфраструктуры.

На сегодняшний момент поддержка развития киберфизических систем осуществляется и в других странах Европы. Например, в *Великобритании* принята Национальная киберстратегия (National Cyber Strategy 2022) [54], отражающая планы страны до 2025 и в перспективе до 2030 года. Данный документ, основывается на положениях Национальной киберстратегии 2016–2021 годов, но в нем отражены более масштабные цели по укреплению положения Великобритании как ведущей кибердержавы. В рамках стратегии большое значение придается критическим технологиям и инфраструктуре, лежащим в основе киберпространства, а также уделяется внимание поддержке британских киберкомпаний в развитии на внутреннем рынке и конкуренции на международном рынке (107 инновационных компаний), активизации международной деятельности по формированию будущего киберпространства и влиянию на него. Настоящая стратегия предполагает реализацию исследований в области проектирования надежных микропроцессорных систем, безопасности операционных технологий и криптографии. В рамках стратегии планируется создание национальной лаборатории по безопасности операционных технологий в качестве нового центра передового опыта, деятельность которого сосредоточена на достижении высочайшего уровня киберустойчивости в партнерстве с отраслевыми предприятиями и научными организациями. Финансовая поддержка Правительства предполагается в объеме 2,6 млрд фунтов (3,2 млрд долл.)¹.

Национальная киберстратегия Великобритании дополняет целый ряд других стратегических документов правительства, например, таких как Цифровая стратегия Великобритании (UK Digital Strategy) [55], направленная на поддержку цифровой трансформации, ускорение роста и дальнейшее построение конкурентоспособной и инновационной цифровой экономики, а также Инновационная стратегия Великобритании (UK Innovation Strategy) [56], в которой изложены цели по развитию экономики на основе инноваций.

С целью изучения возможностей, преимуществ и проблем в области киберфизических систем, а также понимания вариантов формирования базовой киберфизической инфраструктуры Правительство Великобритании в 2022 году провело консультацию и серию дискуссий (по конкретным темам в рамках консультации) – Создание национальной киберфизической инфраструктуры для стимулирования инноваций (Enabling a national Cyber-Physical Infrastructure to catalyse innovation: consultation document) [57]. По итогам обсуждений были определены

¹ Национальная валюта Великобритании – фунты стерлингов – переведены в доллары (по курсу 26 декабря 2022 г.).

потенциальные промышленные и коммерческие возможности для роста глобального лидерства Великобритании в секторах киберфизических технологий и приоритетные области для действий в рамках следующих направлений: люди и культура; исследования, разработки и инфраструктура; безопасность и устойчивость; связь и операционная совместимость; устойчивые рынки; работа на глобальном уровне. Также согласно документу, выпущенному по итогам консультации, в области киберфизических систем к настоящему моменту были проинвестированы проекты в рамках следующих направлений: вычисления (Data & Analytics Facility for National Infrastructure, DAFNI) в размере 8 млн фунтов (9,6 млн долл.); инструменты и возможности визуализации в размере 210 млн фунтов (252,6 млн долл.) от Правительства Великобритании и IBM в Национальный центр цифровых инноваций Хартри (The Hartree National Centre for Digital Innovation, HNC DI), искусственный интеллект в объеме 15,6 млрд фунтов государственных инвестиций начиная с 2014 года. С 2018 по 2021 год в среднем ежегодно инвестировалось более 600 млн фунтов (721,8 млн долл.) в компании, занимающиеся робототехникой и технологиями дополненной и виртуальной реальности (AR / VR).

Большие инвестиции в развитие киберфизических систем и смежных технологий осуществлялись и осуществляются сейчас в *Германии* в рамках национальной стратегической инициативы Индустрия 4.0 (Industrie 4.0) [58]. Принятая 10 лет назад инновационная концепция зарекомендовала себя во всем мире как доминирующая парадигма цифровой трансформации обрабатывающей промышленности. Идея концепции заключается в повышение конкурентоспособности производимой продукции за счет интеграции киберфизических систем в производственные процессы (объединяя реальное и виртуальное пространства в киберфизические производственные системы). Она основана на достижениях немецкой промышленности в области технологий Интернета вещей (IoT) и Интернета услуг (IoS), в рамках ранее проведенных проектов [59].

Учитывая, что сегодня в немецкой обрабатывающей промышленности на вновь построенных заводах удалось полноценно внедрить Интернет вещей и киберфизические производственные системы, а на существующих предприятиях значительно расширились возможности подключения оборудования, инициатива Industrie 4.0 в 2019 году была дополнена экспертами Platform Industrie 4.0 [60] и сфокусирована на трех взаимосвязанных принципах формирования цифровых экосистем: автономность, интероперабельность и устойчивость [61]. До 2030 года предполагается создать основу для будущей экономики данных в соответствии с требованиями социальной рыночной экономики: делая упор на открытые экосистемы, разнообразие и плюрализм, и поддерживая конкуренцию между всеми заинтересованными сторонами на рынке [62]. По мнению экспертов развитие ряда технологических трендов в ближайшие 10 лет окажет влияние на принципы, заложенные в концепции. К ним относятся: промышленный искусственный интеллект (позволит автоматически интерпретировать производственные данные), периферийные вычисления, гибридные команды рабочих и коллаборативных роботов, промышленные сети 5G на заводах, автономные внутрипроизводственные логистические системы, надежные информационные инфраструктуры. Поддержка этих направлений позволит создать бездефектное производство и обеспечить превосходное качество продукции, что как предполагается станет конкурентным преимуществом Германии по сравнению с другими странами. К настоящему моменту одним из масштабных проектов развития направлений инициативы Industrie 4.0 является проект Gaia-X по созданию европейской облачной платформы в виде сетевой системы, которая связывает множество поставщиков облачных услуг друг с другом [63; 64]. Создание собственной платформы поддерживается Правительством страны и рассматривается в первую очередь как инструмент восстановления технологического суверенитета Европы и альтернатива уже существующим облачным сервисам США и Китая, которые используют немецкие компании [65].

Подобно немецкой инициативе в *Китае* разработан и принят Стратегический план развития производственного сектора «Сделано в Китае 2025» (Made in China 2025) [66; 67]. План направлен на поддержку промышленности в достижении технологического передового уровня за счет быстрого развития десяти высокотехнологичных отраслей (электромобили, информационные технологии и телекоммуникации нового поколения, передовая робототехника и искусственный интеллект, сельскохозяйственные технологии, аэрокосмическая техника, новые синтетические материалы, передовое электрооборудование, развивающаяся биомедицина, железнодорожная инфраструктура и высокотехнологичная морская техника). Документ предполагает разработку передовых технологий за счет инвестиций в НИОКР, накопления интеллектуальной собственности, принятия четких технических стандартов.

Также в Китае в 2021 году был принят 14-й пятилетний план социально-экономического развития (2021–2025) и долгосрочные цели развития до 2035 года Китайской Народной Республики (The 14th Five-Year Plan (2021–2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China). Среди задач, представленных в плане, в том числе предполагается сосредоточить внимание на достижении крупных прорывов в основных технологиях, включая искусственный интеллект следующего поколения, полупроводники, облачные вычисления, а также на создании национальных лабораторий и инновационных центров. Кроме того, планируется, что к 2025 году на цифровую экономику будет приходиться около 10% производства новой продукции Китая [68].

В соответствии с 14-м пятилетним планом в 2022 году Центральный комитет Коммунистической партии Китая и Государственный совет выпустили Стратегический план по расширению внутреннего спроса (The Outline of the Strategic Plan for Expanding Domestic Demand (2022–2035), который подразумевает увеличение инвестиций в создание надежной системы внутреннего спроса, оптимизацию структуры распределения, повышение качества предложения и улучшение рыночной системы [69]. Среди ряда мер [70], направленных на обеспечение роста внутреннего спроса, относительно развития технологий, планируется реализация научно-технических проектов в таких передовых областях, как искусственный интеллект, квантовые технологии и наука о мозге. Кроме того, предполагается создание кластеров передового производства и ускорение цифровизации малых и средних предприятий. Также существенные ресурсы будут направлены на формирование национальной интегрированной системы центров обработки больших данных [71].

В *Российской Федерации* тематика развития киберфизических систем и смежных технологий рассматривалась в рамках утвержденной программы «Цифровая экономика Российской Федерации» на период 2018–2024 гг. (распоряжение от 28 июля 2017 г. № 1632-р.) [72; 73], но в 2018 году в целях реализации указа Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» на ее основе была сформирована национальная программа «Цифровая экономика Российской Федерации», которая в дальнейшем обновлялась в соответствии с уточнениями государственной повестки (Указ от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»). Бюджет программы составляет 1 052 млрд руб. [74]. Программа предполагает увеличение внутренних затрат на развитие цифровой экономики, создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств, использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями [75]. В рамках Программы среди прочих мер уделяется внимание изменениям в нормативном регулировании и формированию стандартов в области цифровой экономики (например, в информационной безопасности, в том числе по формированию требований и методик проверки киберфизических систем, проектов стандартов безопасности для киберфизических систем и др.), а также созданию цифровых платформ (в первую очередь на государственном уровне) [76].

В состав Национальной программы входит 9 федеральных проектов:

- «Нормативное регулирование цифровой среды»;
- «Кадры для цифровой экономики»;
- «Информационная инфраструктура»;
- «Информационная безопасность»;
- «Цифровые технологии»;
- «Цифровое государственное управление»;
- «Искусственный интеллект»;
- «Обеспечение доступа в Интернет за счет развития спутниковой связи»;
- «Развитие кадрового потенциала ИТ-отрасли».

В рамках проектов помимо развития информационной инфраструктуры (широкополосного доступа к сети Интернет для социально значимых объектов, госорганов, удаленных населенных пунктов), предполагается реализация пилотных проектов по развитию новых технологий, в том числе относящихся к тематике киберфизических систем. Так, например, в рамках федерального проекта «Цифровые технологии» осуществляется поддержка

перспективных высокотехнологичных направлений, таких как квантовые коммуникации, квантовые вычисления, мобильные сети связи пятого поколения (5G). Технологии высокоскоростной передачи информации позволят автоматизировать производственные процессы, а также будут способствовать развитию Интернета вещей. В рамках Проекта осуществляется грантовая поддержка малых и крупных компаний, разрабатывающих отечественные решения в области информационных технологий, а также поддержка внедрения на предприятиях отечественных ИТ-решений, поддержка по льготному лизингу для содействия внедрению цифровых технологий и платформенных решений на основе отечественных программно-аппаратных комплексов, методическому сопровождению разработки и реализации компаниями стратегий цифровой трансформации на основе отечественных ИТ-решений [77].

Кроме того, поддержка разработки отечественных технологий искусственного интеллекта и кадровой сфер по данному направлению осуществляется в рамках федерального проекта «Искусственный интеллект» [78]. В рамках развития данного направления создано 6 исследовательских центров в области искусственного интеллекта [79]. На сегодняшний момент в рамках данного направления в рамках федерального проекта «Нормативное регулирование цифровой среды» была подготовлена Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г. (утверждена распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р) (см. подробнее в разделе 2.4) [80].

Как и в других государствах в России реализуются меры, направленные на обеспечение кибербезопасности. В рамках Национальной программы реализуется федеральный проект «Информационная безопасность», направленный на обеспечение устойчивости и безопасности информационной инфраструктуры, конкурентоспособности отечественных разработок и технологий информационной безопасности и формирование эффективной системы защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности [81]. Среди прочих мер в рамках проекта предусмотрено формирование национального киберполигона, который Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации разворачивает по всей стране, к настоящему моменту создано 5 полигонов [82].

С целью развития отдельных высокотехнологичных направлений были сформированы дорожные карты в рамках соглашений, заключенных между Правительством Российской Федерации и государственными корпорациями и компаниями с государственным участием [83]. Документы по каждому направлению подразумевают реализацию комплексного плана мероприятий, увязывающего инициативы и проекты по формированию необходимых нормативных мер, разработке ключевых технологий и внедрению продуктов и услуг на рынки.

В 2022 году в соответствии с поручением Президента Российской Федерации дорожные карты были актуализированы. По итогам года были дополнены и приняты документы по следующим направлениям: «Квантовые вычисления», «Квантовые коммуникации», «Искусственный интеллект», «Современные и перспективные сети мобильной связи», «Новое промышленное программное обеспечение» и «Новое общесистемное программное обеспечение». В рамках дорожных карт заявлено более 300 проектов, большая часть которых будет финансироваться из средств компаний (на общую сумму более 200 млрд руб.), остальные проекты будут реализованы за счет привлечения кредитных (около 20 млрд руб.) и грантовых (более 23 млрд руб.) средств [84]. Реализация проектов будет способствовать импортозамещению цифровых решений в различных отраслях экономики.

По итогам проведенного анализа нормативного правового регулирования, в том числе государственных программ поддержки развития направления киберфизических систем по НИРам и НИОКРам можно отметить, что стратегические документы разных стран отличаются содержанием и имеют свою специфику, обусловленную как уровнем развития технологий и научных достижений в отдельных областях, так и экономическими, социальными и другими факторами развития государств. Тем не менее в данных документах прослеживаются следующие схожие положения:

- Государственная поддержка направлена на разработку, производство и применение собственных технологий с целью обеспечения независимости от поставщиков из других стран. Стратегические документы предполагают поддержку развития киберфизических систем в целом и относящихся к ним отдельных смежных технологий;

- Формирование и принципы участия в международных консорциумах для работы над отдельными проектами, регламентируется нормами и правилами, установленными в интересах государства, иницирующего программу или проект. Соблюдение организациями-участниками из других стран установленных правил отслеживается;
- Цифровизация производства и возрастающий уровень проникновения цифровых технологий (в том числе цифровых приложений) в обычную жизнь граждан побуждает государства направить ресурсы на обеспечение информационной безопасности. В связи с этим в стратегических документах уделяется существенное внимание механизмам поддержки технологических решений обеспечения кибербезопасности различных секторов экономики, формированию компетентных кадров в данной сфере, а также нормативно-правовому регулированию взаимодействия внутри/вовне государства.

Таким образом, можно говорить о том, что государственная технологическая политика, в том числе в области киберфизических систем, направлена не на интеграцию, а на наращивание собственных возможностей и конкурентных преимуществ стран.

2.4 Национальный и международный нормативно-технический ландшафт по киберфизическим системам

В рамках текущего раздела представлен обзор национального и международного нормативно-технического ландшафта по киберфизическим системам. В обзоре приведены ведущие организации, регулирующие деятельность в области киберфизических систем, а также перечень стандартов и примеры нормативной правовой документации, направленные на регулирование отношений в области киберфизических систем, кибербезопасности и некоторых смежных технологий.

2.4.1 Международный нормативно-технический ландшафт по киберфизическим системам

Ведущими центрами международной стандартизации в области технологий киберфизических систем являются Международная электротехническая комиссия (International Electrotechnical Commission, IEC, МЭК) и Международная организация по стандартизации (International Organization for Standardization, ISO, ИСО) [85].

Помимо этого, деятельность по стандартизации в области киберфизических систем, кибербезопасности и смежных технологий проводят следующие международные организации:

- Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST);
- Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE);
- Британский институт стандартов (British Standards Institution, BSI);
- Немецкий институт по стандартизации (Deutsches Institut für Normung e.V. / German Institute for Standardization, DIN);
- Немецкий союз электротехники (Verband Deutscher Elektrotechniker / Association of German Electricians, VDE);
- Немецкая комиссия по электротехнике, электронике и информационным технологиям при Немецком институте по стандартизации и Немецком союзе электротехники (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE / German Commission for Electrical, Electronic & Information Technologies of DIN and VDE; DKE);
- Американский национальный институт стандартов (American National Standards Institute, ANSI);
- Международный союз электросвязи (International Telecommunication Union, ITU) и отдел стандартизации электросвязи Международного союза электросвязи (International Telecommunication Union – Telecommunication sector, ITU-T);
- Европейский комитет по стандартизации (Comité Européen de Normalisation / European Committee for Standardization, CEN);

- Европейский комитет электротехнической стандартизации (Comite Europeen de Normalisation Electrotechnique / European Committee for Electrotechnical Standardization, CENELEC);
- Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI);
- Североамериканская корпорация по надежности электроснабжения (North American Electric Reliability Corp., NERC);
- Управление стандартизацией Китая (Guobiao Standards / Standardization Administration of China, GB);
- Фонд «Открытая связь» (Open Connectivity Foundation, OCF).

В частности, Национальный институт стандартов и технологий США (NIST) отмечают, что технологии киберфизических систем тесно связаны с реализацией Интернета вещей, промышленного Интернета вещей, интеллектуальными сетями («Smart Grid»), «умным» городом («Smart City»), «умным» производством («Smart manufacturing») и т.п. [86; 87]. Видение NIST относительно развития концепции киберфизических систем представлено в нормативных документах, таких как «Основы для киберфизических систем: том 1, обзор» («Framework for Cyber-Physical Systems: Volume 1, Overview»), «Киберфизические системы и Интернет вещей» («Cyber-Physical Systems and Internet of Things»), «Основы международной технической рабочей группы «умного» города с поддержкой Интернета вещей» («International Technical Working Group on IoT-Enabled Smart City Framework»), «Основы и дорожная карта NIST для стандартов в области интероперабельности «умных» сетей, Версия 4.0» («NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0») и др. [88–94].

Опубликованный документ «Основы для киберфизических систем: том 1, обзор» направлен, в первую очередь, на определение надежности киберфизических систем, которая формируется на основе защищенности (security), конфиденциальности (privacy), безопасности (safety), надежности (reliability) и устойчивости (resilience) [88].

Так, направление киберфизических систем в рамках деятельности NIST регулируется Общественной рабочей группой (Cyber-Physical Systems Public Working Group, CPS PWG), которая разделена на 5 основных направлений: «Словарь и справочная архитектура» («Vocabulary and Reference Architecture»), «Примеры применения» («Use Cases»), «Расчет времени» («Timing»), «Кибербезопасность и конфиденциальность» («Cybersecurity and Privacy»), «Совместимость данных» («Data Interoperability») [95]. Целью рабочей группы по киберфизическим системам при подготовке отчета выступало определение общего понимания киберфизических систем, основополагающей концепции и уникальных параметров. В частности, были рассмотрены области применения киберфизических систем и связанные с ними барьеры, а также предложены мероприятия для устранения выявленных барьеров.

Другая публикация NIST «Киберфизические системы и Интернет вещей» содержит анализ происхождения терминов «киберфизическая система» и «Интернет вещей». Документ устанавливает единую концепцию для обоих понятий и приводит пояснение закономерным взаимосвязям для технологий киберфизических систем и Интернета вещей.

Помимо прочего, NIST в сотрудничестве с Институтом программных интегрированных систем при Университете Вандербильта (Institute for Software Integrated Systems at Vanderbilt University) разработало платформу «Универсальная киберфизическая среда для государства» Universal CPS Environment for Federation (UCEF) для упрощения проектирования киберфизических систем [96–98].

Таким образом, деятельность NIST, в частности, Общественной рабочей группы по киберфизическим системам NIST, направлена преимущественно на формирование единой концепции и подхода к определению киберфизических систем и смежных технологий, областей их применения, унификации понятий и архитектуры технологий, а также исследования обеспечения функциональности и безопасности применения технологий. Как отмечают эксперты рабочей группы, их исследования направлены на совместную с сообществом разработку новых унифицированных методов проектирования, эксплуатации и обеспечения безопасности киберфизических систем, которые могут послужить основой для исследований в рамках разработки стандартов и нормативной документации, регулирующей политику и деятельность в сфере киберфизических систем [99].

Не менее значимая деятельность по формированию подходов к концепции киберфизических систем проводится Международной организацией по стандартизации (ISO, ИСО) совместно с Международной электротехнической комиссией (IEC, МЭК). Так, ISO выделяет группу смежных технологий, которые тесно взаимосвязаны с концепцией киберфизических систем и, фактически, обеспечивают ее развитие. К таким технологиям ISO относит робототехнику, Интернет вещей, «умные» города и автономные транспортные средства [100]. В связи с этим в обзоре нормативно-технической деятельности ISO в области киберфизических систем приведены следующие технические комитеты (стандарты, разработанные техническим комитетом, приведены в Приложении 1):

1. ISO/TC 299 Робототехника (Robotics);
2. ISO/TC 241 Системы управления безопасностью дорожного движения (Road traffic safety management systems);
3. ISO/TC 22 Дорожные транспортные средства (Road vehicles);
4. ISO/TC 127 Техника для земляных работ (Earth-moving machinery);
5. ISO/TC 204 Интеллектуальные транспортные системы (Intelligent transport systems);
6. ISO/TC 268 Устойчивые города и населенные пункты (Sustainable cities and communities);
7. ISO/IEC JTC1/SC41 Интернет вещей и цифровые двойники (Internet of things and digital twin);
8. ISO/IEC JTC 1 / SC 27 Информационная безопасность, кибербезопасность и защита конфиденциальности (Information security, cybersecurity and privacy protection) [101];
9. ISO/IEC JTC 1 Информационные технологии (Information technology);
10. ISO/TC 59 / SC 17 Устойчивость зданий и сооружений гражданского строительства (Sustainability in buildings and civil engineering works);
11. ISO/TC 205 Проектирование зданий с учетом экологических требований (Building environment design).

Международная стандартизация по робототехнике также преимущественно осуществляется комитетом ISO/TC/184/SC2. В него входит 6 рабочих групп: WG01 «Словарь и технические характеристики», WG03 «Безопасность в промышленности», WG07 «Безопасность роботов персонального назначения», WG08 «Роботы сервисные», WG09 «Безопасность средств робототехники, используемых для медицинского оборудования» (совместно с TC62A МЭК), WG 10 «Модульность для сервисных роботов» [102]. Также в рамках профильного технического подкомитета ISO / IEC JTC 1 / WG 09 «Big Data» (ИСО / МЭК СТК 1 / РГ 9 «Большие данные») разрабатываются проекты международных стандартов в области технологии больших данных.

Помимо этого, ISO разработал стандарт ISO 23704-1:2022 «Общие требования к «умным» машинным системам с киберфизическим управлением – Часть 1: Обзор и фундаментальные принципы» («General requirements for cyber-physically controlled smart machine tool systems (CPSMT) — Part 1: Overview and fundamental principles»), в котором установлены основные определения киберфизических систем, относящихся к производству, и требования к организации управления станками [103].

Другие примеры деятельности в области нормативного регулирования и стандартизации киберфизических систем на международном уровне, в том числе в сфере кибербезопасности, приведены в Приложении 2. В частности, рассмотрены стратегии Правительства Соединенного Королевства, дорожные карты развития NASA, приведены некоторые международные стандарты в области киберфизических систем и отчеты об оценке возможности применения киберфизических систем такими странами, как Канада, Германия, Бельгия, Швейцария, Китай, Индия, Япония и др.

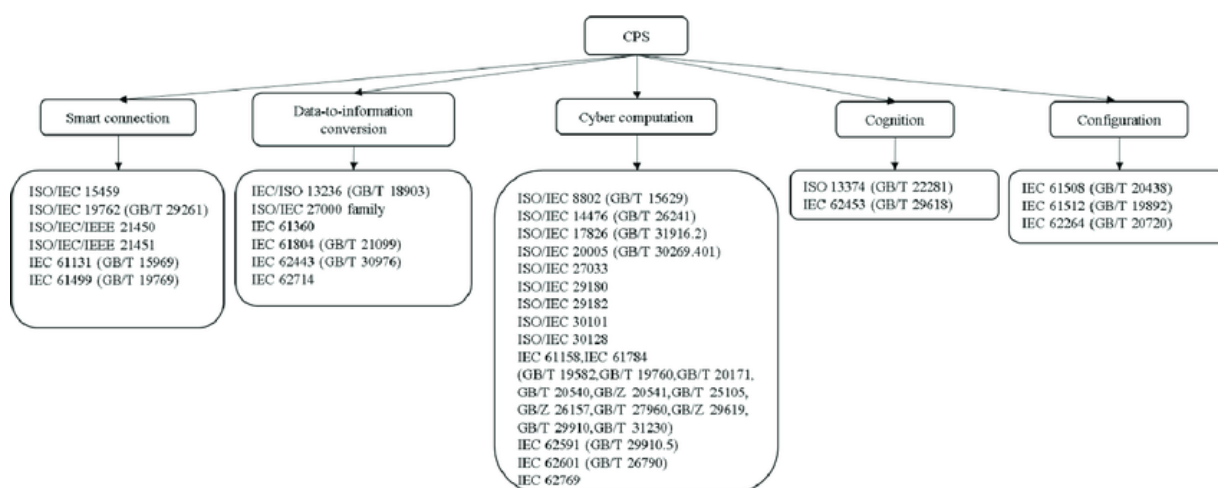
Некоторые примеры международных программ и нормативных документов, направленных на формирование нормативно-технического ландшафта в области технологий Индустрии 4.0, и некоторые рекомендации по совершенствованию нормативно-технического регулирования в области киберфизических систем и кибербезопасности приведены в работах [104–111].

Например, в отчете по результатам исследования «Развитие законодательства о робототехнике и киберфизических системах», проведенном ООО «Дентонс Юроп» по заказу Фонда «Сколково» в 2018 году, нормативное регулирование киберфизических систем рассмотрено преимущественно в контексте технологий робототехники и

искусственного интеллекта. Это может быть связано с тем, что по состоянию на 2018 год технологии киберфизических систем практически не регулировались государствами.

Авторы публикации «Обзор технических стандартов и патентного портфеля по внедрению киберфизических систем в передовое производство» («A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing», 2016), в свою очередь, приводят структуру стандартов по киберфизическим системам на основе нормативно-технических документов ISO, IEC, GB, которые они считают наиболее релевантными относительно технологии киберфизических систем (Рисунок 17) [105]. Авторы рассматривают систему стандартов с учетом разделения на 5 уровней архитектуры киберфизических систем.

Рисунок 17. Обзор стандартов ISO, IEC, GB в области киберфизических систем



Источник: «Обзор технических стандартов и патентного портфеля по внедрению киберфизических систем в передовое производство» («A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing»), 2016 г. [105]

Таким образом, можно отметить, что основная международная деятельность по регулированию киберфизических систем ведется организациями из США и некоторых стран Европейского союза, в том числе в тесном сотрудничестве с организациями, осуществляющими стандартизацию на национальном или международном уровне. В документах, составляющих основу международного нормативно-технического ландшафта по киберфизическим системам, преимущественно рассматриваются аспекты стандартизации для конкретных технологий, составляющих основу киберфизических систем. В то же время Правительства некоторых стран, например, Великобритании и Японии, ведут активную деятельность по включению киберфизических систем в инновационные стратегии на национальном уровне, ожидая значительные преимущества от повсеместного применения киберфизических систем.

2.4.2 Национальный нормативно-технический ландшафт по киберфизическим системам

В Российской Федерации для разработки национальных стандартов и участия в разработке соответствующих международных стандартов в области киберфизических систем в 2017 году был создан профильный технический комитет 194 «Кибер-физические системы» (ТК 194, приказ Росстандарта от 27 марта 2017 г. № 642 «О создании технического комитета по стандартизации «Кибер-физические системы»») [112]. Деятельность ТК 194 реализуется в рамках выполнения национального проекта «Нормативное регулирование цифровой среды», входящего в паспорт национальной программы «Цифровая экономика Российской Федерации» (см. раздел 2.3). Так, в частности, в рамках национального проекта Распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р была утверждена Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г. (ответственный орган – Минэкономразвития России) [113]. Целью Концепции выступает определение основных подходов к трансформации системы нормативного регулирования в РФ для обеспечения возможности создания и применения технологий искусственного интеллекта и робототехники в

различных сферах экономики, а также отношений, складывающихся в связи с разработкой и применением технологий, определение правовых барьеров, препятствующих разработке и применению указанных систем.

Технический комитет 194 выделяет следующие цели нормативно-технической деятельности [114]:

- Создание современной системы нормативно-технического регулирования в России;
- Вовлечение широкого круга представителей российского технологического бизнеса в работу по формированию современного нормативно-технического регулирования в России;
- Проактивная работа российских экспертов в сфере нормативно-технического регулирования на международном уровне.

В качестве задач деятельности технического комитета можно отметить следующее:

- Разработка и внедрение национальных стандартов;
- Разработка и внедрение международных стандартов;
- Гармонизация международных стандартов на национальном уровне;
- Развитие рыночной и технологической экспертизы по направлению перспективных технологий;
- Решение задач нормативно-технического регулирования в рамках ключевых государственных программ.

Деятельность технического комитета «Киберфизические системы» включает в себя 6 технологических направлений:

1. Интернет вещей;
2. Умные города;
3. Большие данные;
4. Умное производство;
5. Искусственный интеллект;
6. Умная энергетика.

Кроме того, технический комитет 194 активно вовлечен в реализацию программ Национальной технологической инициативы (НТИ). Так, в рамках НТИ реализуется план мероприятий («дорожная карта») «Технет» (передовые производственные технологии) Национальной технологической инициативы, который предусматривает в том числе мероприятия по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Технет» (передовые производственные технологии)².

Один из пунктов плана мероприятий по совершенствованию законодательства по направлению «Технет» – утверждение и актуализация «Перспективного плана стандартизации в области передовых производственных технологий на 2018–2025 годы» (утвержден Министерством промышленности и торговли РФ и Росстандартом в 2019 году) [116]. 28 сентября 2020 года было представлено и утверждено первое обновление перспективного плана, 21 марта 2022 года было представлено второе обновление и был утвержден актуализированный Перспективный план стандартизации в области передовых производственных технологий на 2018–2025 гг. (с изменением №1, №2) [117–119]. Текущая версия перспективного плана стандартизации включает свыше 130 стандартов и состоит из 5 укрупненных разделов, один из которых – «Стандарты в области кибер-физических систем». В рамках стандартизации в области киберфизических систем до 2022 года были приняты, в частности, следующие предварительные национальные стандарты:

1. ПНСТ 416–2020 Система киберфизическая. Общие положения;
2. ПНСТ 417–2020 Система киберфизическая. Термины и определения.

² План мероприятий («дорожная карта») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Технет» (передовые производственные технологии) был утвержден распоряжением Правительства Российской Федерации от 23 марта 2018 года № 482-р [115].

ПНСТ 416–2020 «Система киберфизическая. Общие положения» устанавливает общие положения и принципы в области киберфизических систем. ПНСТ 417–2020 «Система киберфизическая. Термины и определения» устанавливает термины и определения в области киберфизических систем. Разработка предварительных национальных стандартов была проведена АО «Всероссийский научно-исследовательский институт сертификации» (ВНИИС) и АО «Российская венчурная компания» (РВК)³.

Стандарты, планируемые к разработке в области киберфизических систем и приведенные в перспективном плане стандартизации, представлены в Приложении 3. Национальные стандарты будут взаимосвязаны и гармонизированы с международными стандартами в аналогичных сферах, разрабатываемыми в рамках ИСО и МЭК.

Помимо стандартов в области киберфизических систем, ТК 194 проводит подготовку нормативно-технической документации в направлении передовых производственных технологий, таких как умное производство, Интернет вещей и др. Перечень некоторых национальных стандартов и предварительных национальных стандартов, разработанных в рамках деятельности технического комитета 194, по смежным технологиям приведен в Приложении 4. Также в Приложении 4 приведен перечень разработанных национальных стандартов и предварительных национальных стандартов по смежным технологиям, разработанных другими техническими комитетами. На текущий момент в рамках реализации перспективного плана стандартизации в области передовых производственных технологий дополнительно запланирована разработка более 50 национальных стандартов и предварительных национальных стандартов, в том числе по технологиям, смежным с киберфизическими системами.

В рамках сотрудничества России с международными институтами стандартизации в 2022 году официально опубликован первый международный стандарт по промышленному Интернету вещей, разработка которого велась по инициативе ПАО «Ростелеком» на базе Технического комитета по стандартизации 194 «Кибер-физические системы»: ISO / IEC 30162:2022 «Требования к совместимости устройств, сетей и систем промышленного Интернета вещей» (Internet of Things (IoT) – Compatibility requirements and model for devices within Industrial IoT systems) [114]. Утверждение стандарта состоялось на уровне ключевых международных организаций – Международной организации по стандартизации и Международной электротехнической комиссии (ISO / IEC). Принятый стандарт устанавливает единые требования к совместимости различных устройств и систем промышленного Интернета вещей (IIoT). Стандарт призван стать основой для реализации концепции умного производства на практике и обеспечить возможности для продвижения российских технологий. Документ доступен на официальных ресурсах ISO и IEC.

Так, разработка международного стандарта ISO / IEC 30162:2022 была запущена в 2018 году при участии экспертов из США, Китая, Южной Кореи, Японии [121]. ТК 194 «Кибер-физические системы» представляет интересы Российской Федерации в профильном подкомитете крупнейших международных организаций в области стандартизации ISO / IEC JTC 1 / SC 41 «Интернет вещей и цифровые двойники» («Internet of things and digital twin»). Основной фокус деятельности подкомитета затрагивает Интернет вещей (IoT), промышленный Интернет вещей (IIoT), сенсорные сети, технологии беспроводной связи и смежные с ними цифровые технологии, рассматривая такие аспекты стандартизации, как термины и определения, вопросы эталонных архитектур, требования к системам и их совместимости, а с 2021 года также вопросы стандартизации цифровых двойников. В рамках деятельности технического комитета ISO / IEC специалисты ТК 194 являются редакторами и соредакторами более десятка международных стандартов [122; 123]. Технический комитет 194 «Кибер-физические системы» совместно с ПАО «Ростелеком» планируют инициировать разработку еще двух международных стандартов цифровых технологий в интересах развития отечественных решений в сфере цифровых и телекоммуникационных технологий.

Также на базе Государственного научного центра России Федерального государственного автономного научного учреждения «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики» (ЦНИИ РТК) приказом Росстандарта от 01 сентября 2016 г. № 1246 создан технический комитет по стандартизации ТК 141 «Робототехника», в рамках которого выполняется деятельность по подготовке

³ В 2020 году АО «Российская венчурная компания» передана под управление Российского фонда прямых инвестиций (РФПИ) [120].

стандартов нового комплекса национальных стандартов «Роботы и робототехнические устройства» [124; 125].

Таким образом, проведенный анализ свидетельствует о том, что в национальном нормативно-техническом ландшафте по киберфизическим системам присутствуют значительные резервы развития. Утверждение стандартов в области киберфизических систем и смежных технологий будет способствовать обеспечению импортонезависимости, а также активному распространению решений на основе цифровых технологий на российском рынке.

Основные технические идеи, в рамках которых реализуются национальные программы и развиваются международные организации по стандартизации в сфере киберфизических систем, можно резюмировать следующим образом [126]:

- выявление критических пробелов в текущей нормативно-технической документации;
- необходимость определения формальных основ и общих принципов киберфизических систем, которые поддерживают полный перечень вариантов их применения;
- поддержка принятия решений и обеспечение проектирования продуктов на основе нормативной документации в сфере киберфизических систем;
- объединение технической документации и реального опыта промышленных корпораций для решения задач в области киберфизических систем, «умного» города, «умного» производства» и других смежных технологий;
- разработка платформы для проведения испытаний киберфизических систем;
- выявление и продвижение инноваций, содействие проводимым мероприятиям по разработке стандартов в области киберфизических систем.

ГЛАВА 3. ОСНОВНЫЕ ИГРОКИ И ПРОЕКТЫ НА РЫНКЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ НАПРАВЛЕНИЯ «ТЕХНЕТ» НТИ

В данной главе был проведен анализ основных игроков и проектов на рынке киберфизических систем в применении к «сквозным» технологиям направления «Технет» НТИ. Была проведена оценка успешных бизнес-моделей и лучших практик на рынке, инвестиций, сделок M&A, коопераций, новых крупных проектов с учетом их планов, участников и сумм привлеченных инвестиций, а также были рассмотрены причины закрытия неудавшихся проектов.

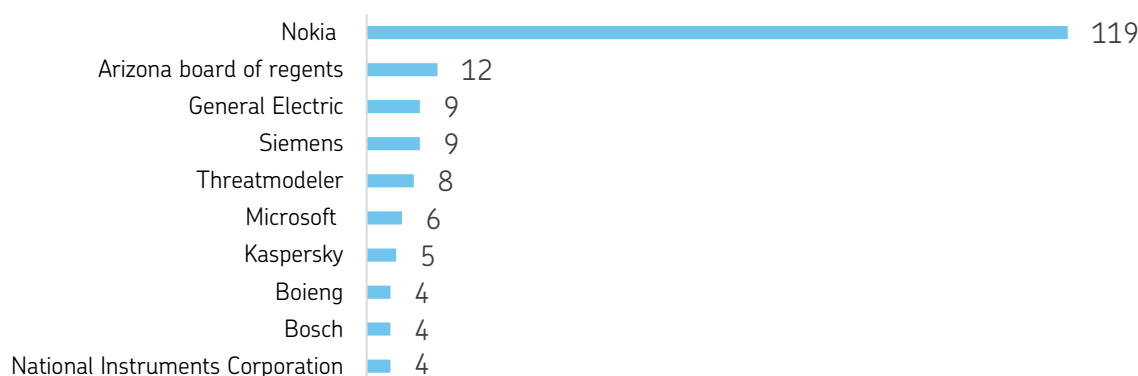
Для определения основных игроков и проектов на рынке киберфизических систем центром НТИ СПбПУ был выбран онлайн-сервис Lens.org, специализирующийся на составлении базы данных патентов и научной литературы [127]. Именно патенты по тематике «киберфизические системы» и их владельцы были включены в список ключевых игроков на рынке, поскольку это позволяет выявить действительные разработки компаний в соответствующей сфере.

Таким образом, в качестве ключевых игроков были выбраны 10 компаний и организаций, имеющих наибольшее количество патентов на рынке киберфизических систем. В выборке учитывались только те патенты, которые имели активный (действующий) правовой статус на конец 2022 года.

3.1 Основные игроки направления киберфизических систем: количество, рыночные доли, описание продуктов и разработок

Согласно данным выборки с сервиса Lens.org ключевыми компаниями и организациями на рынке являются финская компания Nokia, управляющий совет системы университетов штата Аризона (The Arizona Board of Regents, далее – ABOR), американская корпорация General Electric и немецкая компания Siemens. Эти организации в общей сумме владеют более 40% действующих патентов по тематике «киберфизические системы» (149 из 343) к концу 2022 года [127].

Рисунок 18. Основные игроки на рынке киберфизических систем по количеству патентов (ед.)



Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Lens.org, 2022 [127]

Такие крупные компании, как американская корпорация Microsoft, немецкая компания Bosch и американская компания Boeing, также попали в список основных игроков на рынке киберфизических систем.

Таблица 3. Основные игроки на рынке киберфизических систем

№	Компания	Страна	Тип деятельности	Выручка (млрд долл.)	Рыночная капитализация (млрд долл.)
1	Arizona board of regents	США	Научно-производственное объединение	0,003	

№	Компания	Страна	Тип деятельности	Выручка (млрд долл.)	Рыночная капитализация (млрд долл.)
2	Boieng	США	Публичная компания	62,29	120,02
3	Bosch	Германия	Частная компания	78,74	515,72
4	General Electric	США	Публичная компания	74,2	103,23
5	Kaspersky Lab	Россия	Акционерное общество	0,754	1,9
6	Microsoft	США	Публичная компания	184,9	2510
7	National Instruments	США	Публичная компания	1,47	5,74
8	Nokia	Финляндия	Публичная компания	25,8	35,33
9	Siemens	Германия	Публичная компания	75,26	138,74
10	Threatmodeler Software	США	Научно-производственное объединение	0,006	

Источник: Инфраструктурный центр «Технет» СПбПУ по материалам Companies Market Cap, 2022 [128]

Среди последних проектов по направлению киберфизических систем наибольшее распространение получили проекты компании Nokia в области телекоммуникаций, корпорации General Electric в сфере кибербезопасности, компании Siemens в области управления жизненным циклом изделия, а также организации Arizona Board of Regents [127].

В последние 4 года финская компания Nokia, занимающаяся производством телекоммуникационного оборудования, фокусируется на разработке передовых киберфизических технологий, в числе которых можно выделить следующие:

- Система кодирования для инкрементного резервирования гибридного автоматического запроса повторной передачи (Automatic repeat request, ARQ) для беспроводных сетей (Encoding system for incremental redundancy for hybrid ARQ for wireless networks) – способ кодирования внешним кодировщиком набора информационных битов, где происходит выполнение каждым полярным субкодировщиком полярного кодирования битов, принятых от внешнего кодировщика, для соответствующей передачи гибридного ARQ с инкрементным резервированием.
- Способ передачи сегментированных ограничений сети в беспроводных сетях 5G (Transmission of network slicing constraints in 5G wireless networks) – способ передачи, основанный на обратной связи централизованного устройства (centralized unit, CU) и распределенного устройства (distributed unit, DU), при котором CU может корректировать ограничения QoS (Quality of Service, «качество обслуживания») для каждого сегмента.
- Методы обработки коллизий полупостоянного планирования для беспроводных сетей (Techniques for handling semi-persistent scheduling collisions for wireless networks) – метод, основанный на способности пользовательского устройства определять возможность появления коллизий полупостоянного планирования (semi-persistent scheduling, SPS) в течение интервала времени передачи (transmission time interval, TTI).
- Метод компенсации эффекта Доплера во внеземных сетях (Doppler Compensation in Non-Terrestrial Networks) – способ коммуникации во внеземных сетях при помощи набора кривых доплеровского сдвига для различных расстояний до одной или нескольких спутниковых орбит.
- Настройка сегментирования сети (Network Slice Configuration) – способ сегментирования, основанный на сравнении и определении возможности выделения запрошенной услуги в отдельный сетевой сегмент [129–133].

Совет регентов Аризоны (The Arizona Board of Regents), ответственный за управление системой университетов штата Аризона, также занимается разработкой технологий в сфере киберфизических систем, выступая от лица Аризонского государственного университета (Arizona State University, ASU) и Университета Северной Аризоны (Northern Arizona University, NAU). Среди последних разработок ABOR присутствуют:

- Системы и методы контурного прогнозирования киберфизического управления фотоэлектрической решеткой (Systems and methods for skyline prediction for cyber-physical photovoltaic array control) – различные варианты использования киберфизической системы для обеспечения облачного прогнозирования управления фотоэлектрической решеткой.
- Системы с применением иерархических уровней безопасности (Systems Implementing Hierarchical Levels of Security) – системы и способы обеспечения аутентификации с переменным доступом, отвечающие потребности в иерархическом уровне безопасности, который может включать использование множества физически неклонировуемых функций (physically unclonable functions, PUF) и/или распределение набора ключей аутентификации с состояниями «безразлично».
- Системы, способы и устройства для использования совместного моделирования физической модели и самоадаптивного прогнозирующего контроллера с использованием гибридных автоматов (Systems, Methods, and Apparatuses for Utilizing Co-Simulation of a Physical Model and a Self-Adaptive Predictive Controller Using Hybrid Automata) – набор технологий, предполагающий генерирование гибридных автоматов как вариации начальных состояний объекта путем применения входных данных объекта к исходной модели, что позволяет создавать прогностические модели объектов с новыми настройками параметров.
- Обеспечение физически неклонировуемых функций дополнительными случайными троичными состояниями (Securing physically unclonable functions with additional random ternary states) – технология предполагает применение физически неклонировуемых функций (physically unclonable functions, PUF) с использованием троичных состояний для реализации систем безопасности.
- Усовершенствованные модели метода опорных векторов для краткосрочного прогнозирования выработки электроэнергии на ветроэлектростанциях (Support vector machine enhanced models for short-term wind farm generation forecasting) – технология, предполагающая использование метода опорных векторов при помощи усовершенствованной марковской модели для получения краткосрочных прогнозов результатов выработки энергии ветра [134–138].

Американская корпорация General Electric, которая занимается производством множества видов техники, среди всех своих проектов также имеет разработки в области киберфизических систем. Среди них:

- Фреймворк для разработки поведенческого мониторинга киберфизических систем (Framework to develop cyber-physical system behavior-based monitoring) – компьютерная платформа, позволяющая получать от устройства удаленного оператора необходимые данные о поведении системы, которые в дальнейшем могут быть использованы для создания модели обнаружения аномалий в киберфизических системах.
- Обнаружение и защита от атак с переключением режимов в киберфизических системах (Detection and protection against mode switching attacks in cyber-physical systems) – технология, позволяющая за счет оценки текущего состояния киберфизической системы генерировать варианты ее режимов, чтобы в дальнейшем использовать новую полученную индикацию для переопределения текущего режима киберфизической системы во избежание кибер-атак.
- Динамические физические водяные знаки для обнаружения атак в киберфизических системах (Dynamic Physical Watermarking For Attack Detection In Cyber-Physical Systems) – технология, при которой компьютерная платформа благодаря постоянному мониторингу состояния динамических физических водяных знаков позволяет обнаружить аномалии в киберфизических системах и потенциальные попытки кибер-атак.
- Система и способ обнаружения аномалий и киберугроз в ветряной турбине (System and method for anomaly and cyber-threat detection in a wind turbine) – технология, при которой компьютерная

платформа обнаружения аномалий может получать доступ к модели аномалии, генерировать набор ее признаков, а после составлять список возможных решений угрозы и обозначать векторы принятия решения.

- Обнаружение, локализация и нейтрализация кибератак для беспилотных летательных аппаратов (Cyber-attack detection, localization, and neutralization for unmanned aerial vehicles) – технология, позволяющая компьютерной платформе идентифицировать тип угрозы, определить ее признаки и предложить варианты решения проблемы с векторами дальнейшего развития событий [139–143].

Немецкая компания Siemens, фокусирующаяся на сферах электроники и электротехники, начиная с 2014 года также стала проводить исследования и создавать новые технологии в области киберфизических систем. Среди последних можно выделить следующие:

- Контекстно-ориентированный синтез имитационных моделей из функциональных моделей киберфизических систем (Context-Based Synthesis Of Simulation Models From Functional Models Of Cyber-Physical Systems) – технология, которая фокусируется на моделях функционального поведения и состояния с поддержкой моделирования, использующих автоматические и контекстно-зависимые сопоставления элементарных функций функциональной основы с компонентами моделирования, описанными на языках физического моделирования, после чего потенциально полезные циклы процессов распознаются и включаются в функциональную модель.
- Способ классификации и соотнесения компонентов моделирования с функциональными моделями (Method for classifying and correlating simulation components to functional models) – метод, включающий в себя анализ и составление библиотеки компонентов моделирования с построением графиков функций для каждого компонента из множества компонентов моделирования.
- Производственный модуль для выполнения производственной функции над продуктом (Production Module for Performing a Production Function on a Product) – технология, в которой производственный модуль для выполнения производственной функции над продуктом сконфигурирован в паре со вторым производственным модулем, который построен для реализации второй производственной функции над продуктом.
- Способ планирования изготовления продукта и производственный модуль с информацией самоописания (Method for planning the manufacture of a product and production module having self-description information) – технология, при которой каждый производственный модуль продукта связан с другим модулем и включает в себя набор информации самоописания в виде базы данных.
- Способ и устройство для обеспечения безопасной эксплуатации технической системы (Method and Apparatus for Providing a Safe Operation of a Technical System) – технология для обеспечения безопасной эксплуатации технической системы, включающей множество компонентов системы [144–148].

3.2 Оценка успешных бизнес-моделей и лучших практик

Проанализировав последние разработки, технологии и проекты компаний в сфере киберфизических систем, Инфраструктурный центр НТИ по направлению «Технет» СПбПУ предлагает свою классификацию бизнес-моделей, применяемых компаниями, для получения более структурированной картины. Среди основных бизнес-моделей выделены:

- Создание передовых технологических решений для повышения производительности уже существующих и эксплуатируемых операционных технологий (Operational technologies, OT) – бизнес-модель, при которой упор делается на применение киберфизических систем в разработке аппаратного и программного обеспечения для повышения эффективности уже существующих технологий и ускорения цифровизации отдельных направлений. Наиболее часто эта бизнес-модель применяется в сферах робототехники, автономных транспортных средств, Интернета вещей

(Internet of Things, IoT) и «умных» городов. Ключевыми компаниями, применяющими эту бизнес-модель, являются Bosch, CityZenith и ABB [149].

- Создание передовых технологических решений для хранения данных и ускоренного обмена ими – бизнес-модель, предполагающая создание технологий, связанных с телекоммуникационными сетями и базами данных. Наиболее яркими представителями применения этой бизнес-модели являются компании Nokia, National Instruments и Boeing [127].
- Создание передовых технологических решений для защиты данных, предотвращения и нивелирования последствий кибератак – одно из самых актуальных направлений применения киберфизических систем, поскольку высокий рост количества киберпреступности ведет к огромным финансовым потерям. В 2021 году общая стоимость ущерба от киберпреступности составила 6 млрд долл. по всему миру, а каждая компания в среднем сталкивалась с 130 попытками взлома своей системы безопасности. Наиболее успешные практики применения технологий киберфизических систем в этой бизнес-модели принадлежат компаниям Siemens, Microsoft и General Electric [150].

Стоит отметить, что большинство компаний не пользуются только одной из вышеперечисленных бизнес-моделей, а чаще используют смешанные модели. Так, финская компания Nokia реализует свои проекты по киберфизическим системам не только в сфере телекоммуникаций и обмена данными, но и в сфере повышения производительности операционных технологий [151].

Ниже приведены примеры некоторых практик применения киберфизических систем крупными компаниями и их исследовательскими центрами.

IUDX – система обмена городскими данными Индии

India Urban Data Exchange (далее – IUDX) – один из проектов внутри направления «Умные города» (Smart Cities) Индии, начатый в 2020 году. Система IUDX была создана в ходе совместной работы Индийского научного института (Indian Institute of Science), Индийского технологического института в Мумбаи (Indian Institute of Technology Bombay), Международного института информационных технологий в Хайдарабаде (International Institute of Information Technology, Hyderabad) и Центра киберфизических систем им. Роберта Боша в Бангалоре (Robert Bosch Centre for Cyber Physical Systems) по заказу Министерства жилищного строительства и городских дел Индии и Министерства электроники и информационных технологий Индии в рамках программы «Умные города» [152]. Причиной создания IUDX выступила растущая необходимость в унификации подходов к цифровизации городов Индии как для систематического технического развития, доступного для каждого города, так и во избежание конфликтов данных между департаментами разных городов [153].

Платформа дает возможность отслеживать и учитывать данные с устройств Интернета вещей, установленных по всем городам, хранить и анализировать демографические и географические данные Индии, сверять записи налоговых, вести архив документов и законов, а также платформа предоставляет доступ к закрытым источникам данных [154].

IUDX оказывает положительное влияние на администрирование городов, управление правительственными данными, предпринимательство, жизнь населения и научный прогресс. На конец 2022 года более 28 городов Индии используют систему обмена городскими данными [155]. В качестве положительных результатов использования технологии IUDX официальные представители отмечают:

- Снижение затрат на разработку и более быстрое применение решений.
- Снижение стоимости проводимых государством операций за счет повышения эффективности предоставления услуг населению.
- Появление новых инновационных решений городских проблем.
- Возможность объединения множества информационных блоков для создания полноценной картины происходящего.
- Возможность более быстрого и легкого обмена данными.
- Появление больших возможностей для предпринимательства.

- Ускорение масштабирования принимаемых решений на территории страны.
- Появление более дешевых услуг для населения.
- Предоставление более качественных услуг населению.
- Проведение более качественных исследований за счет доступа к различным закрытым базам данных.
- Возможность появления инновационных решений партнеров из других стран благодаря доступности данных [154].

MX Industrial Edge – ускорение процесса цифровизации от Nokia

В октябре 2021 года финская компания Nokia объявила о запуске приложения MX Industrial Edge – это облачное решение, позволяющее компаниям ускорить процесс цифровизации их операционных технологий и удовлетворять потребностям Индустрии 4.0. Приложение было создано с целью ускорения цифровой трансформации промышленности путем уникального совмещения технологий вычисления, хранения данных, проводных и беспроводных сетей и автоматизированного управления [151].

MX Industrial Edge позволяет пользователям поддерживать полный контроль над данными с гарантией их безопасности, интегрировать новейшие разработки в операционные технологии компаний, такие как, например, «умная» автоматизация рабочего процесса, а также обеспечивает высокую производительность и безопасность передовых решений. Платформа также предоставляет доступ к другим техническим решениям от компании Nokia, таким как Сети дронов (Drone networks), Групповые коммуникации (Group communications), Частные промышленные сети (Industrial-grade private wireless), Сетевой цифровой двойник (Network Digital Twin) и Облако цифровой автоматизации (Digital Automation Cloud) [156].

К концу 2022 года количество потребителей, использующих платформенное решение MX Industrial Edge, достигло отметки в более чем 1300 предприятий. Пользователи новой передовой технологии среди положительных результатов отмечают:

- Легкость в применении новых решений автоматизации рабочих процессов на предприятиях.
- Доступность данных и скорость их передачи за счет облачного хранилища.
- Гибкость в использовании благодаря поддержке проводных и беспроводных сетей.
- Стабильность и безопасность обновления данных без потери информации или ее утечки.
- Предоставление дополнительных услуг и решений от компании Nokia.
- Высокая адаптивность технологии к другим платформам и экосистемам.
- Высокая скорость промышленного подключения.
- Широкий спектр применения технологии: от коммунальных услуг до нефтегазовой и горнодобывающей промышленности [156].

SIBERprotect – решение киберугроз от Siemens

В 2021 году немецкая компания Siemens представила свое решение по мониторингу кибератак и улучшению киберзащиты – SIBERprotect. Новая система киберзащиты была создана дочерней компанией Siemens Government Technologies (далее – SGT) по заказу правительства США с целью обеспечения максимальной сохранности данных, операционных технологий и критически важных инфраструктур США [157]. Основной причиной создания SIBERprotect послужил резкий рост киберпреступности в мире, активность которой в 2021 году возросла более чем на 600% по сравнению с предыдущим годом [150].

Среди основных функций новой системы киберзащиты можно выделить:

- Обеспечение ответа на кибератаку с миллисекундной задержкой после уведомления в реальном времени;
- Оповещение пользователей о происходящей кибератаке при помощи звуковых, световых и текстовых сигналов;
- Автоматический перевод операционной технологии в безопасный режим и/или карантин при

- обнаружении кибератаки;
- Определение ответных действий согласно предписанному перечню правил киберзащиты компании;
- Автоматическое изолирование сети для предотвращения распространения вредоносного программного обеспечения после его обнаружения;
- Ускоренное восстановление операционной технологии за счет безопасного восстановления резервной копии систем и определения порядка приоритета восстановления [157].

SIBERprotect применяется на большинстве критически важных объектах инфраструктуры США, таких как:

- электростанции, где система киберзащиты подключается напрямую к защитному реле и с него предотвращает попытки стороннего проникновения;
- военные склады и сооружения, где SIBERprotect усиливает защиту объектов за счет имплементации набора правил брандмауэра;
- военно-морские верфи, на которых система моментально отправляет на карантин все системы для предотвращения утечки данных;
- военно-морские корабли, где система способна предотвратить перехват управления автоматизированными системами корабля;
- центры обработки данных, на которых SIBERprotect изолирует появившееся вредоносное программное обеспечение и запускает протоколы безопасности;
- объекты производства, где при попытках вмешательства со стороны запускаются сигналы предупреждения и протоколы устранения угрозы [157].

Согласно отзывам потребителей, результаты внедрения технологии SIBERprotect на объекты критической инфраструктуры являются исключительно положительными. Уэйн Кантрелл, ведущий системный инженер SGT и ответственный за разработку системы SIBERprotect, отмечает, что время для нормализации рабочего графика у потребителей после кибератаки существенно снизилось: ранее требовалось примерно 2000 часов (более 83 суток) для полного нивелирования последствий кибератаки, когда как после установки SIBERprotect нормализация происходит менее чем за 8 часов [158].

3.3 Инвестиции, сделки M&A, кооперация

Компании-лидеры на рынке киберфизических систем и их проекты к концу 2021 года получили не малое количество инвестиций, были задействованы в нескольких сделках слияния и поглощения (Mergers & Acquisitions, M&A), а также вступали в кооперации с другими компаниями в сфере киберфизических систем. Ниже рассмотрены показатели инвестиций в сферу киберфизических систем и совместные проекты ведущих на рынке компаний Nokia, Bosch, Microsoft и Siemens, а также наиболее актуальные стартапы в соответствующем сегменте.

3.3.1 Инвестиции в сферу киберфизических систем

Общие финансовые вложения финской компании Nokia в сферу киберфизических систем на конец 2021 года составили более 1,09 млрд долл., из которых 569 млн долл. – затраты на исследования и разработки в соответствующей сфере, что на 16 млн долл. меньше, чем в предыдущем году. Снижение количества финансовых затрат связано с результатами усилий руководства компании по сокращению базы затрат, а также с высокой окупаемостью последних реализованных проектов (например, MX Industrial Edge). При этом количество купленных акций компании Nokia увеличилось с 5,653 млрд до 5,675 млрд при сокращении количества акционеров с 246 тыс. до 233 тыс. [159].

На конец 2021 года компания Bosch потратила более 6 млрд долл. на свои собственные исследования и разработки, 79% которых были вложены в сферу киберфизических систем, что на 2% меньше значений предыдущего года. Из приоритетных исследований и разработок по капиталовложению отмечаются электрификация автомобильных компонентов, системы помощи водителю, автоматизированное вождение, автомобильная электроника и датчики. Общая сумма вложенных инвестиций в компанию Bosch к концу 2021 года достигла значения в более

чем 600 млн долл., что на 100 млн долл. меньше по сравнению с предыдущим годом [160].

Финансовые вложения компании Microsoft в исследования и разработки составили более 20 млрд долл. на конец 2021 года, что на 1,4 млрд долл. больше, чем в предыдущем году. Из них более 70% были направлены на исследования в области киберфизических систем, а основным драйвером капиталовложений являлась растущая потребность в облачном инжиниринге. Кроме этого, компания Microsoft планирует в ближайшие 5 лет совершить инвестиции в размере 20 млрд долл. в повышение уровня своей кибербезопасности, поскольку количество кибератак на компанию с каждым годом увеличивается (за 2021 год было совершено более 31 млрд зарегистрированных кибератак на Microsoft). Количество привлеченных инвестиций в компанию за 2021 год возросло по сравнению с предыдущим годом, а прибыль от них составила более 1 млрд долл. [161].

На конец 2021 года суммарные капиталовложения компании Siemens в НИОКР по киберфизическим системам составили более 5 млрд долл., что на 0,5 млрд долл. больше вложений предыдущего года. Основными направлениями разработок являлись автономная робототехника, кибербезопасность, искусственный интеллект, автоматизация производственных процессов, системы программного обеспечения, технология цифровых двойников. Большинство из этих технологий также продвигаются при помощи партнерства Siemens с исследовательскими институтами и научными лабораториями и в рамках коллективных проектов при финансовой поддержке государства. Основным подразделением венчурного капитала компании Siemens является Next47, которое занимается капиталовложением в перспективные стартапы, скупая проекты и сотрудничая с ними. Кроме этого, инвестиции в саму компанию выросли на 50% по сравнению с предыдущим годом, суммарно составив более 6 млрд долл. [162].

Стартапы в сегменте киберфизических систем также являются одним из ярких примеров инвестиций в соответствующую технологию. Среди наиболее успешных стартапов в сфере киберфизических систем на конец 2021 года можно выделить китайскую частную компанию ByteDance с ее социальной сетью и искусственным интеллектом Douying, более известным под названием TikTok, с общей суммой инвестиций в 140 млрд долл., компанию SenseTime и ее искусственный интеллект по распознаванию лиц, сумма инвестиций в который составила более 12 млрд долл., и китайскую частную компанию DJI, специализирующейся на производстве летающих дронов и видеоборудования (Приложение 5) [163].

3.3.2 Сделки M&A в области киберфизических систем

Говоря о сделках M&A компании Nokia, которыми занимается ревизионная комиссия компании, в 2021 году никакого слияния с другими компаниями или их поглощения не происходило. Однако в 2020 году Nokia завершила сделку по приобретению компании Elenion Technologies, занимающейся разработкой технологий в областях кремниевой фотоники и телекоммуникаций. Именно передовые знания и технологический опыт компании стали решающими при выборе ее приобретения, поскольку исследования и разработки Elenion Technologies позволят ускорить процесс развития технологий Nokia и, соответственно, ускорить процесс цифровой трансформации промышленности [164].

Компания Bosch в 2021 году начала сделки по приобретению двух организаций: австралийской компании MoTeC, занимающейся разработкой и производством технологий для автоспорта, и нидерландской компании ItoM, специализирующейся на высокочастотных операционных полупроводниках [165; 166]. Внедрение технологий двух приобретенных компаний поможет специалистам Bosch продвинуться в своих разработках в области киберфизических систем, связанных с автомобильной и высокотехнологичной промышленностями [165]. Обе сделки были завершены осенью 2022 года [167].

В 2021 году Microsoft совершила две сделки M&A: приобретение компании ZeniMax, головной компании Bethesda Softworks LLC, занимающейся разработкой видеоигр, за 8 млрд долл., и компании Nuance, специализирующейся на разработке облачных решений и искусственного интеллекта для сферы здравоохранения, за 20 млрд долл. Приобретение двух этих компаний значительно ускорит процесс разработки специализированных облачных решений, а также позволит Microsoft укрепиться на рынке видеоигр и здравоохранения [161]. Кроме этого, приобретение в 2018 году платформы для разработки программного обеспечения GitHub значительно ускорило процесс

разработки новых программных решений специалистами Microsoft, а общая прибыль от GitHub к концу 2021 года составила 7 млрд долл. [161].

За 2021 год компания Siemens совершила несколько сделок по приобретению других компаний на общую сумму более 18 млрд долл. Самыми крупными сделками являлись сделка по приобретению американской компании Varian Medical Systems за 16,4 млрд долл., обладающей перспективными цифровыми решениями и приложениями в области радиационной онкологии и впоследствии интегрированной в Siemens Healthineers, а также сделка по приобретению платформы Supplyframe для цифровизации мировых цепочек поставок электроники за 0,56 млрд долл. Новоприобретенные компании будут стимулировать прогресс развития технологий Siemens в здравоохранении и электронной промышленности [162].

3.3.3 Кооперация компаний в области киберфизических систем

Основным партнером компании Nokia к концу 2021 года являлась компания Joint Audit Cooperation, сотрудничество с которой позволяет обеспечивать прозрачность и эффективность управления цепочками поставок и телекоммуникационными связями. Кроме этого, Nokia стала участницей Альянса ответственного бизнеса (Responsible Business Alliance, RBA), в рамках которого осуществляется управление и помощь по мировым цепочкам поставок. Инвестиции компании в совместные проекты и ассоциированные компании на конец 2021 года составили более 257 млн долл. [159].

В 2021 году компания Bosch активно кооперировалась с компанией Microsoft в сфере киберфизических систем, а именно в разработке программного обеспечения для установления непосредственной связи автомобилей и облачного хранилища данных. Само программное обеспечение базируется на Microsoft Azure – облачной платформе компании Microsoft – и включает в себя дополнительные уникальные программные решения от Bosch. Предполагается, что совместно разработанное программное обеспечение от Microsoft и Bosch позволит не только сократить инновационные циклы, но и минимизировать затраты на разработку нового программного обеспечения для транспортных средств [160].

Одним из крупных совместных проектов Microsoft, начавшихся в 2021 году, стало объединение с консалтинговой компанией Accenture и IT-компанией Avanade в разработке прогрессивных решений по вопросу глобального изменения климата. Совместная деятельность этих компаний предполагает предоставление консультационных услуг и инновационных решений по снижению количества выбросов углерода в атмосферу на всем жизненном цикле производства. Благодаря кооперации планируется ускорить процесс перехода к цифровому производству, распространить технологии низкоуглеродной энергетики, перейти к «зеленой» разработке программного обеспечения, а также обеспечить устойчивое развитие производства при помощи Microsoft Azure и постоянной аналитики [168].

Среди основных коопераций Siemens в 2021 году следует отметить сотрудничество Digital Industries (одного из подразделений Siemens) с немецкой компанией Schaeffler Group по созданию универсальной цифровой платформы с элементами аналитики на основе искусственного интеллекта и цифровым проектированием подшипников. Кроме этого, Digital Industries совместно с Google Cloud приступила к интеграции своих систем автоматизации производства с облачными данными Google, технологиями искусственного интеллекта и машинного обучения. Также, Digital Industries в кооперации с компаниями EOS и DyeMansion представили первую виртуальную эталонную фабрику аддитивного производства для селективного спекания и промышленной постобработки (Virtual additive manufacturing reference factory for selective laser sintering and industrial post-processing) [162].

3.4 Новые крупные проекты: участники, планы, суммы привлеченных инвестиций

В 2021 – 2022 годах компании-лидеры на рынке киберфизических систем также запустили новые перспективные проекты в соответствующей сфере, которые будут реализованы в ближайшем будущем. Среди наиболее крупных из них можно отметить проекты компаний Nokia, Bosch и Siemens, направленные на ускорение цифровизации промышленности, развитие автоматизированных транспортных средств и развитие телекоммуникационных сетей.

Sokol Flex OS – программное обеспечение для цифровой промышленности

Один из новейших проектов немецкой компании Siemens на платформе Linux в кооперации с Yocto Project (проект для создания дистрибутивов Linux для встроенного программного обеспечения и Интернета вещей) и при поддержке архитектуры RISC-V – Sokol Flex OS – стартовавший на рубеже 2021 – 2022 годов и планирующий увидеть свет в 2023 году. Sokol Flex OS – цифровая коммерческая платформа, предполагающая повышение эффективности взаимодействия рабочих групп в промышленной, медицинской, потребительской и авиационной промышленности. Платформа потенциально сможет облегчить управление дистрибутивами, инструментами и приложениями компаний по всей площади предприятия наиболее экономически эффективным способом. Кроме этого, Sokol Flex OS позволит разработчикам создавать свои собственные уникальные продукты на основе Linux, тем самым расширяя как саму платформу, так и интегрируя новые инструменты и функции в свои проекты [169]. Затраты на разработку проекта на начальной стадии за 2022 год составляют более 10 млн долл., а основным инвестором является компания Digital Industries – дочерняя компания Siemens [170].

Среди основных преимуществ программного обеспечения компания Siemens отмечает следующие:

1. Минимизация рисков из-за ускоренной продуктивности – платформа является интегрированной, испытанной и поддерживаемой, что позволяет ускорить время на повышение производительности и обеспечить дифференциацию.
2. Индивидуализация платформы – разработчики, которые используют этот продукт, имеют полный контроль над своей платформой Linux и могут ее настраивать под себя.
3. Расширяемость платформы – легкость в добавлении новых функций и инструментов, а также поддержка стороннего оборудования.
4. Настройка платформы – платформа предполагает наличие дополнительных инструментов для настройки каждого аспекта программного обеспечения и его дополнительных функций.
5. Безопасный Интернет вещей – система безопасности интегрирована во все устройство, что обеспечивает защиту данных в состоянии покоя (data at rest), данных в процессе использования (data in use) и данных в процессе передачи (data in transit). Платформа также включает в себя обновления для системы безопасности в целях устранения баз данных общеизвестных уязвимостей информационной безопасности (Common Vulnerabilities and Exposures, CVE) [169].

Основными особенностями платформы являются:

1. платформа Linux на базе Yocto Project коммерческого уровня;
2. прямое соединение с Интернетом вещей;
3. безопасное обновление программного обеспечения;
4. изоляция приложений при помощи контейнеров Docker (программное обеспечение для контейнеризации приложений);
5. качественная графика благодаря использованию Qt (фреймворк для разработки программного обеспечения);
6. интеграция SourceryTM CodeBench IDE (среда для разработки высокопроизводительных приложений);
7. мультимедиа;
8. широкая поддержка такого оборудования, как Arm, PowerPC, AMD x86, Intel x86, RISC-V;
9. наличие продуктов и услуг для поддержки клиентов на всех стадиях жизненного цикла их проектов: начиная от концепта и заканчивая развертыванием [169].

Кроме этого, платформа включает в себя дополнительные пакеты функций, например «Искусственный интеллект и машинное обучение», который позволит разработчикам сэкономить время на машинном обучении пропуская шаги по интеграции в платформу, что дает возможность сразу перейти к разработке и производству технологий [169].

ATTENTION – искусственный интеллект для автомобилей

Запущенный в апреле 2021 года, проект ATTENTION преследует своей целью создание метода прогнозирования травматизма уязвимых участников дорожного движения (vulnerable road users, VRU), таких как пешеходы и велосипедисты, в режиме реального времени. Проект реализуется в рамках исследовательской программы правительства Германии «Новые транспортные средства и системные технологии» («New vehicle and system technology») [171]. Основными участниками проекта являются:

1. Общество инженерных услуг по методу конечных элементов (Gesellschaft für FEM Ingenieurdienstleistungen) DYNAmore, Штутгарт, Германия.
2. Общество Фраунгофера – Институт Эрнста Маха (Fraunhofer Gesellschaft – Ernst Mach Institut (EMI)), Фрайбург-в-Брайсгау, Германия.
3. Компания по разработке программного обеспечения QualityMinds, Нюрнберг, Германия.
4. Инженерная и технологическая компания Bosch, Герлинген, Германия.
5. Университет Штутгарта – Институт моделирования биомеханических систем (University of Stuttgart – Institute for the Modeling and Simulation of Biomechanical Systems (IMSB)), Штутгарт, Германия [172].

В качестве ассоциированного партнера выступает предприятие Mercedes-Benz. Проект финансируется за счет Федерального министерства экономики и борьбы с изменением климата Германии, а сумма привлеченных инвестиций в ATTENTION составила более 1,8 млн долл. [172].

Проект предполагает использование процессов и функций искусственного интеллекта, основанных на данных, цифровых моделей человека и данных с транспортных средств, а также виртуальных испытаний. Методы искусственного интеллекта используются для определения риска получения травм в конкретных ситуациях на основе данных, полученных с транспортных средств и виртуальных испытаний. Исследование цифровой модели человека позволяет создать связь между областью науки о моделировании и уже существующими исследованиями института Cyber Valley, специализирующегося на разработках в сфере искусственного интеллекта. В проекте сочетаются модели каждой части тела человека и методы искусственного интеллекта для генерации движений моделей, а также методы машинного обучения. Именно совокупность всех этих методов будет в конечном итоге использоваться для модели прогнозирования травм. Кроме этого, искусственный интеллект будет учитывать, кто именно являлся сторонами столкновения: пешеход, велосипедист или кто-то другой [172]. Такое решение позволит не только обеспечить в будущем безопасную и эффективную транспортировку, но и развить и внедрить новые стратегии минимизации рисков для автоматизированных транспортных средств [171].

Среди ключевых достижений, которые должны будут быть достигнуты в ATTENTION, отмечают создание базы данных о местоположении и движении пешеходов и велосипедистов. Для более точного биомеханического прогнозирования движений и развития искусственного интеллекта планируется создать и исследовать базу данных аварий. В дальнейшем, данные, полученные в ходе виртуальных испытаний модели потенциальных травм, будут сравниваться с реальными данными об авариях и сохраняться в дополнительной базе данных о столкновениях и травмах [171].

Неха-Х – передовые технологии 6G в Европе

Проект Неха-Х – передовой технологический проект компаний Европейского Союза, обеспечивающий связь между физическим и цифровым мирами. Среди основных направлений проекта можно отметить разработку таких ключевых технологических средств, как:

1. новые технологии радиодоступа на высоких частотах, а также технологии локализации и зондирования с высоким разрешением;
2. подключенный интеллект с помощью управляемого воздушного интерфейса;
3. архитектурные средства 6G для дезагрегации сети и динамической надежности [173].

В проект входят поставщики новейших технологий, операторы сетей и высокотехнологичные компании. Всего

Неха-Х объединяет в себе 25 организаций из 9 европейских стран: Финляндии, Швеции, Германии, Франции, Италии, Испании, Греции, Турции и Хорватии. Лидерами проекта являются такие организации, как Nokia и Ericsson, занимающиеся разработкой в области телекоммуникаций. Основными поставщиками в области промышленных технологий являются компании Siemens, Atos и Intel, предоставляющие современные технологические решения в сферах искусственного интеллекта и управления сетью. В Неха-Х также входят исследовательские институты, проводящие соответствующие исследования по тематикам 5G/6G в целях максимизации усилий, вложенных в проект [174]. Финансирование проекта происходит в рамках специальной программы Европейского Союза по исследованиям и инновациям, а сумма вложенных инвестиций по гранту составляет более 12 млн долл. [175].

Проект предполагает 4 стадии развития с соответствующими целями. В рамках первой стадии планируется заложить основы для комплексной архитектуры системы, где будет реализовываться концепция соединения интеллекта, устойчивости, надежности, инклюзивности и экстремального опыта компаний путем разработки 6G «ткани». Здесь будут проведены анализы существующих трендов в технологиях и тенденций в обществе, определены основные услуги и варианты использования Неха-Х, выведены показатели устойчивости, гибкости, инклюзивности, определено первоначальное видение архитектуры проекта, оценена нормативно-правовая среда с точки зрения распространения технологии по миру, обозначены цели устойчивого развития и проанализированы остаточные риски кибербезопасности современных сетей [176].

Во второй стадии будет сделан упор на обеспечение исключительной производительности радиосвязи в направлении 6G за счет разработки и оценки ключевых компонентов радиотехники для следующего поколения с помощью более высоких диапазонов и локализации/зондирования. В рамках этой стадии будут разработаны ключевые инновационные технологии обеспечения радиосвязи для достижения сверхвысокой скорости передачи данных и пропускной способности с учетом аппаратных и канальных аспектов, а также будут соединены физический и цифровой миры с помощью передовых подходов к локализации и зондированию [176].

Третья стадия подключит интеллект к 6G путем предоставления методологии, алгоритмов и архитектурных требований для сети, основанной на искусственном интеллекте и управляемой им. Эта стадия проекта повысит производительность воздушного интерфейса 5G/6G за счет внедрения решений на основе искусственного интеллекта низкой сложности, а также предложит концепции дизайна для обучающей платформы 5G/6G, способной оптимально поддерживать и решать распределенные рабочие нагрузки [176].

В заключительной, четвертой стадии проекта планируется эволюция сети и расширение в направлении 6G, где будут предоставлены средства для создания интеллектуальной сети сетей за счет деагрегирования сети и динамической надежности. В рамках этой стадии будут разработаны архитектурные компоненты, которые смогут поддерживать новый гибкий сетевой дизайн, полную интеграцию искусственного интеллекта и программируемость сети. С реализацией последних задач четвертой стадии Неха-Х будет повышена производительность сети 5G/6G в экстремальных условиях, где сходятся цифровой, физический и человеческий миры благодаря функциональности специального назначения (например, гибкое модульное производство, связь с нулевым энергопотреблением для датчиков и др.) [176].

3.5 Причины закрытия неудавшихся проектов

Среди проектов в сфере киберфизических систем присутствуют и те, которые были закрыты или отменены до своего полноценного выхода в свет. Среди основных причин закрытия или отмены проектов можно отметить следующие:

1. Экономический кризис компании (замедленные темпы роста, экономический спад);
2. Смена курса в направлении развития технологии;
3. Слабая окупаемость проекта;
4. Устарелость и неактуальность разрабатываемой технологии;
5. Противоречия и разногласия между заказчиком и исполнителем.

Так, в октябре 2022 года компания Amazon закрыла два своих проекта по киберфизическим системам в рамках рабочей группы по робототехнике Amazon. Первым из таких проектов был мини-робот Scout, занимающийся

доставкой товаров на дом и запущенный впервые в 2019 году. Второй проект – Canvas, в рамках которого разрабатывались и выпускались роботы, предназначенные для транспортировки предметов на складах. Canvas также был запущен в 2019 году в качестве стартапа и в тот момент сумел собрать более 100 млн долл. на старте. Сама компания отмечает, что такие сокращения проектов прежде всего вызваны необходимостью пересмотреть финансовые затраты компании в связи с замедленными темпами ее роста и грядущим экономическим спадом. Кроме этого, Amazon заявила об изменении вектора исследований в сфере робототехники. Также, представители компании отмечают, что технологии, разработанные в рамках Scout и Canvas будут и дальше применяться внутри компании и послужат основой для будущих технологий в этой области [177].

Компании Ford и Volkswagen также заявили о закрытии одного из своих стартапов – Argo AI, искусственного интеллекта для автоматизированных автомобилей. Проект был запущен еще в 2017 году и в общей сумме собрал более 2,7 млрд долл. инвестиций, однако, начиная с октября 2022 года, проект закрывается, а его существующие технологии переходят к Ford и Volkswagen. Основными причинами закрытия проекта являются снижение окупаемости технологии, а также изменение вектора развития технологий компаний – теперь обе компании больше сосредоточены на разработке расширенных вспомогательных систем помощи водителю, а не на автоматизированной технике. Обе компании также заявили, что текущие решения, которые были выпущены Argo AI, также останутся коммерческими в плане доступа, а технологии перейдут в существующие проекты компаний, такие как Ford Escape Hybrids [178].

2 года назад компания Google остановила свой проект по созданию цифровой модели города Торонто, Канада. Дочерняя компания Google Sidewalk Labs на протяжении нескольких лет занималась разработкой и созданием «умного» города Торонто с использованием передовых технологий, таких как автоматизированные транспортные средства, цифровые двойники и др. Проект был остановлен в 2020 году по причине внутренних несогласованностей правительства Торонто и компании, а также в связи с сильным экономическим спадом на фоне обострения эпидемии коронавирусной инфекции COVID-19. Кроме этого, представители Sidewalk Labs отмечали, что многие их наработки по этому проекту успели устареть, появились более актуальные технологии, отвечающие современным вызовам [179].

ГЛАВА 4. ОСНОВНЫЕ ТЕХНОЛОГИИ И РАЗРАБОТКИ НА РЫНКЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В ПРИМЕНЕНИИ К «СКВОЗНЫМ» ТЕХНОЛОГИЯМ НАПРАВЛЕНИЯ «ТЕХНЕТ» НТИ

4.1 Основные технологии, применяемые на рынке киберфизических систем

Цифровая трансформация производственной сферы и других сфер экономики предполагает разработку инновационных методов внедрения киберфизических систем в технологические, производственные и бизнес-процессы компаний. Как было отмечено ранее развитие киберфизических систем тесно взаимосвязано с рядом технологий, которые отчасти рассматриваются в рамках направления «Технет» НТИ:

- Цифровое проектирование и моделирование;
- Робототехника;
- Промышленный (Индустриальный) Интернет;
- Промышленная сенсорика;
- Новые материалы;
- Аддитивные технологии;
- Большие данные.

Киберфизические системы интегрируют взаимодействующие между собой физические и цифровые/виртуальные/информационные компоненты. К элементам физической среды (аппаратной) зачастую относят [102; 180]:

1. Робототехническое оборудование и устройства;
2. Средства сбора и/или обработки информации из внешней среды (датчики, сенсоры и проч.)⁴.

К элементам информационной (виртуальной) среды чаще всего относят:

1. Технологии проектирования и моделирования (системы автоматизированного проектирования, средства управления технологическими и бизнес-процессами, цифровые двойники и проч.);
2. Интернет вещей;
3. Облачные вычисления;
4. Большие данные.

Совершенствование основных технологий, применяемых на рынке киберфизических систем, представленных выше, способствует развитию новых «умных» материалов и аддитивных технологий производства. Их использование позволяет повысить эффективность процессов прототипирования и создания конечной продукции с определенными заданными свойствами, а также ускорить процесс цифровой трансформации, в том числе может положительно сказаться на степени внедрения КФС в производственные и технологические процессы предприятий. Учитывая это, новые материалы и аддитивные технологии также были рассмотрены в ходе анализа, результаты представлены в Приложении 6. Дополнительные материалы исследования по направлениям «новые материалы» и «аддитивные технологии».

4.1.1 Физические компоненты киберфизических систем

Робототехническое оборудование и устройства

Робототехника является одной из основных технологий КФС. От надежности и производительности внедренных специализированных робототехнических комплексов зависит работа систем КФС, где подобные решения реализованы. Использование робототехнического оборудования позволяет автоматизировать производственные и

⁴ Средства сбора и/или обработки информации из внешней среды были вынесены в отдельный пункт с целью разделения составляющих КФС на физические и виртуальные компоненты несмотря на то, что устройства сбора и/или обработки информации из внешней среды являются частью технологий Интернета вещей.

технологические процессы предприятий, что приводит к повышению производительности, уровня безопасности производств, улучшению качества выпускаемой продукции, а также к снижению издержек и сроков изготовления.

Таблица 4. Робототехническое оборудование и устройства

Робототехническое оборудование и устройства	
Функции	Выполнение основных технологических операций (сварка, формообразование, окрашивание и др.)
	Выполнение вспомогательных операций (транспортные операции, складирование и др.)
	Выполнение пространственных перемещений со сложной траекторией
	Манипуляции с деталями (выкладка, сборка, соединение и др.)
	Мониторинг, контроль качества и проверка безопасности
Области применения	«Умные дома», «Умные города», «Умное производство»
	Пищевая и перерабатывающая промышленность
	Торговля
	Медицина и фармацевтика
	Строительство и недвижимость
	Транспорт и логистика
	Авиационная и аэрокосмическая отрасли
	Телекоммуникационная отрасль
	Электроэнергетика
Технологии/ решения в основе	Недропользование
	Промышленные роботы (универсальные, сборочные, сварочные, окрасочные, перегрузочные, обрабатывающие и др.)
	Сервисная робототехника (роботы для профессиональной уборки, роботы для обследования и технического обслуживания, роботы для строительства и сноса и др.)
	Технологии сбора информации
	Технологии искусственного интеллекта
Эффекты от внедрения	Автоматизация производства и рациональное использование производственных площадей
	Минимизация или полное исключение влияния человеческого фактора
	Повышение точности и качества выполнения технологических операций
	Увеличение времени безотказной работы (срока службы оборудования)
	Снижение влияния человеческого фактора
	Снижение затрат и себестоимости продукции
	Автоматизация производственного процесса и внедрение робототехнического оборудования может окупиться в течение 1–3 лет [181]
Средний уровень УГТ	УГТ7–9 (по миру)
	УГТ6–9 (по России)
Компании-разработчики/ производители (примеры)	

Источники: МГУ имени М.В.Ломоносова на основе данных МИР, ГБУ АПР, 2020 [182; 183]

Уровень промышленной автоматизации в России остается сравнительно низким. Плотность роботизации в России (количество промышленных роботов на 10 000 рабочих мест в отрасли), которая демонстрирует уровень

использования промышленных роботов в стране, имеет показатель, равный 6, в то время как, среднемировая плотность роботизации – 113 [184]. Данный фактор негативным образом влияет на темпы роста рынка производственных КФС, включающих роботизированные устройства.

Для России также характерно наличие большого числа специалистов, компетентных в сервисной робототехнике нежели в промышленной – соотношение промышленных и сервисных робототехников в России составляет 1:10 [183]. Среди сдерживающих факторов развития робототехники в России можно выделить [182]:

- длительные сроки проведения НИР/ НИОКР;
- высокую стоимость роботизации существующий производственной инфраструктуры/ создания новой, необходимой для внедрения КФС;
- недостаточное количество отечественной радиоэлектронной аппаратуры и элементной компонентной базы (сервомоторы, редукторы, контроллеры и проч. преимущественно импортируются) для интеграции робота в производственный процесс;
- недостаточное количество профессиональных специалистов.

Для повышения автономности и адаптируемости КФС необходимо активно внедрять робототехническое оборудование и устройства, которые позволяют автоматизировать производственные процессы. В робототехнических комплексах также могут быть использованы технологии искусственного интеллекта, Интернета вещей, облачных вычислений и новых материалов, посредством которых могут быть созданы более эффективные и автономные КФС.

Средства сбора и/ или обработки информации из внешней среды

Получение данных в режиме реального времени и их дальнейшая обработка являются обязательным условием для существования автономных промышленных киберфизических систем. Данные внешней среды преобразуются в стандартизированную информацию с помощью технологий промышленной сенсорики и «умных» датчиков.

«Умная» сенсорика может самостоятельно обрабатывать, передавать собранные данные измерений, а в отдельных случаях воздействовать на внешний мир с помощью дополнительных исполнительных механизмов. Интеллектуальные датчики обеспечивают более точный и автоматизированный сбор данных о внешней среде с меньшим количеством возможных ошибок. Интеллектуальные средства сбора и обработки информации, как правило, состоят из трех основных компонентов: сенсоров/ датчиков, микропроцессора и средств коммуникации [185]. «Умные» сенсоры и датчики анализируют поступающую извне информацию и позволяют анализировать факторы внешней среды и на их основе в автоматическом или полуавтоматическом режиме оптимизировать работу элементов КФС.

Таблица 5. Средства сбора и/ или обработки информации из внешней среды

Средства сбора и/ или обработки информации из внешней среды	
Функции	Сбор и обработка информации
	Измерение и мониторинг параметров внешней среды
	Контроль и оптимизация операционной деятельности/ процессов
	Идентификация и обнаружение тенденций, отклонений и причинно-следственных связей
	Отправка данных для обработки на удаленный сервер
	Анализ изображений с учетом изменчивости
Области применения	«Умные дома», «Умные города», «Умное производство»
	Пищевая и перерабатывающая промышленность
	Торговля
	Медицина и фармацевтика
	Строительство и ЖКХ
	Транспорт и логистика
	Авиационная и аэрокосмическая отрасли

Средства сбора и/ или обработки информации из внешней среды	
	Телекоммуникационная отрасль
	Электроэнергетика
	Недропользование
Технологии/ решения в основе	Сенсоры и датчики (измерения температуры, давления, инфракрасные датчики и проч.)
	Сенсорные сети
	Технологии искусственного интеллекта, в том числе машинное зрение
	Граничные вычисления
Эффекты от внедрения	Снижение затрат (экономия рабочего пространства, количества используемых материалов и проч.)
	Оптимизация текущих процессов и увеличение производительности
	Минимизация влияния человеческого фактора
	Более быстрое и качественное выявление дефектов, нарушений, и предотвращение аварийных ситуаций
	Сокращение времени простоя оборудования
Средний уровень УГТ	УГТ7-9(по миру)
	УГТ5-9(по России)
Компании-разработчики/ производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных Straits Research, TechTarget, 2020–2022 [186; 187]

Интеллектуальные средства сбора и обработки информации предоставляют возможность получения максимально полной и объективной информации о состоянии оборудования, технологических процессах, производстве в целом и внешних данных в контексте КФС. К факторам, которые стимулируют развитие рынка «умных» датчиков, относят:

- развитие технологий беспроводной связи 5G;
- повсеместное внедрение Интернета вещей или Промышленного интернета;
- использование граничных вычислений;
- внедрение и стандартизацию беспроводных технологий передачи данных с пониженным энергопотреблением или аккумулярованием энергии извне;
- ускорение темпов цифровой трансформации.

При этом множество предприятий до сих пор не используют «умные» датчики, объединенные в сеть и трансформирующие параметры объектов внешней среды в цифровой формат [188]. Развитие рынка промышленной сенсорики предполагает преодоление ряда сдерживающих факторов, таких как [188]:

- высокая стоимость внедрения решения (необходимо снижение стоимости оборудования и радиоэлектронных компонентов, которые используются в производстве «умных» датчиков);
- низкий уровень мобильности большинства видов датчиков и сенсоров;
- высокая энергозависимость устройств (необходимо регулярное обновление батарей и/ или обеспечение бесперебойного доступа к сети питания);
- наличие уязвимости к кибератакам, высокая вероятность утечки данных;
- наличие проблем конфиденциальности и приватности собираемых данных.

Российский рынок решений «умных» датчиков несколько отстает от общемирового. Это связано с недостаточно развитой соответствующей информационной инфраструктурой, отсутствием единых стандартов и протоколов

организации сетевого взаимодействия, а также конфиденциальностью собираемых и передаваемых данных. Реализованные отечественные проекты в сфере Интернета вещей крайне разрознены, в них не заданы и не определены в необходимой мере стандарты взаимодействия датчиков друг с другом, иными элементами КФС и с внешней средой [189].

Одними из наиболее важных задач, решение которых может способствовать развитию отечественных решений «умных» датчиков, являются:

- разработка государственных стандартов в сфере сетевого взаимодействия, Интернета вещей и Промышленного интернета;
- преодоление проблем конфиденциальности собираемых и обрабатываемых данных;
- разработка соответствующих государственных стандартов информационной безопасности и кибербезопасности;
- формирование упрощенного процесса получения патентов и лицензий для «умных» средств сбора и обработки информации из внешней среды.

Наличие системы датчиков и сенсоров необходимы в современных КФС. Развитие отечественного рынка решений «умных» устройств сбора и/или обработки информации является важным условием трансформации производственных мощностей и создания новых высокотехнологичных производств, так как интеллектуальные датчики и сенсоры являются одной из движущих сил перехода к Индустрии 4.0.

4.1.2 Информационные (виртуальные) компоненты киберфизических систем

Технологии проектирования и моделирования

В настоящее время различные промышленные предприятия, медицинские организации и иные компании внедряют решения автоматизации и роботизации производства с целью усовершенствования процессов управления и повышения уровня цифровой интеллектуализации. Данные технологии неразрывно связаны с использованием дополнительных инструментов и субтехнологий проектирования, моделирования, анализа и управления

Технологии цифрового проектирования и моделирования представляют собой совокупность средств, которые в том числе обеспечивают реализацию концепции передового «умного производства» (smart manufacturing), необходимого для создания современных глобально конкурентоспособных технологических продуктов нового поколения. Цифровое проектирование и моделирование включает в себя набор технических средств, таких как системы автоматизированного проектирования, системы управления производственными и технологическими процессами и другие.

Таблица 6. Технологии проектирования и моделирования

Технологии проектирования и моделирования	
Функции	Математическое моделирование и разработка технических систем и конструкций (включая 2D-моделирование и 3D-моделирование)
	Компьютерный и суперкомпьютерный инжиниринг
	Технологическая подготовка производства
	Складская логистика
	Управление данными о продукте и жизненным циклом продукта
	Оптимизация и автоматизация бизнес-процессов
	Мониторинг использования ресурсов в режиме реального времени и отслеживание показателей качественных характеристик продукции
	Контроль производства изделия
	Моделирование поведения объекта во всех ситуациях, включая аварийные, с высокой степенью точности
Области применения	Пищевая и перерабатывающая промышленность

Технологии проектирования и моделирования	
	Медицина и фармацевтика
	Строительство
	Транспорт и логистика
	Авиационная и аэрокосмическая отрасли.
	Телекоммуникационная отрасль
	Электроэнергетика
	Недропользование
Технологии/ решения в основе	Системы автоматизированного проектирования (PLM, CAD, ECAD, EDA, CAE, CAM, PDM, CAPP)
	Средства управления технологическими и бизнес-процессами (BPM, APC, RTO, MES, ACU ТП, SCADA, SPDM, WMS, SCM, ECM, MDM)
	Технологии цифровых двойников (математическое моделирование (ММ), имитационное моделирование)
Эффекты от внедрения	Повышение скорости проектирования и упрощение процессов проектирования продукта в 1,5–2 раза
	Уменьшение затрат на изготовление изделий до 20%
	Повышение надежности систем при обработке больших объемов данных, многоуровневых схем бизнес-процессов и сложных транзакций
	Более эффективная и обоснованная система поддержки принятия решений
	Упрощение испытательного и промышленного контроля состояния продукта
	Снижение влияния человеческого фактора и повышение безопасности конечного продукта
	Быстрое обнаружение дефектов продукта и сокращение количества дефектов во время производственных процессов
Средний уровень УГТ	УГТ8–9 (по миру)
	УГТ7–9 (по России)
Компании-разработчики/ производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных АО «Кодекс», Ассоциации «Технет», 2021–2022 [190; 191]

Объекты, относящиеся к КФС, должны в меньшей степени зависеть от человеческого фактора или быть полностью автономными. Ввиду этого использование современного ПО, в том числе выполняющего функции моделирования, автоматизированного проектирования и управления производственными процессами (системы автоматизированного проектирования, средства управления технологическими и бизнес-процессами, технологии цифровых двойников), является одним из условий внедрения КФС и совершенствования производственных процессов в целом.

Развитию рынка средств проектирования и моделирования в России способствуют не только тенденции цифровой трансформации, но и политика государства в отношении импортозамещения зарубежного ПО, которая способствует разработке отечественных решений. Однако в качестве факторов, сдерживающих рост рынка в России, можно выделить:

- нехватку цифровых унифицированных нормативных требований;

- сложность лицензирования ПО;
- отсутствие или недостаточность правовой и финансовой поддержки технологического трансфера (обмена правами на результаты интеллектуальной деятельности между оборонными и гражданскими предприятиями).

В среднем по миру и по России УГТ цифрового проектирования и моделирования в общей сложности схож. Однако готовые отечественные системы автоматизированного проектирования, средства управления технологическими и бизнес-процессами не в полной мере соответствуют уровню их иностранных аналогов: зарубежные решения зачастую являются более гибкими, функциональными и универсальными. Одними из наиболее важных задач, решение которых может способствовать развитию отечественных решений цифрового проектирования и моделирования, являются [192]:

- выстраивание системы технологического трансфера;
- развитие суперкомпьютерных технологий;
- разработка новых модулей ПО;
- интеграция решений различного класса.

Тенденции цифровой трансформации, внедрение облачных сервисов, интегрированных решений Интернета вещей и проч., способствуют повышению уровня взаимодействия физических и вычислительных компонентов систем с внешней средой. Данные факторы также положительным образом влияют на рост рынка цифрового проектирования и моделирования в рамках реализации «умного производства» и КФС в целом.

Интернет вещей

Киберфизические системы схожи с Интернетом вещей, как упоминалось ранее, но являются более сложными и обширными, могут использовать элементы Интернета вещей для связи источников и адресатов данных. С целью повышения автономности, появления способности к самонастройке и самообучению КФС необходимо объединять совокупность данных элементов посредством технологий Интернета вещей.

Интернет вещей – это совокупность объектов и устройств, объединенных компьютерной сетью и оснащенных специализированным ПО, датчиками, сенсорами и другими технологиями, которые собирают, анализируют, обрабатывают и передают данные другим объектам [193].

Отдельно стоит выделить понятие промышленного (индустриального) Интернета вещей – объединенную совокупность машин, облачных вычислений и других единиц производственного оборудования с целью обеспечения управления технологическим циклом, повышения эффективности и производительности промышленных процессов [194]. Концепция Интернета вещей и Промышленного интернета также позволяет расширить возможности межмашинного взаимодействия – общность технологий, которые позволяют различным приборам и датчикам обмениваться между собой информацией [195].

Таблица 7. Интернет вещей

Интернет вещей	
Функции	Сбор, хранение и анализ данных с устройств
	Прогнозная аналитика
	Мониторинг состояния и использования ресурсов
	Профилактическое обслуживание (выявление потенциальных неисправностей до того, как они повлияют на производство)
	Технологии управления данными о продукте и жизненным циклом продукта
	Оптимизация и автоматизация бизнес-процессов
	Осуществление управляемого подключения множества устройств
Области применения	«Умные дома», «Умные города», «Умное производство»
	Пищевая и перерабатывающая промышленность

Интернет вещей	
	Медицина и фармацевтика
	Строительство
	Транспортная система (морской, речной, железнодорожный транспорт) и логистика
	Авиационная и аэрокосмическая отрасли.
	Телекоммуникационная отрасль
	Электроэнергетика
	Недропользование
Технологии/ решения в основе	Специализированные протоколы передачи данных
	Технологии проводной передачи данных
	Технологии беспроводной передачи данных
Эффекты от внедрения	Потенциальный экономический эффект для мировой экономики к 2030 году – от 5,5 до 12,6 трлн долл. США в год
	Цифровизация предприятий и внедрение новых бизнес-моделей
	Минимизация влияния человеческого фактора и исключения ошибок
	Постоянный мониторинг информационных потоков
	Повышение вовлеченности сотрудников и клиентов
Средний уровень УГТ	УГТ5–9 (по миру)
	УГТ4–8 (по России)
Компании-разработчики/ производители (примеры)	

Источники: МГУ имени М.В.Ломоносова на основе данных Thomas, РБК, 2021–2022 [196; 197]

К факторам, которые стимулируют развитие рынка Интернета вещей, можно отнести:

- рост объемов и скорости передачи информации, а также модернизация технологий 4G и 5G;
- разработку новых объектов хранения данных;
- распространение инновационных методов анализа и сегментирования единой исходной информации.

Сегодня технология Интернета вещей хоть и является неотъемлемой частью многих предприятий и компаний, но все еще находится на стадии своего развития. Рынок Интернета вещей столкнулся с рядом препятствий [198], включая:

- сложность управления изменениями (компании зачастую рассматривают Интернет вещей как некий технологический проект, но не в качестве нового подхода к трансформации всей операционной модели бизнеса);
- проблемы совместимости различных решений (ландшафт Интернета вещей содержит множество частных обособленных экосистем);
- нерешенные проблемы кибербезопасности и конфиденциальности данных.

Для России характерно некоторое отставание в сфере развития Интернета вещей. Большое количество инициатив в сфере Интернета вещей находится на начальной стадии разработок и внедрения. Решения и устройства в данной области малочисленны по номенклатуре и по объему производства, при этом уже существуют

конкурентоспособные технологии Интернета вещей [199]. Особое отставание отмечается в сфере внедрения инновационных подходов к построению сетей (развертывании гибридных облачных инфраструктур), которые необходимы для формирования платформ и приложений Интернета вещей [200]. Одними из наиболее важных задач, решение которых может способствовать развитию отечественных решений Интернета вещей, являются [192]:

- формирование национальных стандартов и нормативов в сфере Интернета вещей;
- внедрение единых требований к совместимости устройств и сетей;
- регулирование в сфере сертификации продуктов и услуг рынка Интернета вещей;
- интеграция решений различного класса.

Ускорение темпов всеобщей цифровизации, автоматизации процессов производства, внедрение облачных технологий, развертывания сетей 4G и 5G способствует развитию рынка Интернета вещей и положительным образом влияет на повышение спроса на решения Интернета вещей. Важным условием распространения технологий Интернета вещей и интеграции с КФС с целью повышения уровня взаимодействия физических и вычислительных компонентов с внешней средой является дальнейшее совершенствование смежных технологий и снижение стоимости их внедрения. Во избежание технологического отставания следует осуществлять разработку и вводить к эксплуатации решения Интернета вещей системным образом, а также активно участвовать в проектах по развертыванию гибридных инфраструктур в тех сферах деятельности, где это необходимо.

Облачные вычисления

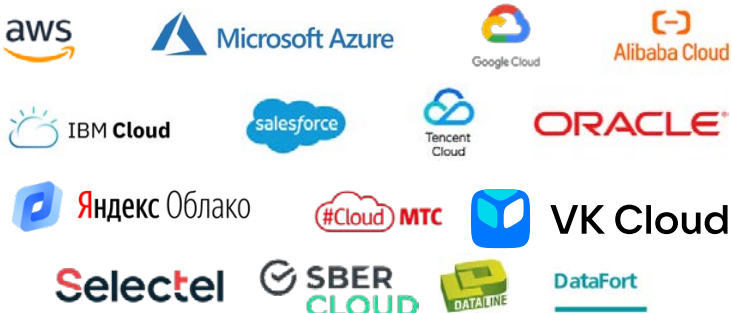
Облачные вычисления играют ключевую роль в глобальной цифровой трансформации, так как посредством данных технологий хранятся и обрабатываются огромные массивы данных из внешней среды. Облачные вычисления являются одной из основ Индустрии 4.0, а также обеспечивают тесную связь и координацию между виртуальными и аппаратными ресурсами КФС [201].

Облачные вычисления (Cloud computing) – это концепция, предоставляющая возможность сетевого повсеместного доступа к масштабируемому и эластичному пулу физических и вычислительных ресурсов с опциями самообслуживания и администрирования [202]. Совокупность данных технологий используется для централизации всех данных и сервисов компании, с которыми пользователь взаимодействует через веб-браузер или специальное приложение.

Современные облачные решения включают в себя вычислительные мощности (серверы), хранилища данных, базы данных, специальное ПО для анализа и трансформации данных, сетевые технологии и иные аналитические инструменты. Эффектами от внедрения и использования данных технологий являются: повышенная скорость, масштабируемость и гибкость технологических процессов компании, и также улучшенная работа элементов КФС, основанных на сборе и аналитике данных.

Таблица 8. Облачные вычисления

Облачные вычисления	
Функции	Увеличение вычислительных мощностей без расширения инфраструктуры
	Объединение ресурсов для обслуживания большого числа пользователей и потребителей
	Создание платформы для совместной работы и обмена данными
	Обеспечение универсального доступа по сети
	Аварийное восстановления данных
	Контроль над всеми данными компании, включая конфиденциальную информацию
	Использование корпоративных данных в любой момент времени (мобильный доступ)
Области применения	«Умные дома», «Умные города», «Умное производство»
	Пищевая и перерабатывающая промышленность
	Торговля
	Медицина и фармацевтика
	Строительство и ЖКХ

Облачные вычисления	
	Транспорт и логистика
	Авиационная и аэрокосмическая отрасли
	Телекоммуникационная отрасль
	Электроэнергетика
	Недропользование
Технологии/ решения в основе	Интернет-технологии (сервисно-ориентированная архитектура, Web 2.0, веб-сервисы и проч.)
	Аппаратное обеспечение (вычислительные технологии, технологии виртуализации и проч.)
	ПО управления облачными системами (автономные центры обработки данных и проч.)
	Распределенные вычисления
Эффекты от внедрения	Снижение капитальных затрат (собственное оборудование, помещение и др.)
	Снижение затрат на инфраструктуру на 15–40% [203]
	Оптимизация текущих процессов и увеличение производительности на 25–30% [203]
	Мгновенное предоставление рабочего виртуального пространства для разработки и тестирования
	Гибкое реагирование на изменения вычислительных потребностей
	Снижение нагрузки на штатных ИТ-специалистов компании
	Минимизация влияния человеческого фактора в процессах обработки данных
Средний уровень УГТ	УГТ8–9(по миру)
	УГТ7–9 (по России)
Компании-разработчики/ производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных Statista, VC.ru, BCG, 2020–2022 [203–205]

В 2022 году облачные решения широко используются практически во всех отраслях экономической деятельности, в особенности в высокотехнологичных отраслях. Процессы внедрения облачных технологий были ускорены глобальной пандемией COVID-19 и продолжительными периодами локдаунов. К факторам, которые стимулируют развитие рынка облачных вычислений, относят [206]:

- внедрение гибридной рабочей модели (облачные решения поддерживают режим совместной удаленной работы);
- внедрение технологий Искусственного интеллекта и Машиного обучения (облачная инфраструктура необходима для работы приложений, так как может хранить достаточный объем данных и вычислительных мощностей);
- распространение модели ХааS («все как сервис» – все услуги, которые оказываются через интернет и с применением облачных вычислений);
- распространение тенденций устойчивого развития.

Несмотря на бурное развитие индустрии облачных вычислений, стоит выделить сдерживающие факторы, среди которых [207]:

- наличие проблем конфиденциальности и приватности собираемых данных;

- отсутствие гибкости нормативных требований по защите данных;
- высокая уязвимость к кибератакам и утечкам данных;
- ограниченный контроль над функционалом облака;
- нехватка экспертов/ ИТ-специалистов в сфере облачных технологий.

Отечественные технологии облачных вычислений несколько отстают по темпам развития от общемировых в связи с тем, что в России еще полностью не сформированы единые стандарты и протоколы взаимодействия при работе с данными, в том числе конфиденциальными. При этом наблюдается рост на российском рынке облачных сервисов, в большей степени связанный с повышением спроса на подобные решения: постепенный переход сотрудников на удаленный формат работы, перевод локальных технологических и бизнес-систем (бухгалтерия, CRM и проч.) в облако, государственное стимулирование внедрения облачных решений в органы власти. При этом имеется ряд задач, решение которых может способствовать развитию отечественных облачных решений, в том числе:

- введение стандартов обмена данными в разрезе облачных сервисов;
- обеспечение информационной безопасности и защиты конфиденциальных данных;
- воспроизводство импортозамещающих технологий;
- усиление компетенций ИТ и телеком-провайдеров.

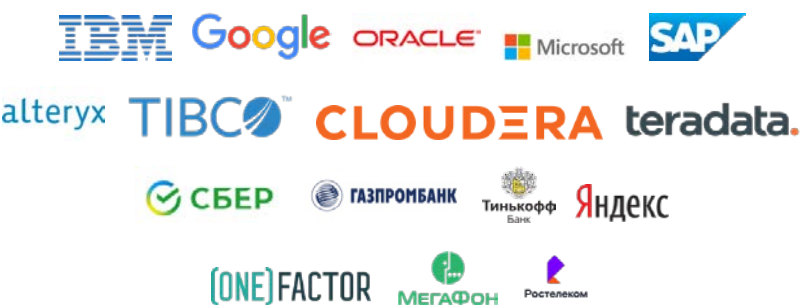
Облачные вычисления являются одним из главных инструментов реализации концепции Индустрии 4.0 и цифровой трансформации. Создание и внедрение производительных КФС не может быть достигнуто в полной мере без их интеграции с технологиями облачных вычислений.

Большие данные

Важной особенностью цифровой трансформации является непрерывное использование слабоструктурированных больших массивов данных [102]. КФС в режиме реального времени получают из внешней среды различные по объему и типу данные. Большие данные представляют собой совокупность технологий сбора, обработки и структуризации массивов гетерогенной информации, которые отличаются следующими характеристиками: тип, размер, скорость обработки и вариативность, что требует использования технологий масштабирования с целью эффективного управления информацией [208]. Преимуществом использования технологий Больших данных является наличие возможности обнаружения данных, имеющих потенциальную ценность, ранее не очевидных.

Таблица 9. Большие данные

Большие данные	
Функции	Сбор, обработка и анализ больших массивов данных
	Формирование баз данных и структурирование разрозненного информационного контента
	Аналитика (описательная, прогнозная, предиктивная и диагностическая)
	Обеспечение доступа ко всему объему постоянно изменяемых данных
	Защита данных (обнаружение несанкционированного доступа и выполнение нормативных требований)
	Аналитика для разработки и запуска продуктов и сервисов
	Анализ клиентского опыта
Области применения	«Умные дома», «Умные города», «Умное производство»
	Пищевая и перерабатывающая промышленность
	Торговля
	Медицина и фармацевтика
	Строительство и недвижимость
	Транспорт и логистика
	Авиационная и аэрокосмическая отрасли
	Телекоммуникационная отрасль

Большие данные	
Технологии/ решения в основе	Электроэнергетика
	Недропользование
	Специальное ПО для работы с базами данных (NoSQL, MapReduce, Hadoop, R и проч.)
	Технологии трансформации необработанных больших данных в полезную информацию (data mining)
Эффекты от внедрения	Инструменты визуализации аналитических данных
	Более качественное и быстрое принятие решений
	Оптимизация текущих процессов и увеличение производительности
	Минимизация влияния человеческого фактора
	Повышение эффективности мониторинга информационных потоков
Средний уровень УГТ	УГТ5-9 (по миру)
	УГТ3-8(по России)
Компании-разработчики/ производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных РБК, Markets and Markets, группы «Деловой Профиль», IBM, 2020–2021 [28; 209–211]

Повсеместное внедрение цифровых технологий приводит к увеличению объемов данных, которые собираются, обрабатываются, передаются и используются в оцифрованном формате. Технологии Больших данных предоставляют возможность хранения подобных массивов информации в различных форматах, а также их качественного быстрого анализа. К факторам, которые стимулируют развитие рынка Больших данных, относят [28]: увеличение объема собираемых данных (около 90% мировых данных было сформировано за период 2020–2021 годы); повышение темпов роста машинно-генерируемых данных; развитие и внедрение технологий Интернета вещей, Искусственного интеллекта; ускорение темпов цифровой трансформации.

В настоящий период времени Большие данные являются одним из приоритетных направлений цифровизации многих предприятий и компаний. Однако развитие рынка технологий Больших данных предполагает преодоление ряда сдерживающих факторов, таких как [209]:

- неоднородность данных, разрозненность источников информации, форматов и качества данных;
- высокие затраты на эксплуатацию вычислительных мощностей (серверов), необходимых для работы с большими массивами данных;
- повышенная уязвимость к кибератакам и утечкам данных;
- наличие проблем конфиденциальности и приватности собираемых данных.

Российский рынок Больших данных находится на стадии своего зарождения и формирования. Дефицит компетентных специалистов и недорогих масштабируемых ресурсов хранения и обработки информации (объектов инфраструктуры), наличие опасений потенциальных пользователей относительно конфиденциальности данных, а также ограничение способов получения и обмена данными являются основными барьерами развития отечественного рынка решений [212]. Однако существует некоторое количество апробированных решений, которые уже сегодня можно использовать для работы с большими объемами неструктурированных данных, а также в КФС [209].

На территории России использование компаниями методов Больших данных неравномерно, в разных индустриях уровень внедрения сильно различается (лидируют банковская сфера и сфера услуг). Одними из наиболее важных задач, решение которых может способствовать развитию отечественных решений Больших данных, являются [210]:

- разработка государственных стандартов сбора и обработки больших объемов данных с фокусом на их стандартизацию;
- обеспечение возможности обмена данных (поощрение обмена отраслевыми данными через саморегулируемые стандарты, обмена анонимными персональными данными на коммерческой основе, обмена релевантными государственными данными с частным сектором);
- формирование упрощенного процесса получения патентов и сертификатов для продуктов и услуг на основе Больших данных.

С целью повышения автономности, самообучаемости и эффективности КФС необходимо внедрять технологии Больших данных, которые позволяют вычлнять из колоссальных объемов информации ценные данные. Интеграция этих технологий является основой для формирования Индустрии 4.0 и стимуляции технологических открытий и инноваций в сфере развития КФС.

4.2 Обзор ключевых научных разработок в России и мире по результатам библиометрического и патентного анализа

Одними из ключевых индикаторов, позволяющих сформировать базовое представление о степени заинтересованности компаний и предприятий страны в реализации научно-исследовательской деятельности, являются публикационная и патентная активности в разрезе заданной предметной области. Отдельно стоит отметить, что результаты патентного анализа в большей степени отражают области коммерческого интереса предприятий страны, поскольку они являются теми направлениями научно-технологического и инновационного развития, в разрезе которых организации вкладывают значительные финансовые средства для защиты собственной интеллектуальной собственности.

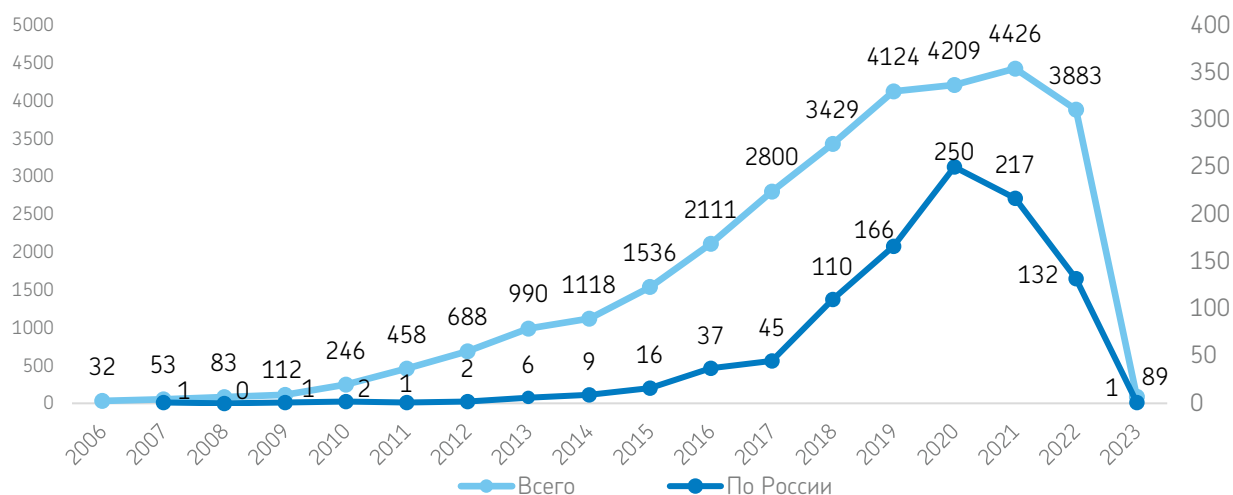
4.2.1 Результаты библиометрического анализа

В целях осуществления инновационной деятельности и разработки перспективных технологичных решений киберфизических систем отечественные и зарубежные компании реализуют по данной тематике научно-исследовательские работы. Анализ публикационной активности был реализован на основе данных библиографической и реферативной базы данных Scopus, для поиска был использован следующий запрос: «TITLE-ABS-KEY (cyber AND physical AND system)». В рамках библиометрического анализа публикационной активности по миру и России рассмотрены данные начиная с 2006 года по настоящее время, так как ранее 2006 года в базе Scopus не было внесено релевантных данных, подлежащих анализу.

В течение 2006–2022 годов наблюдается положительная динамика роста количества публикаций научных работ в области киберфизических систем или смежных тематик. За 2006–2023 годы в базе Scopus было зарегистрировано около 30,4 тыс. статей, отчетов о проведении конференций и проч.

Динамика публикационной активности по миру и по России в целом схожа: в течение 2007–2022 годов наблюдается постепенный рост количества опубликованных научных работ. Наибольший темп прироста по России был зафиксирован в 2019–2020 годах (50,6%), при этом в 2020 году было зарегистрировано наибольшее количество публикаций в сфере КФС – 250 публикаций. Среднегодовой темп прироста количества публикаций, посвященных исследованиям в области развития КФС, в базе данных Scopus по миру и по России за последние 10 лет (2013–2022 годы) равен 16,4% и 40,98% соответственно.

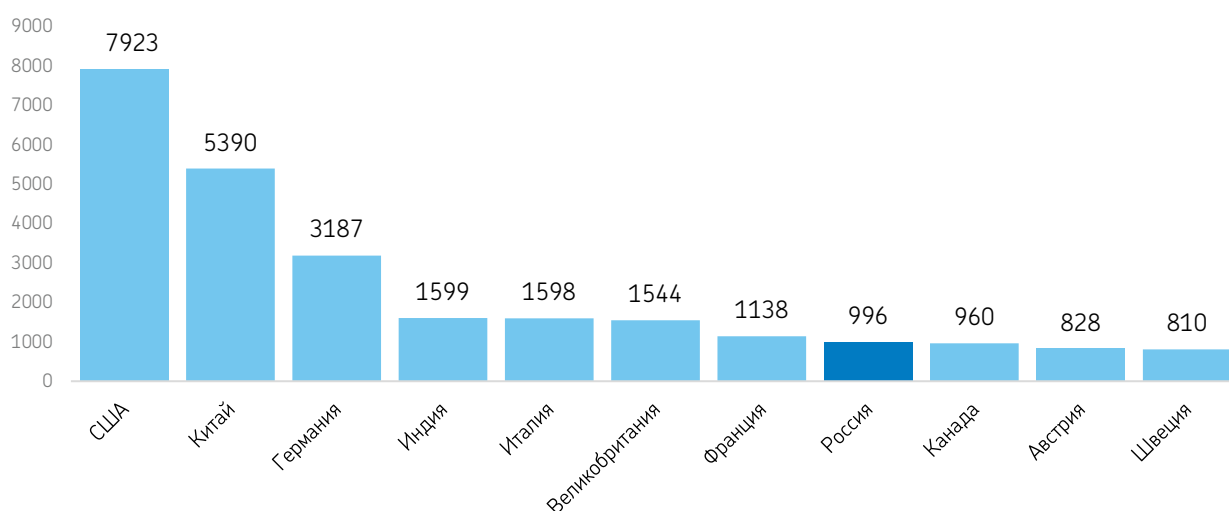
Рисунок 19. Количество научных публикаций в сфере КФС по годам (единиц, 2006–2023 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Лидирующие позиции по количеству публикаций занимают США, Китай и Германия (7,9 тыс., 5,4 тыс. и 3,2 тыс. публикаций соответственно). Россия же в данном рейтинге занимает 8 место с количеством публикаций, равным 996 единиц.

Рисунок 20. Количество научных публикаций в сфере КФС по странам (единиц, 2006–2023 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Публикация считается отнесенной к организации в том случае, если автор или соавтор публикации являлся участником ее составления и указал данные соответствующей организации. Наиболее часто встречающейся организацией являлось Министерство образования КНР (398 публикаций). При этом 3 из 5 наиболее распространенных организаций аффилиации располагаются на территории Китая. В топ-10 организаций аффилиации также входят научные и образовательные организации США (3 организации) и стран Европы (3 организации).

В России наиболее часто встречающимися организациями аффилиации являлись: Национальный исследовательский университет ИТМО, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН) и Санкт-Петербургский политехнический университет Петра Великого (СПбПУ). Большая часть

образовательных и научных организаций, которые опубликовали наибольшее количество публикаций, располагаются на территории Санкт-Петербурга.

Рисунок 21. Количество научных публикаций в сфере КФС по аффилиации (единиц, 2006–2023 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Рисунок 22. Количество научных публикаций в сфере КФС по аффилиации по России (единиц, 2007–2023 годы)

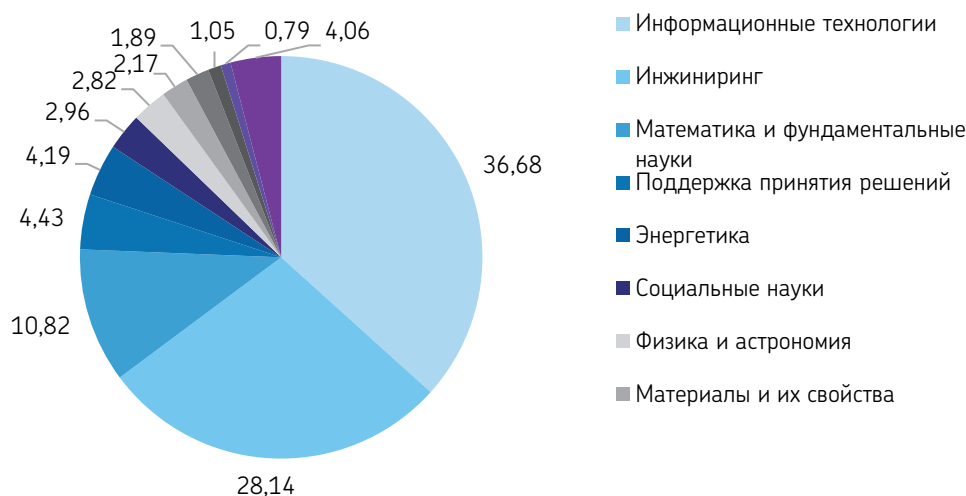


Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Наиболее популярными прикладными направлениями исследований в области КФС, согласно данным библиографической и реферативной базы данных Scopus, стали информационные технологии, инжиниринг, математика и фундаментальные науки и науки рассматривающие вопросы развития систем поддержки принятия решений. Наименее популярными сферами исследований на тему КФС стали области бизнес-администрирования, экологии

и химической инженерии.

Рисунок 23. Количество научных публикаций по предметной области по миру (% , 2006–2023 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Рисунок 24. Количество научных публикаций по предметной области по России (% , 2007–2023 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

В 2006–2023 годах наиболее популярными темами исследований в области КФС являлись:

- общие обозначения, термины, архитектура КФС;
- устройства Интернета вещей, исследование созависимости технологий Интернета вещей и КФС;
- Индустрия 4.0 и «умное» производство (обзор, тренды, прогнозы развития смежных технологий, в том числе КФС);
- прикладные исследования в области разработки КФС и проч.

Наиболее цитируемые работы, опубликованные на территории зарубежных стран, являются в большей степени обзорными и определяющими предметную область КФС и смежных с ними технологий. Отечественные публикации в большинстве своем являются прикладными и в меньшей степени обобщающими. Однако стоит отметить, что количество зарубежных публикаций в разы превышает количество отечественных научных работ, опубликованных в базе данных Scopus: прикладные работы зачастую являются менее популярными источниками данных, так как в

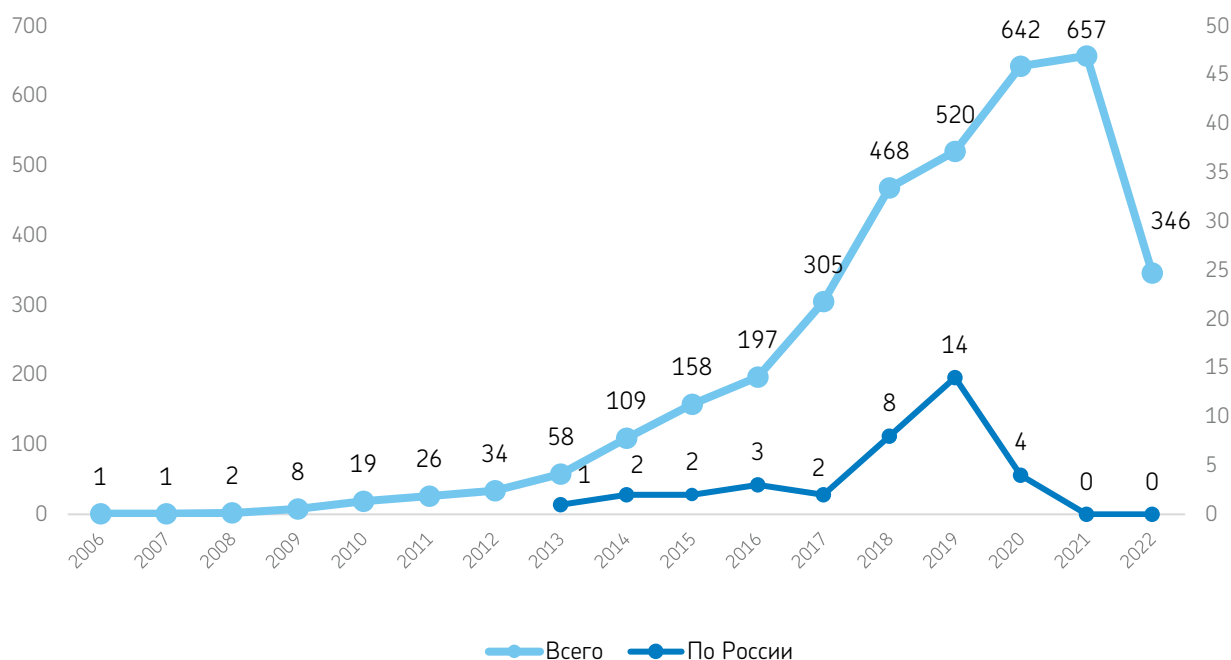
меньшей степени направлены на определение предметной области и описание объекта исследования в целом. Перечень публикаций с наибольшим количеством цитирований представлен в Приложении 7 Результаты библиометрического и патентного анализа.

4.2.2 Результаты патентного анализа

С целью создания перспективных технологичных решений в сфере киберфизических систем, а также получения исключительных прав на инновационные разработки, отечественные и зарубежные компании реализуют по данной тематике НИОКР, результатом реализации которых являются патенты. Анализ патентной активности был реализован на основе данных международной патентной базы данных Questel Orbit, для поиска был использован следующий запрос: «(((cyberphysical+) or (cyber 2D physical+)) 2D (system+))/TI/AB/DESC/ODES/KEYW». Патентный анализ по миру был проведен с 2006 года, по России – с 2013 года по настоящее время соответственно, так как ранее указанных периодов в Questel Orbit не было внесено релевантных данных, подлежащих анализу.

В рамках развития технологий КФС и защиты результатов интеллектуальной деятельности (получения патентов) в разрезе данной предметной области в течение 2006–2022 годов, согласно информации из международной патентной базы данных Questel Orbit, было подано 3550 заявок на получение патента в сфере КФС, из которых большая часть была зарегистрирована патентными ведомствами Китая и США, а также Всемирной организацией интеллектуальной собственности (далее – ВОИС) и Европейским патентным ведомством (далее – ЕПВ). В России за 2013–2022 годы было зарегистрировано 34 заявки на получение патента в сфере КФС.

Рисунок 25. Количество поданных заявок на защиту патентов в сфере КФС по годам (единиц, 2006–2022 годы)

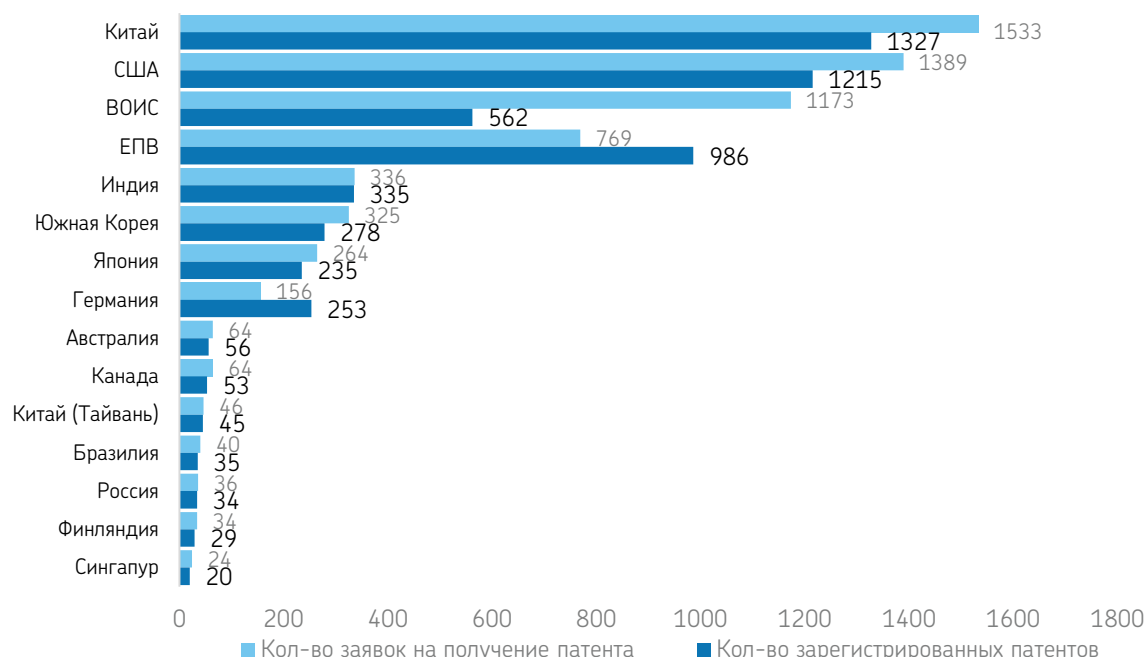


Источник: МГУ имени М.В.Ломоносова на основе данных международной патентной базы данных Questel Orbit

Большая часть зарегистрированных (полученных) патентов приходится на Китай, США, Европу (патенты были получены от Европейского патентного ведомства (ЕПВ) и патентных ведомств отдельных европейских стран). От российского патентного агентства – Федеральной службы по интеллектуальной собственности (далее – ФИПС) – за 2013–2022 годы было получено 34 патента.

Наибольшим интересом к выходу на рынок решений КФС обладают Китай, США, Индия, Южная Корея, Япония и Германия. Эти же страны отличаются большей готовностью к выходу на рынок и запуском производства в сфере КФС.

Рисунок 26. Количество патентов в сфере КФС по патентным агентствам стран (единиц, 2006–2022 годы)

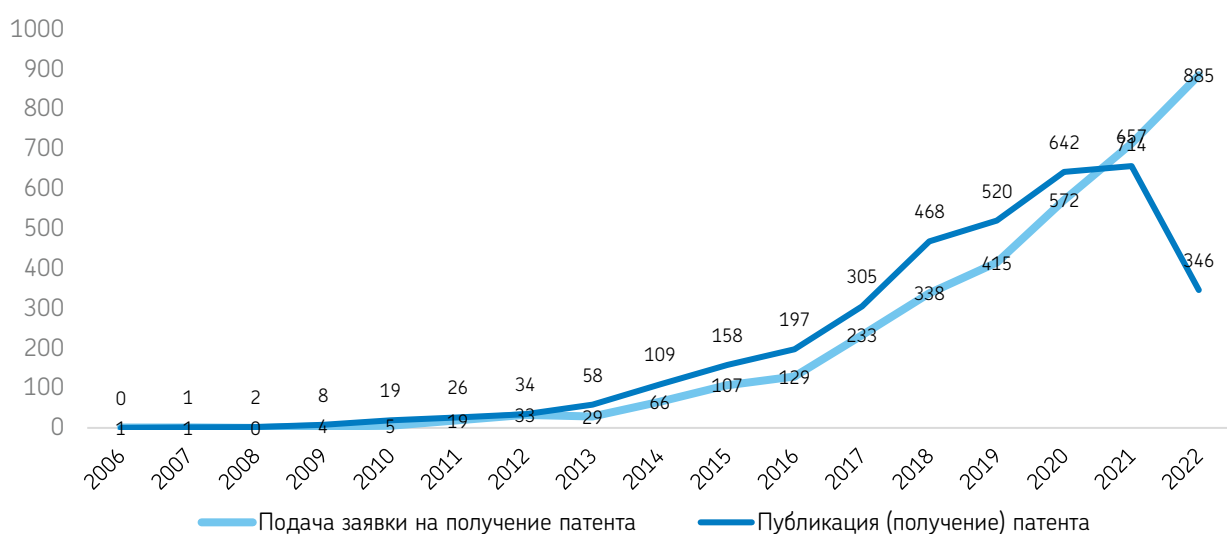


Источник: МГУ имени М.В.Ломоносова на основе данных международной патентной базы данных Questel Orbit

Согласно анализу количества поданных заявок на получение патента и количества публикаций (получения) патентов в мире, в течение 2006–2022 годов наблюдается положительная динамика количества заявок на получения патента в сфере КФС. При этом количество публикаций (получения) патентов в сфере КФС в течение 2007–2021 годов также постепенно возрастает.

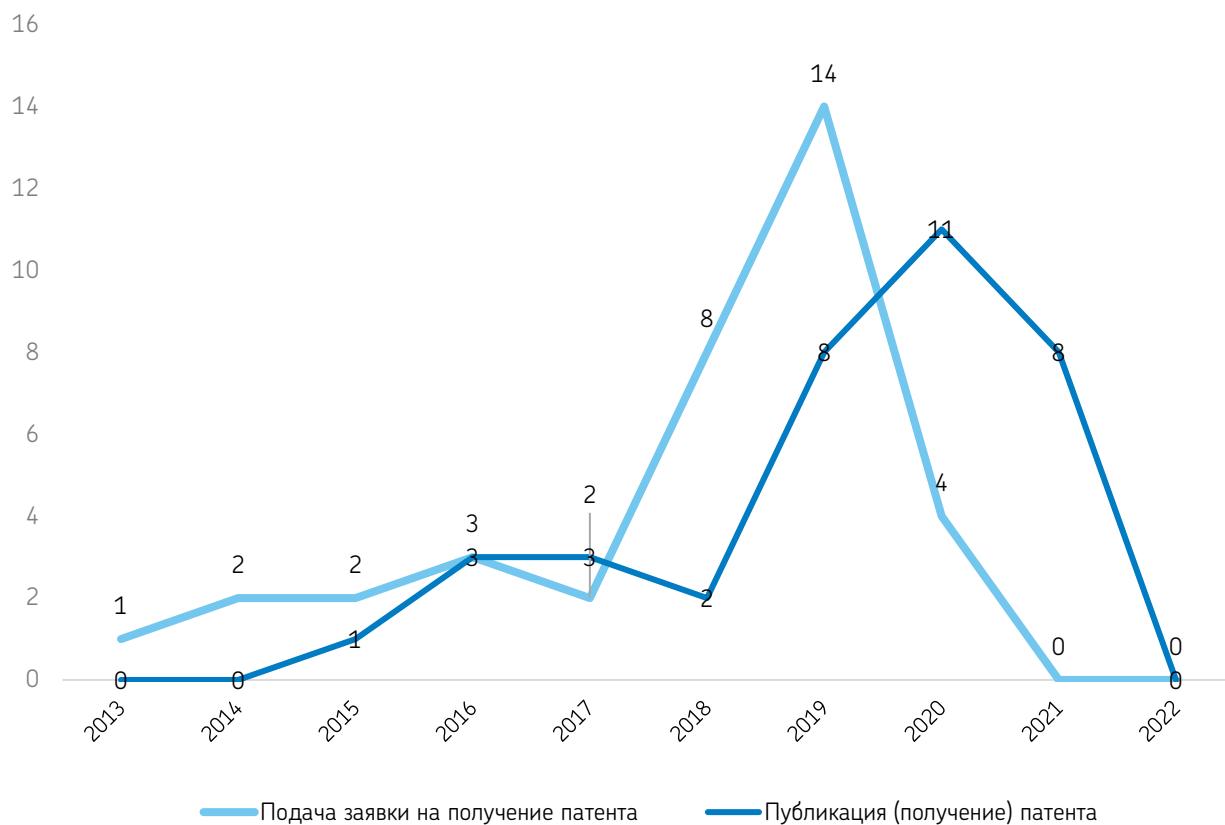
В России наблюдался значительный рост количества заявок на получение патента в сфере КФС в 2017–2019 годах (среднегодовой темп прироста был равен 164,57%). Аналогичная динамика была отмечена в 2018–2020 годах в разрезе количества публикаций (получения) патента (патентные документы публикуются национальными и региональными патентными ведомствами через 18 месяцев после того, как патентная заявка была впервые опубликована).

Рисунок 27. Анализ временной динамики по миру (единиц, 2006–2022 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных международной патентной базы данных Questel Orbit

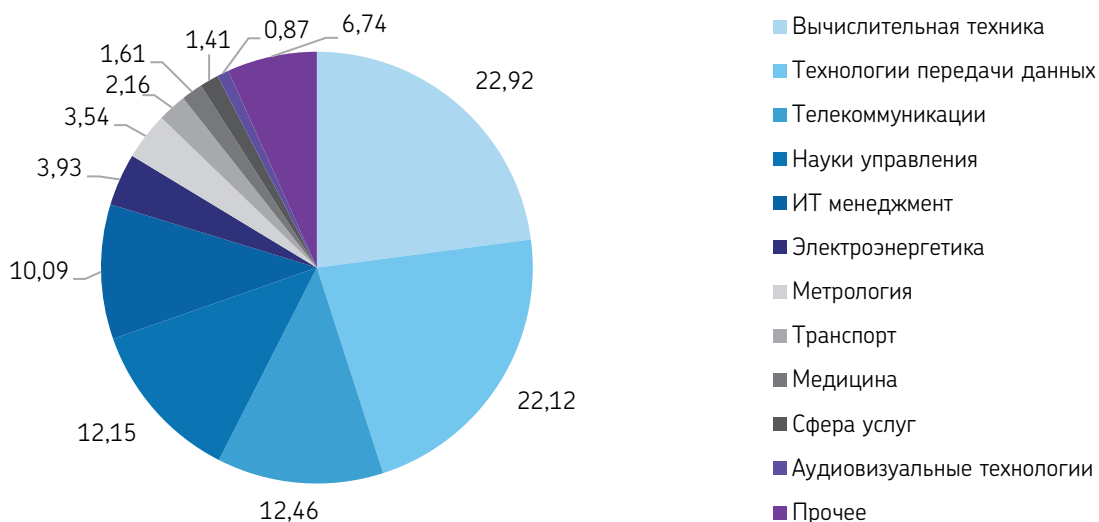
Рисунок 28. Анализ временной динамики по России (единиц, 2013–2022 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных международной патентной базы данных Questel Orbit

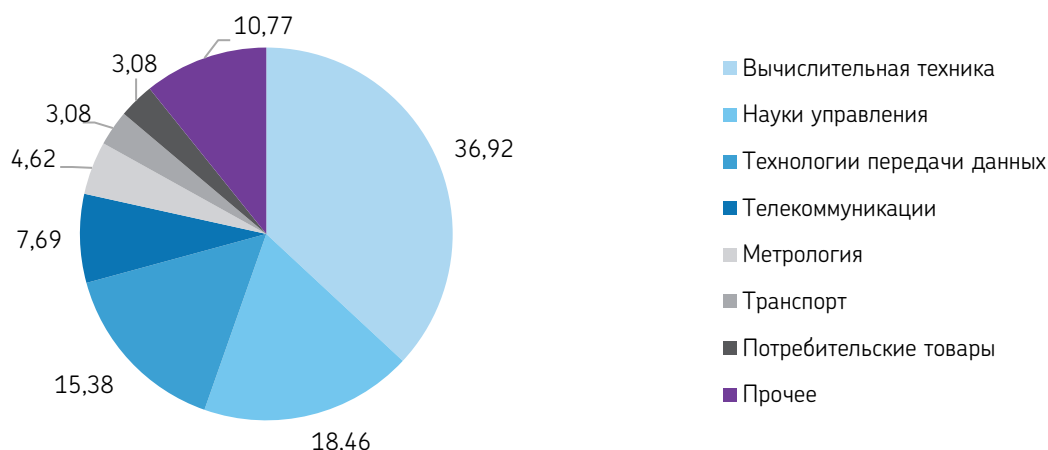
Наиболее популярными прикладными областями патентов в области КФС, согласно данным международной патентной базы данных Questel Orbit, стали вычислительная техника, технологии передачи данных, телекоммуникационные технологии и науки управления. Наименее популярными сферами публикации патентов в сфере КФС стали области медицины, сферы услуг и аудиовизуальных технологий.

Рисунок 29. Количество патентов по предметной области по миру (% , 2006–2022 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Рисунок 30. Количество патентов по предметной области по России (% , 2013–2022 годы)



Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

В 2006–2022 годах наиболее популярными подклассами публикаций (получения) патентов в области КФС стали⁵:

- G06F – обработка цифровых данных с помощью электрических устройств;
- H04L – передача цифровой информации;
- G06N – компьютерные системы, основанные на специфических вычислительных моделях и проч.

Наиболее релевантные изобретения, признанные патентными агентствами зарубежных стран, международными патентными агентствами и Российским агентством по патентам и товарным знакам (Роспатент), связаны с реализацией механизмов информационной безопасности и кибербезопасности КФС. Это объясняется тем, что методы и системы организации безопасности данных в КФС являются наиболее востребованными технологиями/решениями. Сбор и обработка данных из гетерогенных источников, контроль работы робототехнических устройств и проч. требуют колоссальных вычислительных затрат, необходимых для обеспечения работы защищенных протоколов связи и защиты данных в целом. Ввиду этого патентирование систем и методов контроля безопасности в КФС являются в наибольшей степени релевантными решениями и изобретениями на рынке. Перечень наиболее релевантных опубликованных патентов представлен в Приложении 7 Результаты библиометрического и патентного анализа.

4.3 Технологический радар рынка киберфизических систем

При исследовании рынка было выделено 8 технологий/ компонентов и 34 субтехнологии, в большей степени используемых в киберфизических системах.

Таблица 10. Технологии и субтехнологии КФС

№	Технология КФС	№ субтехнологии	Субтехнология КФС
1	Робототехническое оборудование и устройства	1.1	Промышленная робототехника
		1.2	Сервисная робототехника
		1.3	Технологии сбора информации
		1.4	Технологии искусственного интеллекта
2	Средства сбора и/ или	2.1	Сенсоры и датчики

⁵ Наиболее релевантные патенты отобраны внутренними инструментами Questel Orbit по комплексному показателю или «силе патента», формируемому на основе ряда индикаторов, таких как срок действия патента, географический охват семейства, цитируемость патента, наличие лицензий или споров по документам семейства, объем прав и проч., выгрузка и/ или определение которого не представляются возможными.

№	Технология КФС	№ субтехнологии	Субтехнология КФС
	обработки информации из внешней среды	2.2	Сенсорные сети
		2.3	Технологии искусственного интеллекта, в том числе машинное зрение
		2.4	Граничные вычисления
3	Технологии проектирования и моделирования	3.1	Системы автоматизированного проектирования
		3.2	Средства управления технологическими и бизнес-процессами
		3.3	Технологии цифровых двойников
4	Интернет вещей	4.1	Специализированные протоколы передачи данных
		4.2	Технологии проводной передачи данных
		4.3	Технологии беспроводной передачи данных
5	Облачные вычисления	5.1	Интернет-технологии
		5.2	Аппаратное обеспечение
		5.3	ПО управления облачными системами
		5.4	Распределенные вычисления
6	Большие данные	6.1	Специальное ПО для работы с базами данных
		6.2	Технологии трансформации необработанных больших данных в полезную информацию
		6.3	Инструменты визуализации аналитических данных
7	Новые материалы	7.1	Ударопрочные и физически-устойчивые новые материалы
		7.2	Новые материалы аддитивного производства
		7.3	Электропроводные новые материалы
		7.4	Новые жаропрочные материалы
		7.5	Новые биоматериалы
		7.6	Самовосстанавливающиеся материалы
		7.7	Суперсплавы
8	Аддитивные технологии	8.1	Технология послойного построения изделия из расплавленной пластиковой нити (FDM)
		8.2	Технология лазерного сплавления металлического порошка (SLM)
		8.3	Технология инфузионного напыления материала (SLS)
		8.4	Лазерная стереолитография, отверждение жидкого фотополимерного материала под действием лазера (SLA)
		8.5	Технология затвердевания фотополимера с помощью цифровой светодиодной проекции (DLP)
		8.6	Технологии быстрого прототипирования (MJM, PolyJet, CJP)

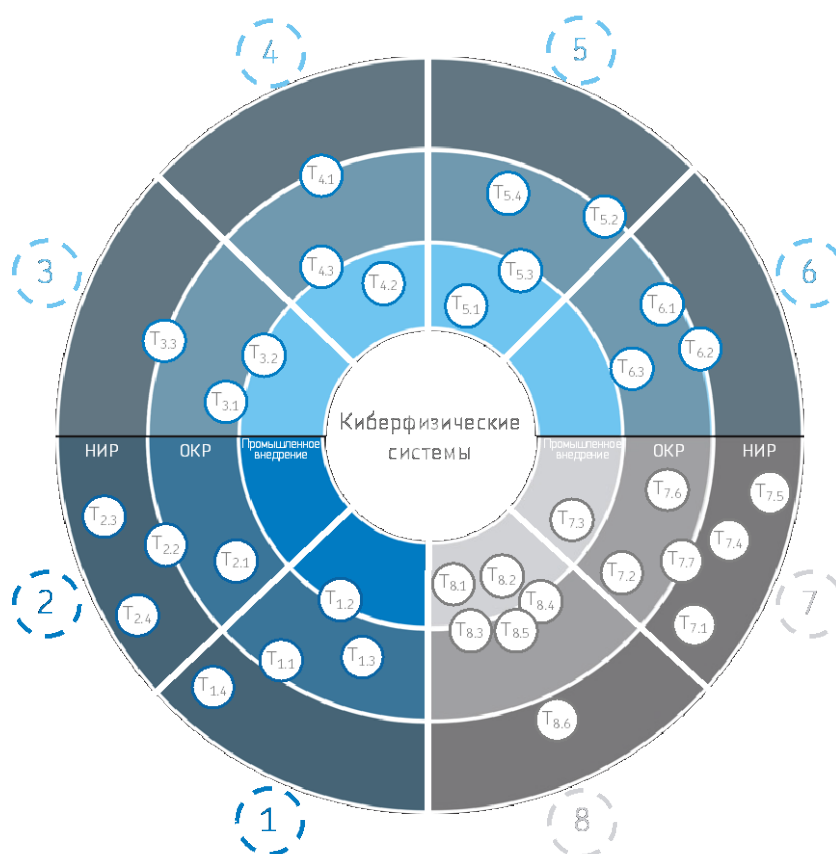
Источник: МГУ имени М.В.Ломоносова

Развитие отечественного рынка киберфизических систем может быть реализовано комплексным образом, что требует достижения паритетного или опережающего уровня развития технологий и субтехнологий КФС относительно мирового рынка решений в данной области. Наиболее значимыми точками роста отечественных технологий КФС были выделены:

1. Робототехническое оборудование и устройства: промышленная робототехника и технологии искусственного интеллекта в робототехнике;
2. Средства сбора и/или обработки информации из внешней среды: сенсорные сети, технологии искусственного интеллекта в контексте сбора/обработки данных, граничные вычисления;
3. Технологии проектирования и моделирования: технологии цифровых двойников;
4. Интернет вещей: технологии сбора/обработки информации;
5. Облачные вычисления: аппаратное обеспечение, распределенные вычисления;
6. Большие данные: специализированное ПО для работы с базами данных, технологии

- трансформации необработанных больших данных в полезную информацию;
7. Новые материалы: технологии создания новых ударопрочных и физически-устойчивых материалов, жаропрочных материалов, биоматериалов, суперсплавов;
 8. Аддитивные технологии: технологии быстрого прототипирования.

Рисунок 31. Технологический радар отечественного рынка КФС



Источник: МГУ имени М.В.Ломоносова

«Сквозные» технологии направления «Технет» НТИ схожи с рассмотренными технологиями, составляющими основу киберфизических систем. Разработка и совершенствование данных технологий будет способствовать своевременному развитию отечественного рынка киберфизических систем, ускорению темпов внедрения КФС в технологические, производственные и бизнес-процессы отечественных предприятий.

ГЛАВА 5. ПОКАЗАТЕЛИ ПО КОМПАНИЯМ «ТЕХНЕТ» НТИ, СПЕЦИАЛИЗИРУЮЩИХСЯ НА РАЗРАБОТКЕ РЕШЕНИЙ В ОБЛАСТИ РАЗВИТИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ, ВОВЛЕЧЕННЫМ В РЕАЛИЗАЦИЮ НАПРАВЛЕНИЯ НТИ

5.1 Количество компаний НТИ

В рамках настоящей главы представлены результаты анализа компаний, входящих в перечень направления «Технет» НТИ и производящих продукты и / или разрабатывающих проекты в области развития киберфизических систем. Перечень исследуемых компаний был составлен на основе реестра «НТИ 1000»:

- были выделены компании, которые реализуют продукцию на рынке «Технет» (всего на рынке «Технет» действуют 165 компаний);
- далее определены компании, которые реализуют продукцию на рынке «Технет», относящуюся к киберфизическим системам (непосредственно КФС, а также их составные элементы и смежные технологии, всего 68 компаний).

В результате анализа было отобрано 68 компаний и 91 проект/продукт, соответствующие исследуемой области киберфизических систем и технологиям, выделенным в 4 главе.⁶

Информационной базой исследования стали реестр «НТИ 1000», система СПАРК-Интерфакс и сайты компаний.

5.1.1 Анализ компаний по технологическому типу

Анализ данных о деятельности компаний, позволяет сделать вывод о неравномерном представлении на рынке киберфизических систем шести технологий (выделенных в 4 главе) с преимуществом в пользу технологий проектирования и моделирования (см. таблицу 11). Наименьшее количество компаний наблюдается в области технологий «Облачные вычисления» и «Большие данные». Ниже представлены результаты анализа общей и средней выручки компаний по технологическим типам.

Таблица 11. Распределение компаний по технологиям производимой продукции (единицы)

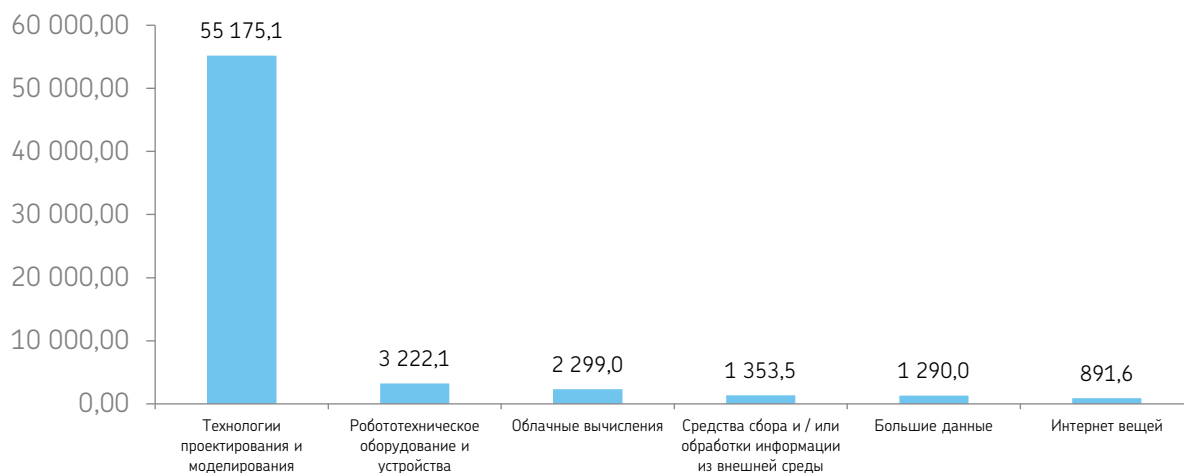
№	Технология	Количество компаний
1	Робототехническое оборудование и устройства	18
2	Средства сбора и / или обработки информации из внешней среды	18
3	Технологии проектирования и моделирования	24
4	Интернет вещей	10
5	Облачные вычисления	4
6	Большие данные	5

Источник: МГУ имени М.В.Ломоносова, 2022 год

По результатам анализа, наибольшей востребованностью на рынке КФС пользуются технологии проектирования и моделирования: продукты данных технологий опережают продукцию второй по средней выручке технологии «Облачные вычисления» в 4,66 раз за период 2017–2021 года и в 17,1 раз опережают продукцию второй по суммарной выручке технологии «Робототехническое оборудование и устройства».

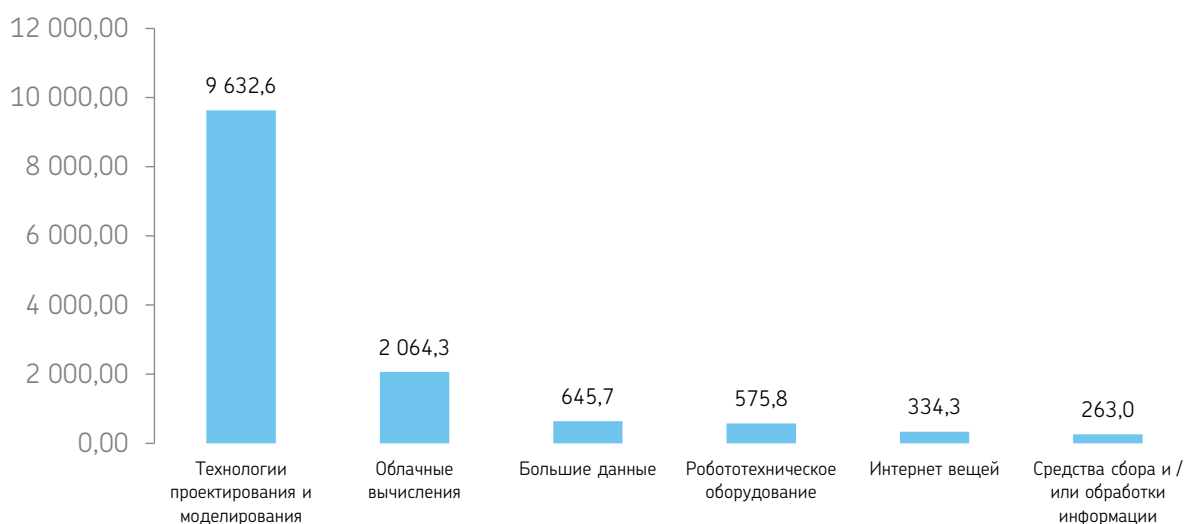
⁶ В связи с тем, что одна компания может производить / разрабатывать несколько продуктов / проектов, их количество неодинаково.

Рисунок 32. Общая выручка компаний в рамках технологий (млн руб., 2021 год)



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

Рисунок 33. Средняя выручка компаний в рамках технологических типов (млн руб., 2017–2021 годы)



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

5.1.2 Географический анализ компаний

Географическая принадлежность компании определялась по фактическому расположению головного офиса. Компании, занимающиеся разработкой КФС, представлены в 27 субъектах Российской Федерации. При этом в 15 субъектах зарегистрировано по одной компании. Лидерами рейтинга являются города федерального значения Москва (17 компаний) и Санкт-Петербург (10 компаний), что обосновывается научной, инфраструктурной и экономической развитостью данных субъектов, а также возможностью наиболее удобного взаимодействия с контрагентами (12).

Высокое место в рейтинге занимает Новосибирская область – один из наиболее развитых субъектов азиатской части Российской Федерации с большим количеством вузов и научно-исследовательских институтов, готовящих кадры с навыками проектирования КФС. Наибольшая плотность рассматриваемых компаний наблюдается в Центральном и Сибирском федеральных округах (по 7 субъектов).

Таблица 12. Распределение компаний по регионам (единицы)

№	Субъект	Количество компаний	№	Субъект	Количество компаний
1	Москва	17	15	Ивановская область	1
2	Санкт-Петербург	10	16	Иркутская область	1
3	Новосибирская область	4	17	Калининградская область	1
4	Астраханская область	3	18	Калужская область	1
5	Московская область	3	19	Кемеровская область	1
6	Пермский край	3	20	Омская область	1
7	Томская область	3	21	Приморский край	1
8	Красноярский край	2	22	Республика Марий Эл	1
9	Ленинградская область	2	23	Ростовская область	1
10	Республика Татарстан	2	24	Смоленская область	1
11	Ярославская область	2	25	Тюменская область	1
12	Свердловская область	2	26	Ханты-Мансийский АО	1
13	Алтайский край	1	27	Челябинская область	1
14	Белгородская область	1			

Источник: МГУ имени М.В.Ломоносова, 2022 год

Далее представлен анализ величины средней выручки компаний НТИ по субъектам Российской Федерации (13 и 34). Лидерами рейтинга по средней выручке за период с 2017 по 2021 год среди субъектов Российской Федерации являются Ярославская область и Алтайский край. Высокие позиции субъектов в рейтинге связаны с малым количеством компаний в субъекте (2 в Ярославской области и 1 в Алтайском крае соответственно) при успешных финансовых показателях компаний в рассматриваемый период (согласно открытым базам данных общая выручка ПАО «ОДК-САТУРН» в 2021 году превышала 52 млрд руб., что выводит Ярославскую область на первое место по средней выручке за 2017–2021 годы). Традиционно высокие места в рейтинге занимают города федерального значения Москва и Санкт-Петербург. Смоленская область также находится на высоких позициях в рейтинге: причиной этому послужило то, что в рамках данного субъекта осуществляет деятельность 1 компании, обладающая высокими финансовыми показателями.

Таблица 13. Средняя выручка по субъекту Российской Федерации (млн руб., 2017–2021 годы)

№	Субъект	Средняя выручка	№	Субъект	Средняя выручка
1	Ярославская область	21 920, 0	15	Ленинградская область	57,0
2	Алтайский край	403,8	16	Красноярский край	45,2
3	Москва	196,3	17	Ивановская область	37,8
4	Смоленская область	178,7	18	Иркутская область	24,5
5	Санкт-Петербург	150,7	19	Республика Марий Эл	17,8
6	Новосибирская область	91,6	20	Астраханская область	11,7
7	Томская область	88,0	21	Белгородская область	11,1
8	Московская область	87,8	22	Калининградская область	6,8
9	Калужская область	84,7	23	Ханты-Мансийский АО	4,1
10	Тюменская область	79,3	24	Ростовская область	2,1
11	Свердловская область	78,1	25	Омская область	0,1
12	Кемеровская область	76,6	26	Приморский край	н/д ⁷

⁷ «Н/д» – нет данных.

№	Субъект	Средняя выручка	№	Субъект	Средняя выручка
13	Пермский край	71,7	27	Челябинская область	н/д
14	Республика Татарстан	66,4			

Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

Рисунок 34. Средняя выручка по субъекту Российской Федерации (млн руб., 2017–2021 годы)⁸



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

5.2 Краткое описание продуктов и услуг компаний НТИ

Анализ продуктов проводился в соответствии с перечнем выделенных технологий киберфизических систем на основе открытых источников (сайта «НТИ1000» и сайтов компаний НТИ). Отнесение продукта к технологии производилось на основе анализа ключевых функциональных особенностей, используемых субтехнологий, специфики продукции и позиционирования ее компанией-производителем.

В рамках каждой из технологий были определены 5⁹ наиболее релевантных, высокотехнологичных и востребованных продуктов с самым высоким УГТ, соответствующих требованиям участников рынка киберфизических систем. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ по технологическим направлениям представлены в Приложении 8 Описание продуктов и услуг по отдельному направлению НТИ.

Робототехническое оборудование и устройства

В части робототехнического оборудования и устройств компаниями НТИ суммарно реализуется 9 продуктов, которые ориентированы на решение таких задач, как:

- калибровка оборудования и устройств (например, геометрических параметров рабочих мест);

⁸ Исследование проводилось на основе данных до 2021 года включительно, территориальное деление России представлено по состоянию на конец 2021 года, соответственно

⁹ В рамках настоящего исследования определено, что наиболее эффективно и наглядно будет иллюстрировать именно 5 наиболее релевантных, высокотехнологичных и востребованных продуктов несмотря на то, что в составе технологии компаниями направления «Технет» НТИ может производиться более 5 разных продуктов.

- регуляция климата в помещении (например, борьба с запыленностью воздуха);
- выполнение механических операций на производстве и в открытом пространстве при помощи роботизированных комплексов и промышленных установок (например, манипуляции с продукцией при ее производстве, в том числе штрихкодирование);
- обучение роботостроению (например, для участия в сфере спортивного роботостроения).

Как показательный пример стоит отметить роботизированные комплексы Robo-C и Promobot V.4, производимые ООО «Промобот», поскольку они по своим функциональным характеристикам конкурируют с мировыми лидерами: Amy Robotics [213], Canbot [214], Chuangze Intelligent [215], Hancorn [216], LG [217]. По результатам анализа топ-5 продуктов компаний можно заключить, что отечественные разработки технологии «Робототехническое оборудование и устройства» находятся на паритетном уровне развития с зарубежными аналогами: российские продукты позволяют выполнять аналогичный и более широкий набор операций.

Средства сбора и / или обработки информации из внешней среды

Компаниями НТИ реализуются 12 продуктов, относимых к КФС, в рамках технологии «Средства сбора и / или обработки информации из внешней среды». Продукция ориентирована на решение таких задач, как:

- контроль температурных параметров (например, контроль температуры в печи);
- контроль производственных процессов при помощи субтехнологии машинного зрения (например, контроль конвейерных линий);
- распознавание образов: лиц, документов, QR-кодов, знаков транспортных средств и прочих внешних данных (например, распознавание лиц людей в потоке);
- локальное позиционирование объектов (например, отслеживание локации оборудования на производстве);
- дефектоскопия конвейерной продукции (например, поиск бракованной продукции);
- инвентаризация складской продукции (например, сбор и оптимизация данных о грузе на паллетах).

Среди наиболее релевантных, высокотехнологичных и востребованных продуктов технологии «Средства сбора и / или обработки информации из внешней среды» можно выделить: ПО контроля процессов по видео (искусственный интеллект) компании ООО «ВИДЕОМАТРИКС», Система распознавания данных на основе искусственного интеллекта (ООО «НВИАЙ СОЛЮШЕНС»), Система локального позиционирования (ООО «НИЛАР»), Система автоматизированной дефектоскопии на производстве (ООО «ПАВЛИН ТЕХНО»), Автоматизированная система инвентаризации (ООО «ЦАПК»).

В основе отечественной продукции настоящей технологии используются передовые субтехнологии искусственного интеллекта и машинного зрения. При сравнении перечисленных выше продуктов с зарубежными аналогами можно сделать вывод, что отечественные разработки находятся на паритетном уровне развития, что говорит об их потенциальной востребованности у заказчиков. Большинство отечественных и зарубежных продуктов технологии «Средства сбора и / или обработки информации из внешней среды» используются для автоматизации бизнес-процессов в рамках производства товаров, чаще всего это выявление дефектов продукции на производстве и оптимизация складской логистики.

Технологии проектирования и моделирования

Компаниями НТИ суммарно реализуется 15 продуктов, относящихся к технологиям проектирования и моделирования. Продукция ориентирована на решение таких задач, как:

- управление системами защиты информации (например, единый центр управления системой защиты корпоративной информации);
- моделирование и прогнозирование физических параметров процессов при помощи субтехнологий цифровых двойников (например, моделирование нестационарных течений динамических процессов);

- автоматизация бизнес-процессов (например, автоматизация удаленного взаимодействия с клиентами);
- виртуальное обучение сотрудников;
- аналитика Больших данных (например, прогнозирование будущего состояния объекта);
- копирование реальных объектов в 3D;
- управление жизненным циклом продукции (например, автоматическое отслеживание перемещения продукции);
- управление логистикой поставок (например, автоматическое планирование доставок);
- планирование и контроль деятельности промышленного оборудования (например, отслеживание промышленных погрузчиков и контроль доступа к ним).

К наиболее релевантным, высокотехнологичным и востребованным продуктам технологий проектирования и моделирования можно отнести: Цифровой двойник предприятия/объекта/системы (имитационное моделирование с целью прогнозирования) и Система предиктивной аналитики ремонта (ООО «ЭТТОН ГРУП»), Система создания цифровой копии объектов и территорий в 3D (АО «ТЕРРА ТЕХ»), Система конвейерного отслеживания продукта (ООО «ВИДЕОМАТ-РИКС»), Система контроля работы и энергоэффективности промышленного оборудования (ООО ИЦ «СТАНКО-СЕРВИС»).

Интернет вещей

Компаниями НТИ суммарно на рынке реализуется 5 продуктов технологии «Интернет вещей»: Цифровой шлем для удаленной техподдержки (ООО «ИНТЕЛЛИДЖЕНТ АЙДИАС»), Система автоматизации домов и прочих зданий (ООО «ИРИДИУМ»), Набор «Умная теплица ЙоТик М2» (ООО «МГБОТ»), «Умный холодильник» (ООО «НЕОХОУМ»), Система управления генерацией и распределением тепловой энергии «Аврора» (ООО «СОФТ М»). Продукция ориентирована на решение таких задач, как:

- оказание удаленной техподдержки (например, оказание техподдержки посредством VR / AR-инструментов);
- управление системой «Умный дом»;
- организация системы «Умного овощеводства»;
- организация «Умного производства».

Устройства технологии «Интернет вещей», производимые компаниями НТИ, в основном ориентированы на организацию и управление системами класса «Умный дом» и «Умное производство». Они сопоставимы с зарубежными аналогами благодаря использованию новейших стандартов связи и обработки данных устройств Интернета вещей, при этом отдельно можно подчеркнуть разработку компании ООО «СОФТ М» «Автоматизированная система управления и мониторинга энергообъектов «Аврора», которая по своим функциональным характеристикам опережает зарубежный аналог «Danfoss Energy Metering system» [218]. Отечественная система помимо контроля энергопотребления также проводит мониторинг сигнализации и режима работы других телеметрических систем, помимо энергетических [219].

Облачные вычисления

Компаниями НТИ на рынке суммарно реализуется 5 систем по направлению «Облачные вычисления»: Система предотвращения утечек информации и контроля информационных потоков (АО «ИНФОВОТЧ»), Промышленный межсетевой экран (АО «ИНФОВОТЧ»), Система выявления нелояльных сотрудников InfoWatch Employee Monitoring (АО «ИНФОВОТЧ»), Сервис бизнес-аналитики (ООО «АЛАН-ИТ»), Система мониторинга и управления работой сети фотосепараторов (ООО «СИСОРТ»). Продукция ориентирована на решение таких задач, как:

- защита информации (например, контроль исходящей информации на предмет конфиденциальных данных);
- анализ эффективности и характера поведения сотрудников (например, отслеживание деятельности сотрудника и расчет ее эффективности);

- бизнес-аналитика и прогнозирование (например, аналитика и прогнозирование потребления электроэнергии ЖКХ).

Системы, производимые компаниями НТИ, конкурентны на мировом рынке за счет использования современных технологических решений, например, функционал системы выявления непояльных сотрудников «InfoWatch Employee Monitoring» компании АО «ИНФОВОТЧ» шире, чем системы «Employee Monitoring Software» компании Kickidler, поскольку позволяет также проводить мониторинг вводимого текста, геолокации устройств и фотоснимков экранов для кражи данных [220; 221].

Большие данные

Компаниями НТИ суммарно реализуется 5 устройств технологии «Большие данные», к которым можно отнести следующие: Система проактивного мониторинга бизнес-сервисов (ООО «7ТЕК»), ПО автоматизации управления жизненным циклом продукции (ООО «ЭТТОН ГРУП»), «Умная» система контроля телеметрии грузовых автомобилей и автобусов (ООО «КВАНТОР»), Система мониторинга и предиктивного анализа работы оборудования промышленных объектов с использованием технологий Интернета вещей (ООО «САТЕЛ ПРО»), Комплексная инфраструктурная цифровая платформа для беспроводного автоматизированного контроля и учета коммунальных ресурсов (ООО «АУРА 365»). Продукция ориентирована на решение таких задач, как:

- аналитика бизнес-сервисов и элементов производства, в том числе предиктивная (например, оповещение о возможных сбоях элементов бизнес-сервиса на основе прогнозирования);
- автоматизация управления жизненным циклом оборудования;
- «Умный» контроль телеметрии (например, контроль показателей грузовой автомобильной техники).

Продукция в рамках направления «Большие данные», производимая компаниями НТИ, находится на паритетном уровне развития по сравнению с зарубежными аналогами, в большинстве направлений использования решения ориентированы на улучшение бизнес-процессов путем аналитики данных. В ряде продуктов данного типа реализованы системы предиктивной аналитики, то есть системы, которые могут предсказывать будущие параметры тех или иных физических сущностей.

По итогам анализа можно сделать вывод о том, что наибольшая концентрация производимой продукции приходится на технологии проектирования и моделирования, поскольку она содержит 29,4% численности всех продуктов в рамках КФС. При этом данные технологические решения также являются самыми разнообразными в части набора реализуемых задач. Также относительно развитой является продукция технологии «Средства сбора и / или обработки информации из внешней среды», данный тип содержит 23,5% от общей численности всех продуктов КФС в рамках направления «Технет» НТИ. Наименее распространены среди российских компаний НТИ продукты технологии «Облачные вычисления», «Большие данные» и «Интернет вещей».

5.3 Объемы выручки от продажи продуктов и услуг компаний НТИ в рамках сегментов направления НТИ

В рамках работ по рыночной оценке российских компаний в области КФС был проведен анализ объемов выручки в разрезе технологий и динамики рынка последних лет. Информационной базой раздела является система СПАРК-Интерфакс. В случае выпуска компанией продукции, принадлежащей к нескольким технологиям, общая выручка компании учитывалась при подсчетах по всем технологиям, представленным в продукции такой компании. В таблице 14 представлены данные по объему выручки и связанным параметрам.

Таблица 14. Ранжированный объем выручки от продажи продуктов компаний НТИ (2021 год)

№	Технология	Количество компаний	Количество продуктов	Общая выручка за 2021 год, млн руб.	Средняя выручка за 2021 год, млн руб.	Относительный прирост общей выручки за 2021 год к 2017 году, %
1	Робототехническое оборудование и	17	17	3 222,1	179,0	116,4

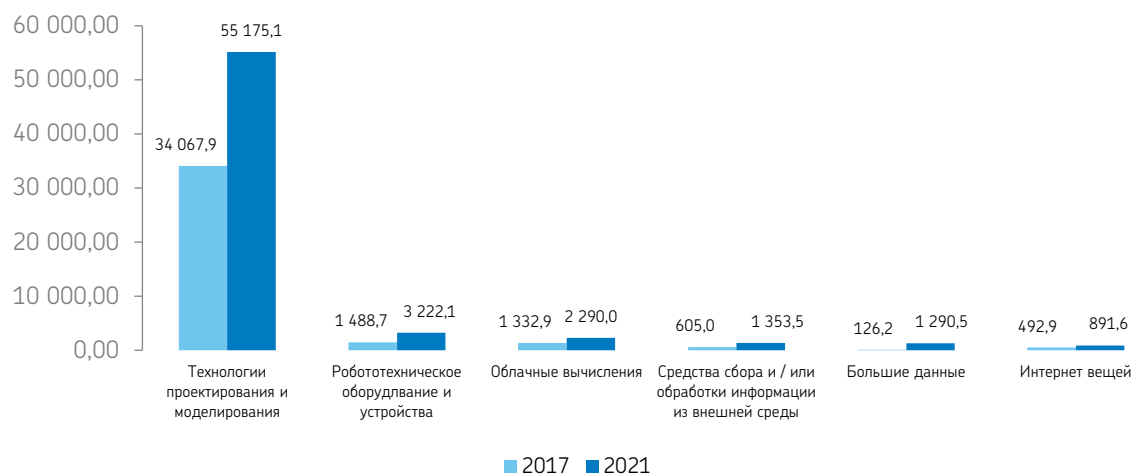
№	Технология	Количество компаний	Количество продуктов	Общая выручка за 2021 год, млн руб.	Средняя выручка за 2021 год, млн руб.	Относительный прирост общей выручки за 2021 год к 2017 году, %
	устройства					
2	Средства сбора и / или обработки информации из внешней среды	18	24	1 353,5	75,2	123,7
3	Технологии проектирования и моделирования	24	27	55 175,1	2 299,0	61,9
4	Интернет вещей	10	11	891,6	89,2	80,9
5	Облачные вычисления	4	6	2 298,9	574,7	72,5
6	Большие данные	5	7	1 290,5	258,0	922,2

Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

Наибольшее значение общей выручки можно отметить у технологий проектирования и моделирования – в 2021 году показатель составил 55 175,1 млн руб. При этом объем выручки по данной технологии превышает суммарный объем других пяти технологий в 6 раз. Вторую по величине долю рынка занимают решения технологии «Облачные вычисления» – суммарная выручка компаний с продукцией данной технологии в 2021 году составила 2 298,9 млн руб.

По наибольшей средней выручке в 2021 году также лидируют компании в области технологий проектирования и моделирования. При этом значение средней выручки по данному направлению превышает суммарный объем других пяти технологий практически в 2 раза. Высокое место в рейтинге свидетельствует о большом объеме спроса на решения для проектирования и моделирования среди потребителей, в частности, потому что такие решения используются для решения широкого спектра задач.

Рисунок 35. Динамика общей выручки компаний по технологиям (млн руб., 2017–2021 годы)

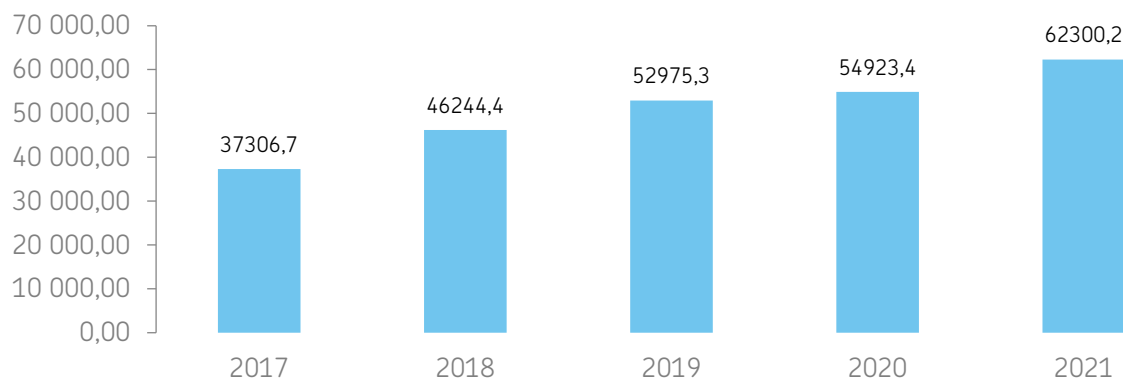


Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

По итогам анализа данных общей выручки компаний НТИ в динамике можно сделать вывод о росте выручки во всех технологиях продукции КФС в 2021 году по сравнению с 2017 годом. Наибольший рост выручки наблюдается у компаний, производящих продукцию в рамках технологий «Большие данные» (рост в 10,2 раза). Высокие темпы роста также наблюдаются у компаний, производящих продукцию в рамках технологий «Средства сбора и / или обработки информации из внешней среды» (рост в 2,2 раза) и «Робототехническое оборудование и устройства» (рост в 2,2 раза). Самый низкий темп роста выручки наблюдается у компаний в области технологий проектирования и моделирования (рост в 1,6 раза). Это обусловлено величиной рынка данных систем, что усложняет сохранение высоких темпов роста ввиду масштаба и насыщенности рынка: согласно международным

исследованиям, мировой рынок средств проектирования и моделирования является крупным, а быстрый рост невозможен из-за его насыщенности как с точки зрения потребителей, так и с точки зрения производителей / разработчиков [222; 223]. Это релевантно и для отечественного рынка технологий проектирования и моделирования НТИ. Далее представлены результаты анализа изменения объема общей выручки компаний с 2017 по 2021 годы.

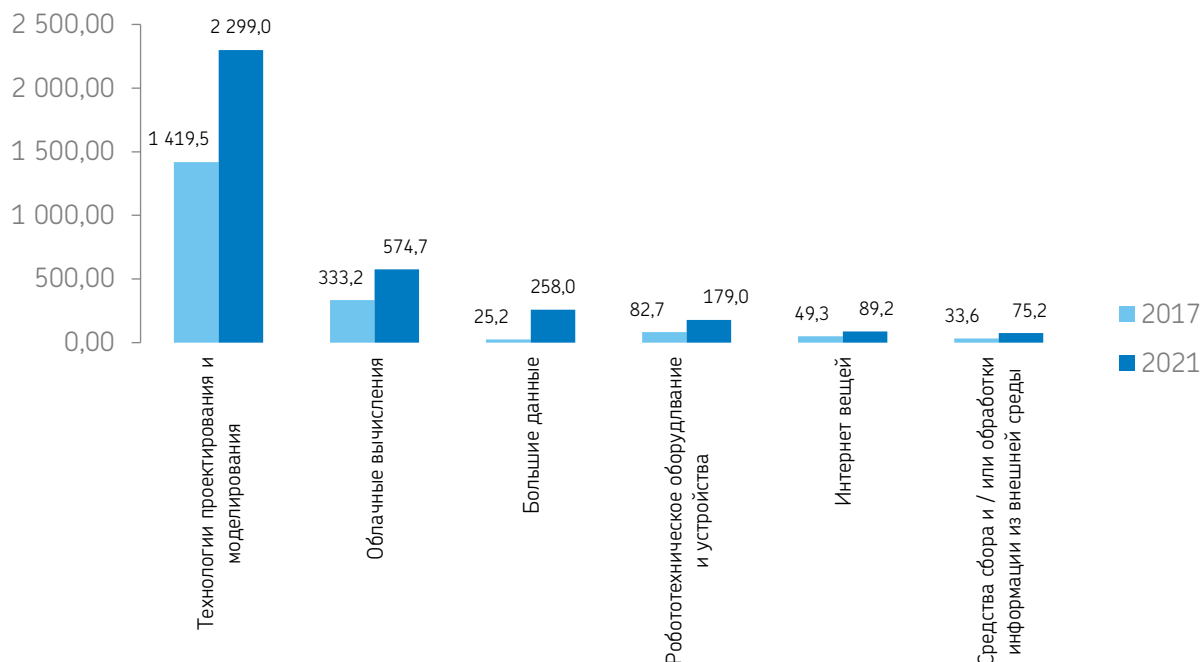
Рисунок 36. Динамика общей выручки компаний (млн руб., 2017–2021 годы)



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

По результатам анализа, на рынке существует тенденция роста общей выручки компаний в рассматриваемый период. Показатель 2021 года превышает аналогичный 2017 года в 1,7 раз (CAGR – 13,7%). Далее представлены результаты анализа средней выручки компаний НТИ в разрезе технологий (37).

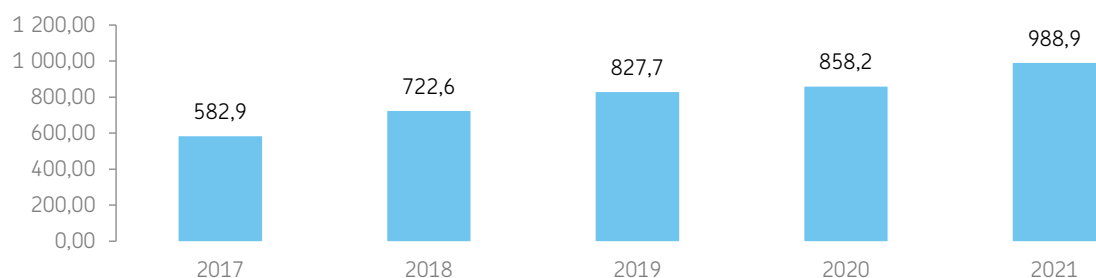
Рисунок 37. Динамика средней выручки компаний по технологиям (млн руб., 2017–2021 годы)



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

Анализ данных, представленных на рисунке 37, позволяет сделать вывод о непрерывном росте средней выручки компаний в разрезе по всем технологиям. Темпы роста средней выручки компаний аналогичны темпам роста общей выручки компаний, описанных ранее. Далее представлены изменения объема средней выручки в течение периода 2017–2021 годы.

Рисунок 38. Динамика средней выручки компаний (млн руб., 2017–2021 годы)



Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, 2022 год

Данные, представленные на рисунке выше, иллюстрируют рост средней выручки компаний из года в год. Снижение темпов роста наблюдается в период с 2019 по 2020 год, причиной которым послужила Пандемия коронавирусной инфекции и случившийся экономический кризис. Показатель 2021 года за рассматриваемый период вырос в 1,7 раз (CAGR – 14,1%).

Рост выручки от реализации КФС как по отдельным технологиям, так и по всей отрасли в целом свидетельствует о популяризации данного кластера субтехнологий в условиях повсеместного внедрения информационных технологий в промышленность. Наиболее востребованными являются средства на основе субтехнологий проектирования и моделирования, помогающие анализировать процессы в окружающем пространстве / на производстве, а также решения, осуществляющие непосредственное взаимодействие с физическим миром, а именно робототехнические устройства.

5.4 Количество компаний НТИ, имеющих экспортную выручку по направлению

Под экспортной выручкой понимается выручка, полученная от реализации продуктов / услуг на внешнем рынке. Оценка объемов экспортной выручки в рамках каждой технологии позволяет сделать вывод о востребованности определенной продукции и перспективах развития рынка КФС в целом. Источником данных об экспортной выручке в рамках настоящего раздела является реестр «НТИ 1000». В таблице 15 представлены данные о количестве компаний, осуществляющих экспорт, и доле экспорта в общем объеме выручки.

Таблица 15. Перечень компаний НТИ, имеющих экспортную выручку (2019 год)

№	Технология	Количество компаний, имеющих экспортную выручку, единиц	Доля экспортной выручки по технологиям в 2019 году от общего объема, %
1	Робототехническое оборудование и устройства	5	14,6
2	Средства сбора и / или обработки информации из внешней среды	5	7,1
3	Технологии проектирования и моделирования	3	13,7
4	Интернет вещей	2	19,4
5	Облачные вычисления	2	5,2
6	Большие данные	0	-

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

По результатам анализа, технология «Интернет вещей» лидирует по наибольшей доле экспортной выручки среди всех компаний по всем технологиям. Высокое место в рейтинге объясняется наличием экспорта лишь у двух компаний, при этом обе компании получают 19,3% и 22,4% всей своей выручки от зарубежных покупателей. Наименьшая доля экспортной выручки наблюдается среди компаний технологии «Облачные вычисления», что объясняется наличием экспорта также у двух компаний, одна из которых имеет низкую долю экспорта (0,81%) и в 4,5 раза

большую выручку относительно второй компании (доля экспорта 24,5%), что нивелирует общее значение.

Необходимо отметить, что компании, реализующие системы технологии «Большие данные», не имеют экспортной выручки. Данный факт частично объясняется тем, что данная технология имеет самое низкое количество продуктов (5) и проектов (1) в своем составе, что эквивалентно технологии «Облачные вычисления», которая имеет самую низкую долю экспортной выручки.

Относительно высокими значениями доли экспортной выручки обладают компании, реализующие свои продукты и проекты в рамках технологий «Робототехническое оборудование и устройства» (доля экспортной выручки в ранжире от 3,7% до 30,5%) и «Технологии проектирования и моделирования» (доля экспортной выручки в ранжире от 0,8% до 62,1%).

Из общей численности компаний (68) всего 15 осуществляют экспорт, что эквивалентно 22%. Распределение долей компаний с экспортной выручкой в общем числе компаний по технологиям отображено ниже на рисунке 39, однако необходимо учитывать тот факт, что одна компания может быть включена сразу в несколько технологий.

Рисунок 39. Доля компаний с экспортной выручкой в общем числе компаний технологии (единиц, 2019 год)



Источник: МГУ имени М.В.Ломоносова, 2022 год

При рассмотрении графика можно сделать вывод о наибольшей доле компаний с экспортной выручкой технологии «Облачные вычисления» (50%). Значимая доля компаний с экспортной выручкой по таким направлениям, как «Робототехническое оборудование и устройства» и «Средства сбора и / или обработки информации из внешней среды» (по 27,8%).

Можно сделать вывод, что экспорт среди российских производителей КФС не является преобладающей тенденцией: только 22% компаний реализуют продукцию на внешнем рынке. Основой КФС являются субтехнологии, выполняющие функции ресурсоемких вычислений, однако такие субтехнологии имеют крайне низкий объем экспорта из России ввиду технологического отставания от зарубежных лидеров [224]. Таким образом, технологические особенности деятельности российских компаний направления «Технет» НТИ являются ограничивающим фактором к большим объемам экспорта, однако рост этого объема возможен в долгосрочной перспективе путем стимулирования отечественных компаний к развитию этого направления.

5.5 Объем экспортной выручки компаний НТИ

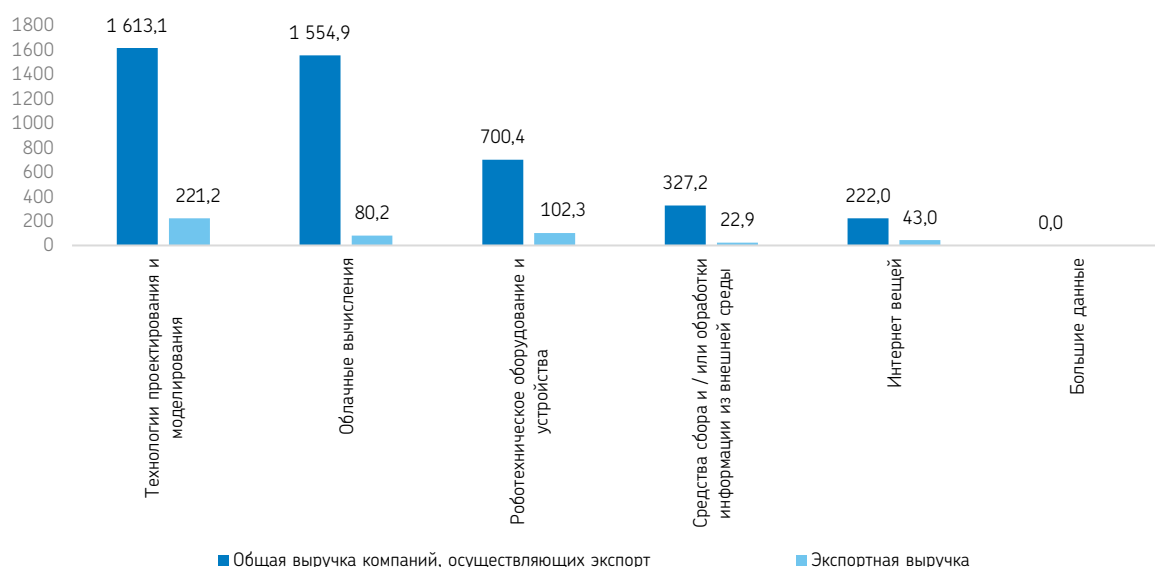
Общая экспортная выручка в рамках одной технологии рассчитывалась как сумма экспортной выручки всех компаний, выпускающих продукцию данной технологии. Под средней экспортной выручкой понимается отношение всей экспортной выручки к числу компаний, осуществляющих экспорт в рамках определенной технологии (технологии, рассмотренные в рамках 4 главы). В таблице 16 представлены результаты анализа экспортной выручки компаний НТИ.

Таблица 16. Ранжированный объем выручки от продажи продуктов компаний НТИ

№	Технология	Общая экспортная выручка за 2019 год, млн руб.	Средняя экспортная выручка за 2019 год, млн руб.
1	Робототехническое оборудование и устройства	102,3	20,5
2	Средства сбора и / или обработки информации из внешней среды	22,9	4,6
3	Технологии проектирования и моделирования	221,2	73,7
4	Интернет вещей	43	21,5
5	Облачные вычисления	80,2	40,1
6	Большие данные	0	0

Источник: МГУ имени М.В.Ломоносова, 2022 год

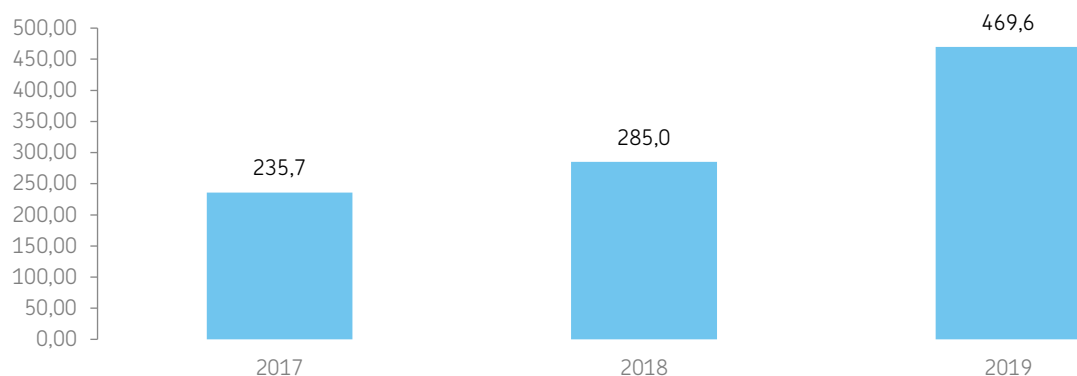
Наибольший объем экспортной выручки, зафиксированный в 2019 году относительно технологий проектирования и моделирования. Высокое значение показателя связано с экспортными показателями компании ООО «С-ИННОВАЦИИ» (62,11% своей годовой выручки объемом в 209,9 млн руб.) и невысоким количеством экспортирующих технологии компаний (3). Высокий результат объясняется деятельностью компании ООО «С-ИННОВАЦИИ», которая получила от зарубежных покупателей. Наименьший объем экспортной выручки наблюдается в рамках продукции технологии «Средства сбора и / или обработки информации из внешней среды», что объясняется невысокими значениями показателей выручки компаний несмотря на их большое количество по данному направлению. Результат остальных технологий находится в промежутке 0–102,26 млн руб. Далее представлены результаты анализа отношения экспортной выручки к общей выручке компаний и динамики экспортной выручки за период 2017–2019 годов.

Рисунок 40. Сравнение общей выручки компаний, осуществляющих экспорт, и их экспортной выручки по технологиям (млн руб., 2019 год)¹⁰

Источник: МГУ имени М.В.Ломоносова, 2022 год

¹⁰ Компании технологии «Большие данные» не осуществляют экспорт продукции, поэтому сравнение значений экспортной и обычной выручки, соответственно, невозможно

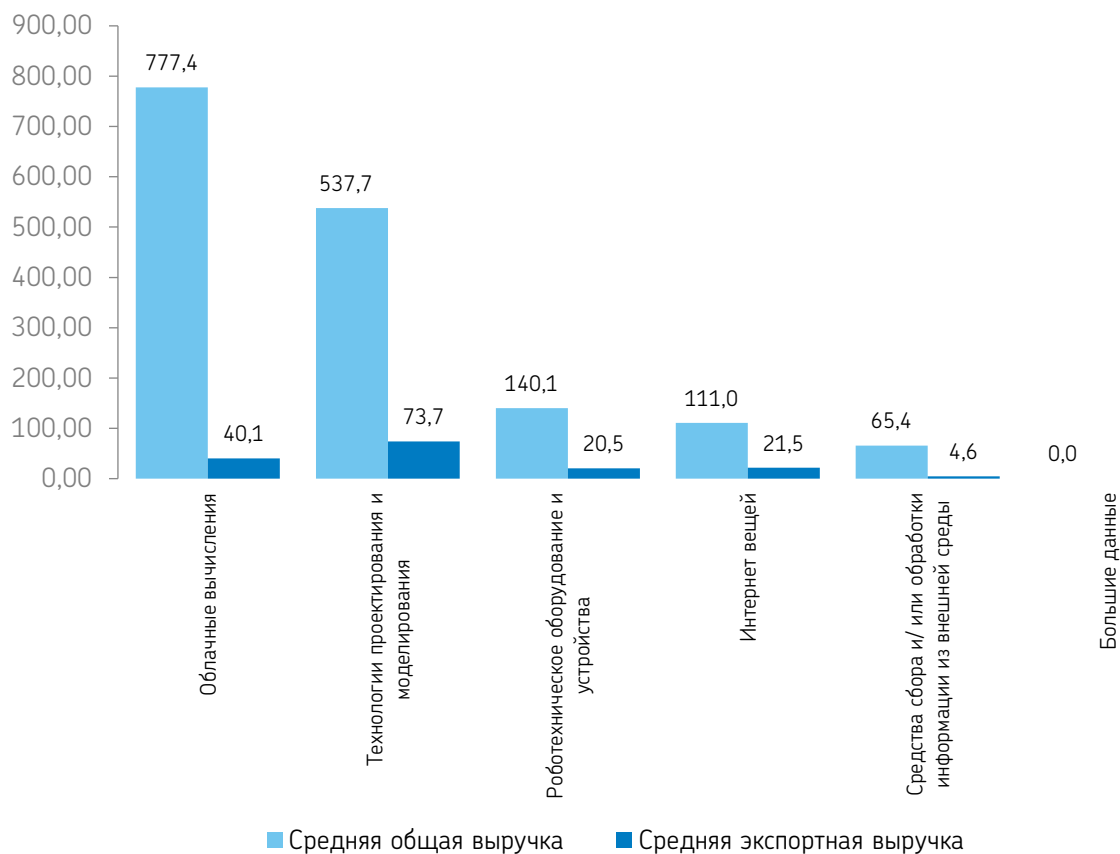
Рисунок 41. Динамика общей экспортной выручки компаний (млн руб., 2017–2019 годы)



Источник: МГУ имени М.В.Ломоносова, 2022 год

По результатам анализа можно отметить тенденцию роста общей экспортной выручки компаний направления КФС, в рассматриваемый период. Показатель 2019 года превышает аналогичный 2017 года в 2 раза (CAGR – 41,2%). Рост экспортной выручки связан с развитием субтехнологий в рамках технологий «Робототехническое оборудование и устройства» и «Технологии проектирования и моделирования», наращиванием компетенций отечественных компаний и выводением новой продукции на экспортный рынок. Далее представлено сравнение отношения средней общей и средней экспортной выручки компаний.

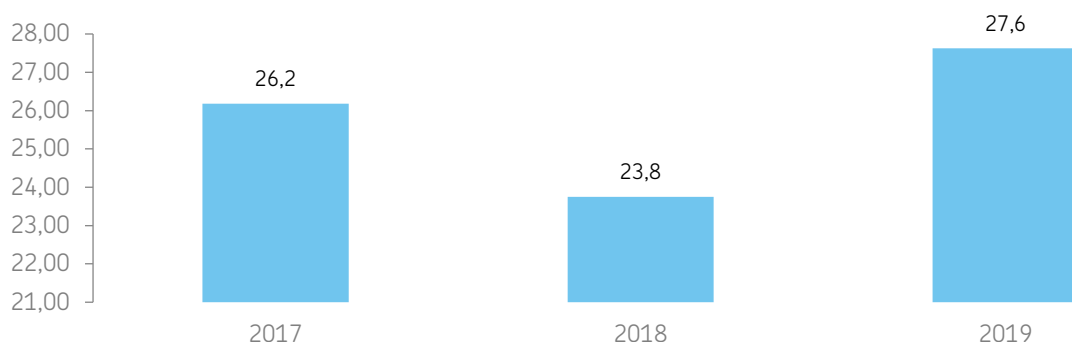
Рисунок 42. Сравнение средней экспортной выручки компаний и их средней общей выручки по технологиям (млн руб., 2019 год)



Источник: МГУ имени М.В.Ломоносова, 2022 год

Анализ данных позволяет сделать вывод о наибольшей средней экспортной выручке по направлению «Технологии проектирования и моделирования». Высокий результат свидетельствует об эффективности работы компаний и востребованности их решений на внешних рынках. Далее представлены результаты изменения значения экспортной выручки компаний направления «Технет» НТИ с 2017 по 2019 год.

Рисунок 43. Динамика средней экспортной выручки компаний (млн руб., 2017–2019 годы)



Источник: МГУ имени М.В.Ломоносова, 2022 год

В период с 2017 по 2019 год средняя экспортная выручка компаний направления «Технет» НТИ увеличилась, значение 2019 года превышает аналогичное 3 года назад на 5,5%, при этом в период с 2017 года по 2018 год значение упало на 9,28%, а в период с 2018 года по 2019 год выросло на 16,31%. Вероятной причиной снижения средней экспортной выручки компаний направления «Технет» НТИ является рост курса доллара и евро по отношению к рублю в 2018 году.

5.6 Количество прав на РИД, зарегистрированных компаниями НТИ

В рамках технологической оценки российских компаний, производящих КФС, был проведен анализ зарегистрированных прав на РИД следующих типов:

1. произведения науки;
2. программы для ЭВМ;
3. базы данных;
4. изобретения;
5. полезные модели;
6. топологии интегральных микросхем;
7. секреты производства (ноу-хау).

В таблице 17 представлены результаты по количеству прав на РИД в разрезе шести технологий и типов РИД. Количество зарегистрированных прав на РИД внутри технологии считалось как сумма таких прав всех компаний, производящих данную продукцию. Информация собиралась из открытых источников и на основе опроса компаний НТИ, однако секреты производства (ноу-хау) являются коммерческой тайной, поэтому они отсутствуют в анализе.

Таблица 17. Количество зарегистрированных РИД компаниями НТИ с разделением по технологиям

№	Технология	Количество прав на РИД							Итого по технологиям
		Произведения науки	Программы для ЭВМ	Базы данных	Изобретения	Полезные модели	Промышленные образцы	Топологии интегральных микросхем	
1	Робототехническое оборудование и устройства	20	23	0	27	17	10	0	97
2	Средства сбора и / или обработки информации из внешней среды	35	55	0	37	9	4	0	140

№	Технология	Количество прав на РИД							Итого по технологии
		Произведения науки	Программы для ЭВМ	Базы данных	Изобретения	Полезные модели	Промышленные образцы	Топологии интегральных микросхем	
3	Средства проектирования и моделирования	68	120	1	268	88	1	0	546
4	Интернет вещей	9	51	0	13	8	0	0	81
5	Облачные вычисления	1	15	0	13	0	0	0	29
6	Большие данные	7	29	0	0	1	0	0	37
7	Итого по количеству прав на РИД	140	293	1	358	123	15	0	-

Источник: МГУ имени М.В.Ломоносова по материалам системы СПАРК-Интерфакс, Информационно-поисковой системы ФИПС и системы ЕГИСУ НИОКТР, 2022 год

Суммарно компаниями НТИ в рамках направления КФС (все рассматриваемые технологии) по состоянию на 2021 год зарегистрировано 930 прав на РИД. В разрезе по типам РИД лидируют изобретения, их по всем компаниям зарегистрировано 358. На втором месте находятся программы для ЭВМ, их по всем компаниям разных технологий зарегистрировано 293. В разрезе по направлениям технологий лидируют «Технологии проектирования и моделирования», компаниями зарегистрировано 546 различных РИД, что превышает суммарное количество РИД по другим технологиям. Крупный объем регистрации изобретений в компаниях, занимающихся технологиями проектирования и моделирования, объясняется большим количеством этих компаний и масштабом их деятельности, а также широтой понятия «изобретение»¹¹. По данным Федеральной службы по интеллектуальной собственности в России за 2020 и 2021 годы среди рассматриваемых в рамках данного исследования типов РИД изобретения также лидируют по количеству электронных заявок на патентование [225].

В дальнейшем с учетом стимулирования развития в России деятельности компаний и государственных органов в сфере создания и регистрации интеллектуальной собственности можно ожидать повышение темпов патентования, в том числе среди компаний НТИ. Одним из факторов является упрощение процедуры подачи заявки и получения патента в рамках «цифровой трансформации» деятельности Федеральной службы по интеллектуальной собственности [225]. Активизация компаний по регистрации собственных разработок необходима для сокращения технологического разрыва России и зарубежных стран.

5.7 Количество реализуемых проектов по отдельному направлению НТИ

В рамках настоящего раздела рассматривается УГТ проектов в соответствии с ГОСТ Р 58048-2017 [226]. УГТ определялся на основании описания проекта в реестре сайта «НТИ 1000». В случае, если информация об УГТ проекта отсутствовала как в реестре «НТИ 1000», так и на официальном сайте компании, УГТ данного проекта в конечных подсчетах не учитывался, однако данный проект все равно рассматривался и включен в настоящее исследование.

В рамках каждой технологии были определены 5 наиболее релевантных, высокотехнологичных и востребованных проектов¹² (подробное описание проектов представлено в Приложении 9 Реализуемые проекты по отдельному направлению НТИ). В топ-5 входили проекты с самым высоким УГТ, отражающие современные тенденции развития рынка КФС. Исследование проводилось на основе публичной информации, предоставляемой отраслевыми компаниями, с выделением ключевых тенденций и инноваций в условиях международного рынка. Результаты

¹¹ Изобретение – техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств), в том числе к применению продукта или способа по определенному назначению. Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо (статья 1350 Гражданского кодекса Российской Федерации).

¹² В рамках настоящего исследования определено, что наиболее эффективно и наглядно будет иллюстрировать именно 5 наиболее релевантных, высокотехнологичных и востребованных проектов несмотря на то, что в составе технологии компаниями направления «Технет» НТИ может производиться более 5 разных проектов.

исследования сопоставлялись с проектами компаний направления «Технет» НТИ, на основе чего и был сформирован конечный перечень.

Робототехническое оборудование и устройства

В части технологии «Робототехническое оборудование и устройства» компаниями НТИ суммарно разрабатываются 8 проектов, которые ориентированы на решение таких задач, как:

- автоматизация производства и / или работы промышленных систем (например, автоматизация управления электрогенераторами);
- выполнение механических операций на производстве и в открытом пространстве при помощи роботизированных комплексов и промышленных установок.

Среди наиболее релевантных, высокотехнологичных и востребованных проектов технологии «Робототехническое оборудование и устройства» представлены следующие 5 проектов: Морская безэкипажная платформа (ООО «НТК «МОРРО-БОТСИСТЕМ»»), Безлюдные технологии транспортировки и добычи руды (ООО «ЦР»), Разработка семейства ветроэнергетических установок, а также интеллектуальной системы управления к ним (ООО «НИИ УРАЛ-МЕТ»), Роботизированная ячейка по финишной полировке (адаптивная) (ООО «ОБРАЗОВАТЕЛЬНАЯ РОБОТОТЕХНИКА»), Комплекс антропоморфных робототехнических устройств (АО «НПО «АНДРОИДНАЯ ТЕХНИКА»).

В рамках проектов технологии «Робототехническое оборудование и устройства» наблюдается тенденция повсеместного использования субтехнологий искусственного интеллекта и машинного зрения. Отечественные проекты отстают от зарубежных аналогов по УГТ, например, сравнивались решения компаний ООО «ЦР», ООО «НИИ УРАЛМЕТ» и ООО «ОБРАЗОВАТЕЛЬНАЯ РОБОТОТЕХНИКА» с зарубежными аналогами компаний Anybus [227], MTU [228], PushCorp [229], соответственно. Однако исходя из описания будущих продуктов компаний НТИ можно сделать вывод о конкурентоспособности решений при их выведении на рынок.

Средства сбора и / или обработки информации из внешней среды

Компаниями НТИ разрабатываются 12 проектов, относимых к КФС, в рамках технологии «Средства сбора и / или обработки информации из внешней среды». Проекты ориентированы на решение таких задач, как:

- контроль температурных параметров;
- контроль производственных процессов при помощи субтехнологии машинного зрения (например, контроль конвейерных линий);
- контроль людского потока (например, подсчет количества людей и распознавание их биометрических показателей).

Пять наиболее релевантных, высокотехнологичных и востребованных проектов технологии «Средства сбора и / или обработки информации из внешней среды»: Автоматизированное измерение температуры людей в потоке (ООО «А1»), Нейтронный анализатор сырья конвейера (ООО «ДИАМАНТ»), Автономный гаджет видео-аналитики (ООО «ПАВЛИН ТЕХНО»), Система контроля дыхания при лучевых процедурах пациента (ООО «ПАВЛИН ТЕХНО»), Биометрический браслет (ООО «ИНТЭК»).

В рамках проектов технологии «Средства сбора и / или обработки информации из внешней среды» наблюдается тенденция повсеместного использования субтехнологий искусственного интеллекта и машинного зрения. Это объясняется их высокой эффективностью в выполнении сложных задач по сбору и обработке информации и простотой внедрения данных решений с технической точки зрения, поскольку рынок наполнен предложениями компаний по поставке чипов, специализирующихся на вычислениях алгоритмов искусственного интеллекта. Отечественные проекты отстают от зарубежных аналогов по УГТ, например, сравнивались решения компаний ООО «А1», ООО «ДИАМАНТ» и ООО «ИНТЭК» с зарубежными аналогами компаний Kelsius [230], Thermo Scientific [231], Empatica [232] соответственно. Однако по планируемым функциональным характеристикам отечественные решения находятся на сопоставимом уровне развития.

Технологии проектирования и моделирования

Компаниями НТИ суммарно разрабатывается 12 проектов в области технологий проектирования и моделирования. Проекты ориентированы на решение таких задач, как:

- управление системами защиты информации;
- моделирование и прогнозирование физических параметров процессов при помощи субтехнологий цифровых двойников;
- автоматизация бизнес-процессов;
- планирование и контроль деятельности промышленного оборудования.

Среди наиболее релевантных, высокотехнологичных и востребованных проектов в области технологий проектирования и моделирования представлены: Аппаратно-программный комплекс управления судами (ООО «НМТ»), Программный комплекс для мониторинга, диагностики, прогнозирования, управления работой электротехнического оборудования и систем электропитания оборудования (объектов) (АО «ФЭСКОМ»), Система проектирования и мониторинга электрооборудования (ООО «ГАРПИКС»), АИС «Месторождение» (ООО «ЭТТОН ГРУП»), Умная фабрика – испытательный полигон для создания промышленного предприятия в рамках Индустрии 4.0 (ПАО «ОДК-САТУРН») [233]. В проектах в области технологий проектирования и моделирования часто используются такие субтехнологии, как нейронные сети, цифровые двойники и имитационное моделирование. Разрабатываемые компаниями НТИ системы на данный момент отстают от зарубежных аналогов, но в перспективе могут являться конкурентоспособными в рамках международного рынка. Проводилось сравнение решений ООО «НМТ», АО «ФЭСКОМ» и ООО «ГАРПИКС» с аналогами компаний Prime Marine [234], Eaton [235] и Schneider Electric [236] соответственно.

Интернет вещей

Компаниями НТИ суммарно разрабатываются 6 проектов технологии «Интернет вещей». Проекты ориентированы на решение таких задач, как:

- организация системы «умного» рыбоводства и «умного» овощеводства;
- работа «умной» промышленности.

Среди наиболее релевантных, высокотехнологичных и востребованных проектов технологии «Интернет вещей» можно выделить следующие: ПАК сбора и обработки данных об объектах (ООО «СЕРВИССОФТ ИНЖИНИРИНГ»), Система контроля работы инженерного оборудования (ООО «СЛУЖБА МОНИТОРИНГА. ТЮМЕНЬ»), Мониторинг холодильного оборудования («умный») (ООО «НЕОХОУМ»), Архитектура Доверенной Открытой Распределенной Системы Управления на основе Промышленного Интернета (ДОРСУ-ПИ) (ООО «МОДУЛЬНЫЕ СИСТЕМЫ ТОР-НАДО»), ПАК для выращивания ценных пород рыб (ООО «ДИЛИБРИУМ»).

Устройства технологии «Интернет вещей», разрабатываемые компаниями НТИ, в основном ориентированы на организацию и управление системами класса «Умный дом» и «Умное производство». Системы считывают множество параметров объектов и в результате обработки данных могут запускать установленные сценарии действий, направленных на сквозную автоматизацию процессов. Разрабатываемые компаниями НТИ системы на данный момент отстают от зарубежных аналогов, но в перспективе могут являться конкурентоспособными в рамках международного рынка. Проводилось сравнение решений ООО «СЕРВИССОФТ ИНЖИНИРИНГ» и ООО «НЕОХОУМ» с аналогами компаний Biz Intellia [237] и Danfoss [238] соответственно.

Облачные вычисления

В рамках технологии «Облачные вычисления» разрабатывается 1 проект – Автоматизированная система видеонаблюдения высокого разрешения (ООО «ИНТЭК») [239]. Решение ориентировано на решение задачи повышения эффективности систем видеонаблюдения. Проект отстает по УГТ от зарубежного аналога – системы «IPC-HFW3441DG-AS-4G-EAU-B» компании Dahua [240], однако на стадии разработки отечественный продукт сопоставим по прогнозируемым функциональным характеристикам.

Большие данные

Компанией НТИ разрабатывается 1 проект технологии «Большие данные» – Цифровая платформа трейсинга алмазов (ООО «7ТЕК») [241], он ориентирован на решение такой задачи, как аналитика запасов месторождений полезных ископаемых. Аналог разрабатываемого проекта на международном рынке отсутствует, таким образом внедрение платформы компании ООО «7ТЕК» в промышленность может стимулировать развитие нового специфического типа технических решений.

По итогам анализа можно сделать вывод о том, что наибольшая концентрация проектов приходится на технологии «Средства сбора и / или обработки информации из внешней среды» и «Технологии проектирования и моделирования»: по 30% от численности всех проектов КФС компаний НТИ. При этом решения являются самыми разнообразными в части набора реализуемых задач. На основе этого можно сделать вывод о том, что эти технологии являются наиболее развитыми в России, в частности в рамках направления «Технет» НТИ.

Также относительно развитыми являются проекты технологий «Робототехническое оборудование и устройства» и «Интернет вещей», они содержат по 20% и 15% от общей численности всех проектов КФС в рамках направления «Технет» НТИ соответственно. Наименее распространены среди российских компаний НТИ проекты технологий «Облачные вычисления» и «Большие данные».

5.8 Технологический ландшафт рынка, занимаемого компаниями НТИ

Технологический ландшафт – это сжатая и комплексная «картина» используемых в отрасли технологий и субтехнологий, ландшафт позволяет оценить степень насыщенности основных направлений развития рынка КФС и их уровень развития в зарубежных странах и в России. В рамках настоящего исследования методом формирования и анализа технологического ландшафта рассматриваются 6 технологий производимых / разрабатываемых компаниями направления «Технет» НТИ продуктов / проектов (технологии, рассмотренные в 4 главе).

Технологический ландшафт формируется исходя из оценки конкурентоспособности продуктов / проектов компаний направления «Технет» НТИ в части КФС относительно зарубежных аналогов. В рамках каждой технологии рассматриваются такие аспекты технологического ландшафта, как назначение группы продукции / проектов и их уровень развития (отставание¹³ / паритет¹⁴ / опережение¹⁵ относительно зарубежных аналогов или отсутствие таковых).

Робототехническое оборудование и устройства

В рамках технологии «Робототехническое оборудование и устройства» компаниями направления «Технет» НТИ реализуется 17 продуктов и проектов. Ниже представлена карточка технологического ландшафта «Робототехническое оборудование и устройства».

Для технологии «Робототехническое оборудование и устройства» наблюдается паритет двух групп решений назначения «Промышленное производство деталей, обеспечение необходимых условий на производстве» и «Обучение и сервис» относительно зарубежных аналогов¹⁶.

В рамках группы решений назначения «Промышленное производство деталей, обеспечение необходимых условий на производстве» для 1 решения не имеется аналогов в мире, 6 решений находятся в паритете с зарубежными аналогами, 4 – отстают по своим функциональным и прочим ключевым характеристикам от зарубежных аналогов. В рамках группы решений назначения «Реализация безлюдных экспедиций / добычи полезных ископаемых /

¹³ Уровень развития «Отставание» свидетельствует о том, что российский продукт / проект отстает от зарубежных аналогов по ключевым функциональным характеристикам

¹⁴ Уровень развития «Паритет» свидетельствует о том, что российский продукт / проект эквивалентен зарубежным аналогам по ключевым функциональным характеристикам

¹⁵ Уровень развития «Опережение» свидетельствует о том, что российский продукт / проект превосходит известные в рамках открытых источников данных зарубежные аналоги по ключевым функциональным характеристикам

¹⁶ Решение – в данном разделе – это понятие, в которое включается продукт (УГТ9) и проект (УГТ1–8)

добычи энергии» наблюдается отставание отечественных компаний: 3 из 4 решений отстают от зарубежных аналогов, при этом только 1 (морская безэкипажная платформа разработки ООО «НТК МОПРОБОТСИСТЕМ» [242]) находится в паритете. Группа решений «Обучение и сервис» находится в паритете с зарубежными аналогами, однако в рамках данной группы 1 решение опережает зарубежные аналоги (сервисные роботы производства ООО «ПРОМОБОТ» [243]) и 1 находится в состоянии отставания от зарубежных аналогов (набор «Динамика ЙоТик М1» производства ООО «МГБОТ» [244]).

В рамках технологии «Робототехническое оборудование и устройства» 47% решений находятся в отстающей позиции по сравнению с зарубежными аналогами, однако также 41,2% решений находятся в условиях паритета, 5,9% – опережают зарубежные аналоги и 5,9% не имеют их. В рамках технологии «Робототехническое оборудование и устройства» наблюдается преимущественный паритет российских разработок с зарубежными аналогами, однако отсутствует тенденция к дальнейшему опережающему росту. Единственным продуктом, который является лидером на мировом уровне, является сервисный робот производства ООО «ПРОМОБОТ», что выражается в его стоимости и публично подтвержденным функциональными возможностями.

Рисунок 44. Карточка технологического ландшафта «Робототехническое оборудование и устройства»

Робототехническое оборудование и устройства		
Назначение	Уровень развития	Отечественные компании
Промышленное производство деталей, обеспечение необходимых условий на производстве	Паритет	  
Реализация безлюдных экспедиций / добычи полезных ископаемых / добычи энергии	Отставание	
Обучение и сервис	Паритет	

Источник: МГУ имени М.В.Ломоносова, 2022 год

Средства сбора и / или обработки информации из внешней среды

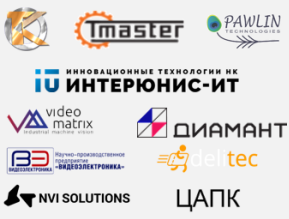
В рамках технологии «Средства сбора и / или обработки информации из внешней среды» компаниями направления «Технет» НТИ реализуется 24 продукта и проекта. Ниже представлена карточка технологического ландшафта «Средства сбора и / или обработки информации из внешней среды».

Для технологии «Средства сбора и / или обработки информации из внешней среды» наблюдается паритет двух групп решений назначения «Контроль технологических, производственных и логистических процессов» и «Сбор биометрических и физиологических параметров человека и иных образов» с зарубежными аналогами. В рамках первой группы решений 1 не имеет зарубежных аналогов, 1 опережает зарубежные аналоги, 9 находятся в состоянии паритета, а 4 отстают от зарубежных аналогов. В рамках группы решений назначения «Сбор биометрических и физиологических параметров человека и иных образов» 1 решение не имеет зарубежных аналогов, 1 опережает их, 3 находятся в состоянии паритета и 2 отстают от зарубежных аналогов. В рамках группы решений назначения «Системы локального позиционирования» наблюдается отставание российских компаний относительно зарубежных аналогов.

В рамках технологии «Средства сбора и / или обработки информации из внешней среды» наблюдается

преимущественный паритет российский разработок с зарубежными аналогами. При этом 8,3% от всех решений опережают зарубежные аналоги по своим свойствам, а 54% не уступают им, на основе чего можно заключить, что российские компании при благоприятных рыночных условиях и снятии ограничений могут выходить на лидирующие позиции.

Рисунок 45. Карточка технологического ландшафта «Средства сбора и / или обработки информации из внешней среды»

Средства сбора и / или обработки информации из внешней среды		
Назначение	Уровень развития	Отечественные компании
Контроль технологических, производственных и логистических процессов	Паритет	
Сбор биометрических и физиологических параметров человека и иных образов	Паритет	
Системы локального позиционирования	Отставание	

Источник: МГУ имени М.В.Ломоносова, 2022 год

Технологии проектирования и моделирования

В рамках технологий проектирования и моделирования компаниями направления «Технет» НТИ реализуется 27 решений и проектов. Ниже представлена карточка технологического ландшафта «Технологии проектирования и моделирования».

Рисунок 46. Карточка технологического ландшафта «Технологии проектирования и моделирования»

Технологии проектирования и моделирования		
Назначение	Уровень развития	Отечественные компании
Мониторинг, имитационное моделирование и прогнозирование	Паритет	
Автоматизация бизнес-процессов	Паритет	
Воссоздание окружающей среды в 3D	Паритет	

Источник: МГУ имени М.В.Ломоносова, 2022 год

Для технологий проектирования и моделирования наблюдается паритет всех трех групп решений относительно зарубежных аналогов. В рамках группы решений назначения «Мониторинг, имитационное моделирование и прогнозирование» 8 находятся в состоянии паритета по отношению к зарубежным аналогам, а 7 отстают от них. Для группы решений назначения «Автоматизация бизнес-процессов» наблюдается следующее распределение: 2 не имеют аналогов, 1 опережает зарубежные аналоги, 3 находятся в состоянии паритета, 4 отстают от зарубежных аналогов. Группа решений назначения «Воссоздание окружающей среды в 3D» состоит из двух: 1 из них находится в паритете с зарубежными аналогами, а 1 отстает, однако первое решение может частично выполнять функции второго, в связи с чем всей группе присвоен статус паритета.

В рамках технологий проектирования и моделирования 44,4% разработок находятся в отстающей позиции по сравнению с зарубежными аналогами, однако также 44,4% решений находятся в условиях паритета, 3,7% опережают зарубежные аналоги и 7,4% не имеют их. На основе этих данных можно ожидать снижения доли отстающих решений в случае сохранения благоприятных экономических условий и международного климата для развития отечественных компаний.

Интернет вещей

Для технологии «Интернет вещей» компаниями направления «Технет» НТИ реализуется 11 продуктов и проектов. Ниже представлена карточка технологического ландшафта «Интернет вещей».

Рисунок 47. Карточка технологического ландшафта «Интернет вещей»

Интернет вещей		
Назначение	Уровень развития	Отечественные компании
Автоматизация промышленных процессов мониторинга и сбора данных	Паритет	     
Автоматизация мониторинга и сбора данных в пищевой промышленности	Отставание	 
Автоматизация мониторинга жилых сооружений и потребительских приборов	Паритет	 

Источник: МГУ имени М.В.Ломоносова, 2022 год

Для технологии «Интернет вещей» наблюдается паритет двух групп решений назначения «Автоматизация промышленных процессов мониторинга и сбора данных» и «Автоматизация мониторинга жилых сооружений и потребительских товаров» относительно зарубежных аналогов. В рамках группы решений назначения «Автоматизация промышленных процессов мониторинга и сбора данных» 1 опережает зарубежные аналоги, 3 находятся в состоянии паритета и 2 отстают от них. В группу решений назначения «Автоматизация мониторинга жилых сооружений и потребительских приборов» включены 2, оба из которых находятся в состоянии паритета. В группу решений назначения «Автоматизация мониторинга и сбора данных в пищевой промышленности» включены 3, два из которых отстают от зарубежных аналогов, а одно находится в состоянии паритета.

36,4% разработок технологии «Интернет вещей» отстают от зарубежных аналогов, 54,5% находятся в состоянии паритета, а 9,1% – опережают зарубежные аналоги. На основе этих данных можно сделать вывод о том, что в рамках технологии «Интернет вещей» отечественные решения в большинстве не отстают от зарубежных аналогов

и успешно с ними конкурируют, при этом имеются перспективы опережающего роста при сохранении благоприятных экономических и технологических условий для этих компаний.

Облачные вычисления

В рамках технологии «Облачные вычисления» компаниями направления «Технет» НТИ реализуется 6 продуктов и проектов. Ниже представлена карточка технологического ландшафта «Облачные вычисления».

Рисунок 48. Карточка технологического ландшафта «Облачные вычисления»

Облачные вычисления		
Назначение	Уровень развития	Отечественные компании
Промышленная аналитика и управление	Паритет	 
Контроль и анализ несистематизированных данных	Паритет	

Источник: МГУ имени М.В.Ломоносова, 2022 год

Для технологии «Облачные вычисления» наблюдается паритет относительно зарубежных аналогов для двух групп решений назначения «Промышленная аналитика и управление» и «Контроль и анализ несистематизированных данных». В рамках первой группы 1 решение не имеет зарубежных аналогов, 1 находится в состоянии паритета и 1 отстает от зарубежных аналогов. В рамках второй группы 1 решение опережает зарубежные аналоги и 2 находятся в состоянии паритета.

В рамках всей технологии «Облачные вычисления» 33,4% разработок опережают зарубежные аналоги или не имеют таковых, 50% решений находятся в состоянии паритета с зарубежными аналогами и 16,6% отстают от них. Решения технологии «Облачные вычисления» сильно зависят от поставок вычислительных микросхем (процессоров), которые в России не производятся по современным технологическим нормам. В соответствии с этим российские системы облачных вычислений находятся под риском снижения доли паритетных устройств и повышения доли отстающих устройств из-за усложненного доступа к новейшим компонентам.

Большие данные

Для технологии «Большие данные» компаниями направления «Технет» НТИ реализуется 6 продуктов и проектов. Ниже представлена карточка технологии «Большие данные».

В рамках технологии «Большие данные» 2 группы решений назначения «Мониторинг бизнес-процессов» и «Анализ и управление бизнес-единицами» находятся в состоянии паритета относительно зарубежных аналогов, при этом лишь одно из первой группы решений не имеет аналогов, а остальные 5 находятся на уровне паритета с зарубежными аналогами. Решения технологии «Большие данные» в 83,3% случаев находятся в состоянии паритета с зарубежными аналогами и в 16,7% случаев не имеют таковых.

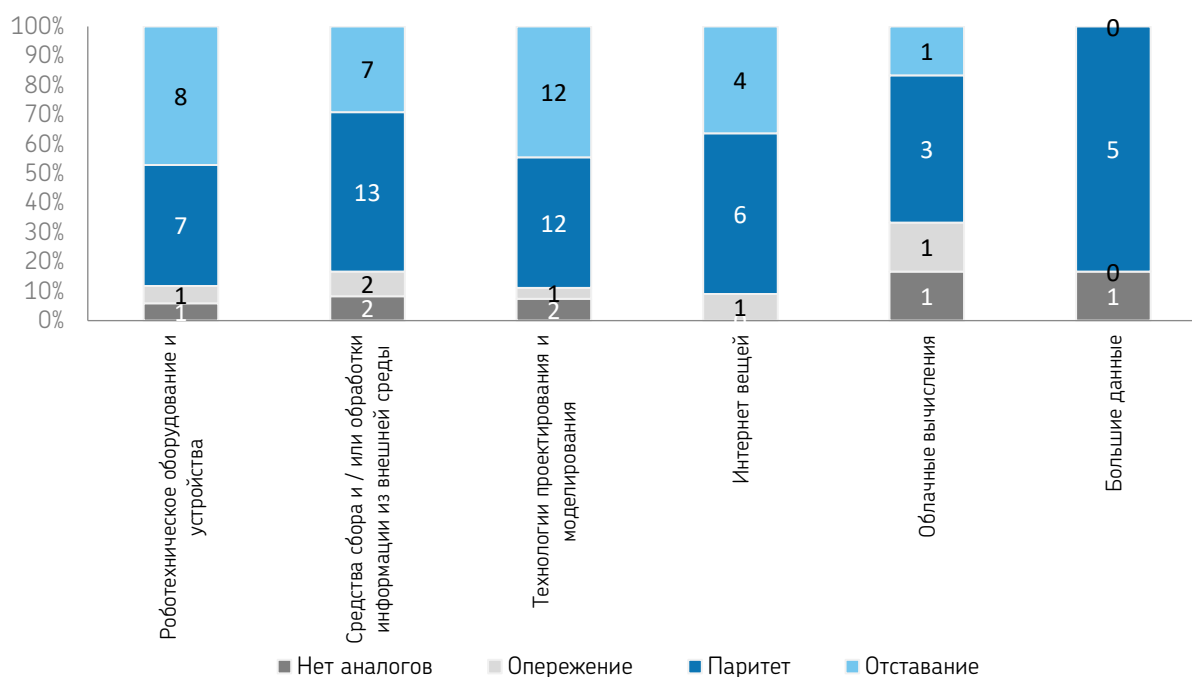
Ниже представлена сводная диаграмма, иллюстрирующая долю продуктов / проектов в составе технологии с опережением, паритетом или отставанием относительно зарубежных аналогов.

Рисунок 49. Карточка технологического ландшафта «Большие данные»

Большие данные		
Назначение	Уровень развития	Отечественные компании
Мониторинг бизнес-процессов	Паритет	  
Анализ и управление бизнес-единицами	Паритет	  

Источник: МГУ имени М.В.Ломоносова, 2022 год

Рисунок 50. Доля продуктов / проектов в составе технологии с опережением, паритетом или отставанием относительно зарубежных аналогов



Источник: МГУ имени М.В.Ломоносова, 2022 год

Наиболее развитой технологией на рынке РФ является «Облачные вычисления»: в рамках данной технологии 16,7% решений опережают зарубежные аналоги и 16,7% не имеют таковых, 50% находятся в паритете. Также необходимо выделить технологию «Большие данные», в рамках которой 83,3% решений находятся в паритете с зарубежными аналогами и 16,7% не имеют аналогов. Самыми отстающими технологиями являются «Робототехническое оборудование и устройства» и «Технологии проектирования и моделирования»: 47% и 44,4% отстающих решений соответственно, 41,2% и 44,4% решений в паритете соответственно.

ЗАКЛЮЧЕНИЕ

В аналитическом отчете рассмотрена концепция киберфизических систем как одного из важнейших элементов развития цифровой промышленности. Киберфизические системы рассмотрены в отчете с позиции применения в рамках 7 «сквозных» технологий направления «Технет» НТИ (цифровое проектирование и моделирование; новые материалы; аддитивные технологии; промышленная сенсорика; робототехника; большие данные; промышленный интернет вещей).

В первой главе отчета киберфизические системы рассмотрены в качестве рыночного явления. Проанализирован уровень сформированности рынка киберфизических систем в целом, приведены оценки объема и темпов роста рынка, демонстрирующие активное развитие данного технологического направления. Кроме того, в рамках анализа сегментов рынка киберфизических систем рассмотрены рынки технологий, составляющих элементы физической (промышленная робототехника, сенсорика и рынок промышленного интернета вещей) и программной среды (рынок цифрового проектирования и моделирования больших данных) киберфизических систем. Также, описаны ключевые тенденции, наблюдаемые на рынке киберфизических систем.

Во второй главе отчета представлены результаты анализа барьеров и рисков, препятствующих развитию рынка киберфизических систем, а также практик нормативного правового регулирования данного рыночного направления. Результаты анализа свидетельствуют о том, что барьеры развития технологий, применяемых на рынке киберфизических систем, отличаются по различным направлениям. Тем не менее, в качестве наиболее крупной проблемы выделяются вопросы обеспечения безопасности. Инициативы в области киберфизических систем и смежных технологий, направленные на поддержку развития данного рыночного направления, реализуются во всем мире. Основной фокус мер государственного регулирования сосредоточен на создании или усилении конкурентных преимуществ с использованием технологий киберфизических систем, а также обеспечении кибербезопасности государственного сектора, объектов инфраструктуры и промышленности. Итоги анализа позволяют утверждать, что в национальном нормативно-техническом ландшафте по киберфизическим системам присутствуют значительные резервы развития. Утверждение соответствующих тематических стандартов будет способствовать обеспечению импортонезависимости, а также активному распространению решений на основе цифровых технологий на российском рынке.

Третья глава отчета содержит результаты анализа основных игроков и проектов на рынке киберфизических систем в применении к «сквозным» технологиям направления «Технет» НТИ. Полученные результаты позволяют заключить, что важнейшими участниками глобального рынка киберфизических систем, оказывающими наибольшее влияние на его развитие, являются крупные зарубежные корпорации. В главе рассмотрены основные бизнес-модели, применяемые ключевыми игроками рынка, а также приведены примеры лучших практик их реализации. Кроме того, изучена активность компаний-лидеров на рынке киберфизических систем с точки зрения реализованных проектов, привлеченных инвестиций, проведенных сделок слияния и поглощения, а также коопераций между компаниями.

Четвертая глава отчета представляет подробный анализ основных технологий на рынке киберфизических систем в применении к «сквозным» технологиям направления «Технет» НТИ. Кроме того, в главе представлен обзор ключевых научных разработок в данной области в мире и в России.

Пятая глава отчета посвящена комплексному рассмотрению широкого перечня показателей, характеризующих деятельность компаний «Технет» НТИ, специализирующихся на разработке решений в области развития киберфизических систем.

ПРИЛОЖЕНИЕ

Приложение 1. Перечень технических комитетов и стандартов, разработанных Международной организацией по стандартизации (ISO, ИСО) совместно с Международной электротехнической комиссией (IEC, МЭК)

В обзоре нормативно-технической деятельности ISO в области киберфизических систем приведены следующие технические комитеты и разработанные стандарты:

1. ISO / TC 299 Робототехника (Robotics);
 - ISO / DIS 5363 Робототехника. Методы проведения испытаний экзоскелетного шагающего робота RACA (Robotics. Test methods for exoskeleton-type walking RACA robot) – в стадии разработки;
 - ISO 8373:2021 Робототехника. Словарь (Robotics. Vocabulary);
 - ISO / FDIS 10218-1 Робототехника. Требования безопасности. Часть 1: Промышленные роботы (Robotics. Safety requirements. Part 1: Industrial robots) – в стадии разработки;
 - ISO / FDIS 10218-2 Робототехника. Требования безопасности. Часть 2: Промышленные роботизированные системы, робототехнические приложения и роботизированные ячейки (Robotics. Safety requirements. Part 2: Industrial robot systems, robot applications and robot cells) – в стадии разработки;
 - ISO 11593:2022 Роботы для промышленной среды. Системы автоматической смены рабочего органа. Словарь (Robots for industrial environments. Automatic end effector exchange systems. Vocabulary);
 - ISO 13482:2014 Роботы и роботизированные устройства. Требования безопасности для роботов личного пользования (Robots and robotic devices. Safety requirements for personal care robots);
 - ISO / TS 15066:2016 Роботы и роботизированные устройства. Коллаборативные роботы (Robots and robotic devices. Collaborative robots);
2. ISO / TC 241 Системы управления безопасностью дорожного движения (Road traffic safety management systems);
 - ISO / DIS 39003 Безопасность дорожного движения. Руководство по этическим аспектам, касающимся безопасности автономных транспортных средств (Road Traffic Safety (RTS). Guidance on ethical considerations relating to safety for autonomous vehicles) – в стадии разработки;
3. ISO / TC 22 Дорожные транспортные средства (Road vehicles);
 - ISO / TR 4804:2020 Дорожные транспортные средства. Безопасность и кибербезопасность автоматизированных систем вождения. Разработка, верификация и валидация (Road vehicles. Safety and cybersecurity for automated driving systems. Design, verification and validation);
4. ISO / TC 127 Техника для земляных работ (Earth-moving machinery);
 - ISO 17757:2019 Техника для земляных работ и добыча. Безопасность автономных и полуавтономных технических систем (Earth-moving machinery and mining. Autonomous and semi-autonomous machine system safety);
5. ISO / TC 204 Интеллектуальные транспортные системы (Intelligent transport systems);
 - ISO 22737:2021 Интеллектуальные транспортные системы. Малоскоростные автоматические системы вождения по заранее установленным маршрутам. Требования к производительности, системные требования и процедуры испытания производительности (Intelligent transport systems. Low-speed automated driving (LSAD) systems for predefined routes. Performance requirements, system requirements and performance test procedures);

6. ISO / TC 268 Устойчивые города и населенные пункты (Sustainable cities and communities);
 - ISO 37181:2022 «Умная» городская инфраструктура. «Умное» передвижение автономных транспортных средств на общественных дорогах (Smart community infrastructures. Smart transportation by autonomous vehicles on public roads);
 - ISO 37106:2021 Устойчивые города и населенные пункты. Руководство по формированию функциональной модели «умного» города для устойчивых населенных пунктов (Sustainable cities and communities. Guidance on establishing smart city operating models for sustainable communities);
 - ISO 37122:2019 Устойчивые города и населенные пункты. Показатели «умных» городов (Sustainable cities and communities. Indicators for smart cities);
 - ISO 37123:2019 Устойчивые города и населенные пункты. Показатели устойчивых городов (Sustainable cities and communities. Indicators for resilient cities);
7. ISO / IEC JTC 1 / SC 41 Интернет вещей и цифровые двойники (Internet of things and digital twin);
 - ISO / IEC 20924:2021 Информационные технологии. Интернет вещей (IoT). Словарь (Information technology. Internet of Things (IoT). Vocabulary);
 - ISO / IEC 21823-1:2019 Интернет вещей (IoT). Интероперабельность систем Интернета вещей. Часть 1: Структура (Internet of things (IoT). Interoperability for IoT systems. Part 1: Framework);
 - ISO / IEC 21823-2:2020 Интернет вещей (IoT). Интероперабельность систем Интернета вещей. Часть 2: Интероперабельность транспорта (Internet of things (IoT). Interoperability for IoT systems. Part 2: Transport interoperability);
 - ISO / IEC 21823-3:2021 Интернет вещей (IoT). Интероперабельность систем Интернета вещей. Часть 3: Семантическая интероперабельность (Internet of things (IoT). Interoperability for IoT systems. Part 3: Semantic interoperability);
 - ISO / IEC 21823-4:2022 Интернет вещей (IoT). Интероперабельность систем Интернета вещей. Часть 4: Синтаксическая интероперабельность (Internet of things (IoT). Interoperability for IoT systems. Part 4: Syntactic interoperability);
 - ISO / IEC 30141:2018 Интернет вещей (IoT). Эталонная архитектура (Internet of Things (IoT). Reference Architecture);
 - ISO / IEC 30147:2021 Информационные технологии. Интернет вещей (IoT). Методология определения надежности систем и услуг Интернета вещей (Information technology. Internet of things. Methodology for trustworthiness of IoT system/service);
 - ISO / IEC 30162:2022 Интернет вещей (IoT). Требования и модель совместимости для устройств в системах промышленного Интернета вещей (Internet of Things (IoT). Compatibility requirements and model for devices within industrial IoT systems);
 - ISO / IEC 30165:2021 Интернет вещей (IoT). Структура Интернета вещей в реальном времени (Internet of Things (IoT). Real-time IoT framework);
8. ISO / IEC JTC 1 / SC 27 Информационная безопасность, кибербезопасность и защита конфиденциальности (Information security, cybersecurity and privacy protection) [101];
 - ISO / IEC 27701:2019 Методы обеспечения безопасности. Расширение стандартов ISO / IEC 27001 и ISO / IEC 27002 для управления конфиденциальной информацией. Требования и рекомендации (Security techniques. Extension to ISO / IEC 27001 and ISO / IEC 27002 for privacy information management. Requirements and guidelines);
9. ISO / IEC JTC 1 Информационные технологии (Information technology);
 - ISO / IEC 24039:2022 Информационные технологии. Эталонная архитектура цифровой платформы «умного» города. Данные и обслуживание (Information technology. Smart city digital platform reference architecture. Data and service);
 - ISO / IEC 30182:2017 Концептуальная модель «умного» города. Руководство по формированию модели интероперабельности данных (Smart city concept model. Guidance for establishing a model

for data interoperability);

10. ISO / TC 59 / SC 17 Устойчивость зданий и сооружений гражданского строительства (Sustainability in buildings and civil engineering works);
 - ISO 21678:2020 Устойчивость зданий и сооружений гражданского строительства. Показатели и критерии. Принципы, требования и рекомендации (Sustainability in buildings and civil engineering works. Indicators and benchmarks. Principles, requirements and guidelines);
11. ISO / TC 205 Проектирование зданий с учетом экологических требований (Building environment design);
 - ISO 17800:2017 Информационная модель интеллектуальной электросети для производственных и жилых объектов (Facility smart grid information model).

Приложение 2. Перечень международной нормативно-технической документации, регулирующей область киберфизических систем

Таблица 18. Перечень нормативно-технической документации, разрабатываемой международными организациями в области киберфизических систем

№	Наименование	Страна, организация	Краткое описание
Северная Америка			
1	Дорожная карта космических технологий. Моделирование, испытания, информационные технологии и обработка (Space Technology Roadmap for TA11, Modeling, Simulation, Information Technology and Processing), 2010 [245–247]	США, Национальное управление по аэронавтике и исследованию космического пространства (National Aeronautics and Space Administration, NASA)	В дорожной карте упоминаются киберфизические системы, робототехника, автономные системы, нанотехнологии и др. в качестве технологий, применимых для развития США в изучении космического пространства.
2	Инициатива моделирования и анализа киберфизических систем (Cyber-Physical Systems Modeling and Analysis (CPSMA) Initiative) [245]	США, Национальное управление по аэронавтике и исследованию космического пространства (National Aeronautics and Space Administration, NASA)	Инициатива разработана с целью получения преимуществ от применения киберфизических систем при осуществлении длительных полетных экспедиций НАСА. Инициатива сосредоточена на функционировании двигателей, автономности и обеспечении жизненного цикла. Ожидается расширение возможностей прогнозирования и управления поведением систем, обеспечение устойчивости, адаптивности, управляемости, достижение безопасности, обеспечение совместной работы в единой среде.
3	Национальная кибер-стратегия США (National Cyber Strategy of the United States of America), 2018 [248]	США, Белый дом	В документе представлена стратегия США по обеспечению кибербезопасности государства.
4	IEEE Кибербезопасность для «умных» сетей (IEEE Cyber Security for the Smart Grid), 2013 [249]	США, Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE)	В документе описываются возможные сценарии угроз для «умных» сетей и предлагаются меры по обеспечению кибербезопасности.
5	IEEE C37.240-2014 Требования к кибербезопасности для систем автоматизации, защиты и управления энергосистем (IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems), 2014 [250]	США, Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE)	Стандарт содержит технические требования к кибербезопасности энергосистемы. На основе практического опыта предложены требования для достижения высокого уровня кибербезопасности систем автоматизации, защиты и управления энергосистем, независимо от уровня напряжения или критичности активов.
6	ANSI / ISA-62443-3-3 (99.03.03)-2013 Безопасность для систем	США, Американский национальный институт	В документе приведены требования и потенциальные возможности

№	Наименование	Страна, организация	Краткое описание
	автоматизации и управления. Часть 3-3: Требования к безопасности систем и уровни обеспечения безопасности (Security for industrial automation and control systems. Part 3-3: System security requirements and security levels), 2013 [251]	стандартов (ANSI – American National Standards Institute), Международное общество автоматизации (International Society of Automation, ISA)	по обеспечению безопасности систем. Помимо этого стандарта были разработаны нормативно-технические документы, регламентирующие деятельность в области кибербезопасности, такие как: • ISA-TR99.00.01-2007, • ISA-62443-1-1-2007, • ISA-62443-2-1-2009, • ISA-TR62443-2-3-2015, • ANSI / ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, • ANSI / ISA-62443-3-2-2020, • ANSI / ISA-62443-4-1-2018, • ANSI / ISA-62443-4-2-2018.
7	GAO-19-332 Рекомендации по защите критически важных объектов инфраструктуры (Critical infrastructure protection), 2019 [252]	США, Счетная Палата (U.S. Government Accountability Office)	В рамках исследования был проведен анализ аварий, возникающих при функционировании энергетических систем, и были сформулированы рекомендации для Федеральной комиссии по регулированию энергетики (Federal Energy Regulatory Commission, FERC) и Министерства энергетики, которые провели оценку предложенных изменений и планируют провести соответствующие мероприятия.
8	Серия стандартов по защите критической инфраструктуры (NERC Critical Infrastructure Protection (CIP) standards) [253]	США, Североамериканская корпорация по надежности электроснабжения (North American Electric Reliability Corp., NERC)	Комплекс стандартов включает 40 стандартов и, в общей сложности, более 100 дополнительных требований, направленных на защиту критической киберинфраструктуры в Северной Америке.
9	Общая система рекомендаций по безопасности (Common Security Advisory Framework. Version 2.0), 2022 [254]	США, Организация по продвижению стандартов структурированной информации (OASIS, Organization for the Advancement of Structured Information Standards)	В документе предложены рекомендации по безопасности в виде структурированной информации о продуктах, взаимодействии и совместной работе заинтересованных сторон.
10	Область знаний безопасности киберфизических систем. Версия 1.0.1 (Cyber-Physical Systems Security Knowledge Area. Version 1.0.1), 2021 [255; 256]	США, Калифорнийский университет в Санта-Крузе (University of California, Santa Cruz)	В документе приведен обзор развивающейся области безопасности киберфизических систем и приведены рекомендации Правительству для устранения возможных угроз по нарушению кибербезопасности.
11	Законопроект относительно кибербезопасности. Закон о защите критических киберсистем (Bill C-26, An Act Respecting Cyber Security (ARCS). Critical Cyber Systems Protection Act), 2022 [257]	Канада, Правительство	В документе устанавливается правовой режим об обязательной защите критически важных киберсистем в некоторых отраслях экономики и приведен инструмент для

№	Наименование	Страна, организация	Краткое описание
			защиты от возникновения киберугроз.
12	Основы кибербезопасности канадского пространства киберинфраструктуры (Fundamentals of Cyber Security for Canada's CI Community), 2016 [258]	Канада, Правительство, рабочая группа Национального кросс-отраслевого форума по критической инфраструктуре (National Cross Sector Forum on Critical Infrastructure working group)	Документ предлагает практические рекомендации по повышению безопасности критической инфраструктуры, меры по смягчению возможных последствий при возникновении угроз и достижению минимального базового уровня кибербезопасности.
13	Стратегия кибербезопасности Канады (Canada's Cyber Security Strategy), 2010 [259]	Канада, Правительство	Документ направлен на формирование Канадской киберсистемы и приводит рекомендации по смягчению последствий кибератак.
Европейский союз (ЕС)			
14	Национальная кибер-стратегия (National Cyber Strategy), 2022 [54]	Соединенное Королевство Великобритании и Северной Ирландии, Правительство	Национальная кибер-стратегия направлена на обеспечение условий для адаптации и внедрения инноваций с учетом вызовов цифровой трансформации и киберпространства. Стратегия является продолжением работы в области кибербезопасности, начатой в 2016 году. В качестве основных направлений деятельности в стратегии выделены: • укрепление кибер-экосистемы; • обеспечение устойчивости; • применение технологий; • обмен опытом; • повышение безопасности и борьба с кибератаками.
15	Создание национальной киберфизической инфраструктуры для стимулирования инноваций: консультационный документ (Enabling a national Cyber-Physical Infrastructure to catalyse innovation: consultation document), 2022 [57; 260]	Соединенное Королевство Великобритании и Северной Ирландии, Министерство бизнеса, энергетики и производственных стратегий	Стратегия направлена на создание инноваций, объединяющих цифровой и физический мир. В качестве технологий, обеспечивающих создание киберфизической инфраструктуры, в документе упоминаются искусственный интеллект, цифровые двойники, робототехника, дополненная и виртуальная реальность, сенсоры и другое. В рамках стратегии предлагают бизнес-сообществу пройти опрос, направленный на выявление возможностей применения киберфизических систем. Отдельное внимание уделено кадрам, культуре, вопросам технических разработок, безопасности, совместимости, устойчивости и совместной работе.

№	Наименование	Страна, организация	Краткое описание
			Некоторые представители бизнеса, в частности, Robotics Growth Partnership, предложили свое видение концепции развития киберфизической инфраструктуры, которая легла в основу консультационного документа [260].
16	Иновационная стратегия Соединенного Королевства (UK Innovation Strategy), 2021 [56]	Соединенное Королевство Великобритании и Северной Ирландии, Министерство бизнеса, энергетики и производственных стратегий	Стратегия рассчитана на период до 2035 года и, в частности, описывает возможность сбора информации от бизнеса (в соответствии со стратегией создания киберфизической инфраструктуры) с целью выявления возможностей применения цифровых двойников и киберфизических систем.
17	Стандарт минимального уровня кибербезопасности Правительства Великобритании (UK Government Minimum Cyber Security Standard), 2018 [261; 262]	Соединенное Королевство Великобритании и Северной Ирландии, Правительство	Первый стандарт в серии технических стандартов, устанавливающим положения кибербезопасности. Документ устанавливает ряд обязательных условий киберустойчивости и кибербезопасности, которые должны быть соблюдены всеми правительственными подразделениями в целях реализации программ Основ политики безопасности и Национальной стратегии по кибербезопасности.
18	Дорожная карта и стратегия по киберфизическим системам (CyPhERS – Cyber-Physical European Roadmap & Strategy), 2013 [263]	ЕС, Европейская комиссия (European Commission)	В рамках проекта была сформирована и предложена стратегия развития Европы, проведена оценка возможностей и угроз, оценен потенциал применения киберфизических систем.
19	Директива по обеспечению безопасности сетевых и информационных систем (Directive on Security of Network and Information Systems), 2016 [264]	ЕС, Европейская комиссия (European Commission)	Директива приводит первые общеевропейские правила к обеспечению кибербезопасности.
20	Научное форсайт-исследование «Этические аспекты киберфизических систем» (Scientific Foresight study Ethical Aspects of Cyber-Physical Systems), 2016 [265]	ЕС, Европейский парламентский отдел исследований (European Parliamentary Research Service)	Исследование направлено на выявление потенциальных этических проблем и связанных с ними последствий возможного развития технологии киберфизических систем, робототехники и искусственного интеллекта до 2050 года. Результатом исследования выступало описание правовых инструментов для прогнозирования последствий будущих разработок в области киберфизических систем, таких как интеллектуальные

№	Наименование	Страна, организация	Краткое описание
			робототехнические системы, связанные с Интернетом вещей.
21	Дорожная карта по стандартизации Индустрии 4.0 в Германии. Версия 4 (German Standardization Roadmap Industrie 4.0. Version 4), 2020 [266]	Федеративная Республика Германия, Немецкая комиссия по электротехнике, электронике и информационным технологиям при Немецком институте по стандартизации и Немецком союзе электротехники (DKE)	В рамках дорожной карты выявлены существующие пробелы в нормативном правовом поле Индустрии 4.0 и предложены рекомендации по совершенствованию законодательства. В дорожной карте также приведен перечень технических комитетов Европейских организаций по стандартизации, регулирующих аспекты Индустрии 4.0, в частности, рассмотрены некоторые технические комитеты IEC, ISO, ISO/IEC, CEN, CENELEC, IEEE, ETSI, ITU-T, IECCE.
22	ETSI TS 103 645 – Кибербезопасность для пользователей Интернета вещей (Cyber Security for Consumer Internet of Things), 2019 [267] ETSI EN 303 645 – Кибербезопасность для пользователей Интернета вещей: базовые требования (Cyber Security for Consumer Internet of Things: Baseline Requirements), 2020 [268]	Французская Республика, Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI)	В феврале 2019 года ETSI представил первый отраслевой стандарт для потребительских устройств, подключенных к Интернету вещей. ETSI 103 645 приводит практические указания в области безопасности Интернета вещей для потребителей. ETSI 303 645, опубликованный в июне 2020 года, устанавливает базовый уровень безопасности для потребительских устройств, подключенных к Интернету вещей, и обеспечивает возможность сертификации продуктов Интернета вещей [269].
23	ISO / IEC TS 27100:2020(en) Информационные технологии – Кибербезопасность – Обзор и концепция (Information technology — Cybersecurity — Overview and concepts), 2020 [270]	Швейцарская Конфедерация, Международная организация по стандартизации (International Organization for Standardization, ISO)	В документе описана кибербезопасность и соответствующая концепция, в том числе то, как она связана с информационной безопасностью и отличается от нее.
24	ISO / IEC TS 27110:2021(en) Информационные технологии, кибербезопасность и защита конфиденциальности – Рекомендации по разработке основ кибербезопасности (Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines), 2021 [271]	Швейцарская Конфедерация, Международная организация по стандартизации (International Organization for Standardization, ISO)	В документе изложены основные рекомендации по формированию основ кибербезопасности в деятельности различных организаций с целью упрощения процедур по обеспечению безопасности.
25	ITU-T X.1060 (06/2021) Структура для создания и эксплуатации центра по защите от киберугроз	Швейцарская Конфедерация, отдел стандартизации электросвязи	В Рекомендации центр по защите от киберугроз (CDC) определен как подразделение, которому отведена

№	Наименование	Страна, организация	Краткое описание
	(Framework for the creation and operation of a cyber defence centre), 2021 [272]	Международного союза электросвязи (International Telecommunication Union – Telecommunication sector, ITU-T)	центральная роль в обеспечении противодействия рискам кибербезопасности в организации. Структура описана как три процесса – построение, управление и оценка, которые CDC должен реализовать на практике. Описаны услуги, которые должна предусмотреть организация для принятия более конкретных мер кибербезопасности.
26	Стратегия 2030 (Strategy 2030), 2021 [273]	Королевство Бельгия, Европейский комитет по стандартизации (Comite Europeen de Normalisation, CEN), Европейский комитет электротехнической стандартизации (Comite Europeen de Normalisation Electrotechnique, CENELEC)	CEN и CENELEC в стратегии указывают, что стремятся помочь Европе воспользоваться преимуществами цифровизации, в частности, устанавливая стандарты для инноваций в области новых технологий, таких как Интернет Вещи, искусственный интеллект, кибербезопасность и квантовые технологии. В частности, функционирует технический комитет по обеспечению кибербезопасности CEN/CLC/JTC 13 – Кибербезопасность и защита данных (Cybersecurity and Data Protection). Помимо этого, был разработан стандарт CLC / TS 50701 Устройства железных дорог – кибербезопасность (Railway applications – Cybersecurity).
27	Стратегическая повестка по стандартизации в области киберфизических систем (Strategic Agenda on Standardization for Cyber-Physical Systems), 2017 [274]	Австрийская Республика, Австрийский технологический институт (AIT Austrian Institute of Technology)	В документе предложена концепция «мультистандарта» (Multi-Standard), который ориентирован на создание согласованной системы стандартов, обеспечивающих деятельность в сфере киберфизических систем. Также приводится описание новых технологических парадигм, возникших в области киберфизических систем, и дается прогноз влияния развития киберфизических систем на требования к безопасности и стандартизации в области Интернета вещей.
Азиатские государства			
28	GB/T 41262-2022 Технические требования к киберфизическим системам обнаружения аномалий для промышленных систем управления (Technical requirements of cyber-physical fusion anomaly detection system for industrial control system), 2022 [275]	Китайская Народная Республика, Управление стандартизацией (Guobiao Standards / Standardization Administration of China)	Документ устанавливает требования к киберфизическим системам, направленным на выявление аномалий. Управление стандартизации также публикует национальные стандарты по обеспечению кибербезопасности.

№	Наименование	Страна, организация	Краткое описание
29	Китай как «Великая кибер-держава»: Два голоса Пекина в телекоммуникациях (China as a “Cyber Great Power”: Beijing’s two voices in telecommunications), 2021 [276]	Китайская народная Республика, Brookings China Strategy Initiative	В документе рассмотрены возможности Китая в формировании кибер-инфраструктуры телекоммуникаций. В частности, проанализированы мнения, выражаемые Правительством, коммерческими организациями и обществом, для формирования цифровой архитектуры страны.
30	Белая книга по стандартизации кибербезопасности 5G (5G 网络安全 标准化 白皮书), 2021 [277]	Китайская Народная Республика, рабочая группа Национального технического комитета по стандартизации информационной безопасности	В Белой книге анализируются основы политики, текущее состояние промышленности, технические характеристики, связанные с кибербезопасностью 5G, риски безопасности и требования к стандартизации сети 5G.
31	Руководство по практике кибербезопасности, 2022 [278]	Китайская Народная Республика, юридическая компания King & Wood Mallesons	В руководстве рассмотрены основные требования к кибербезопасности, механизмы обмена информацией, тенденции развития законодательства в сфере кибербезопасности с учетом текущего уровня правового режима Китая.
32	Структура кибер/физической безопасности (Cyber/Physical Security Framework), 2019 [279]	Государство Япония, Министерство экономики, торговли и промышленности	В документе предложена концепция по формированию интеллектуальной инфраструктуры нового поколения Society 5.0 на основе кибер-физической сети с учетом необходимости обеспечения кибербезопасности.
33	Национальная миссия по междисциплинарным киберфизическим системам (National Mission on Interdisciplinary Cyber Physical Systems) [280; 281]	Республика Индия, Министерство науки и технологий	Деятельность миссии направлена на формирование экосистемы киберфизических систем. Основная задача – выявление потребностей бизнеса и обеспечение совместной работы министерств и сообщества для разработки решений по созданию и внедрению киберфизических систем.

Приложение 3. Стандарты в области киберфизических систем, приведенные в Перспективном плане стандартизации

Таблица 19. Перспективный план стандартизации в области передовых производственных технологий на 2018–2025 годы (с изменениями №1, №2) в области киберфизических систем

№	Наименование, вид, категория разрабатываемого / пересматриваемого нормативного документа	Вид работы	Сроки выполнения		ОКС / ОКПД 2	Вид стандарта	Статус реализации
			начало	окончание			
1	Система киберфизическая. Термины и определения	Разработка ПНСТ	2020	2021	01.040.35, 35.020	Стандарт на термины и определения	Введен в действие ПНСТ 417–2020 Система киберфизическая. Термины и определения
2	Система киберфизическая. Общие положения	Разработка ПНСТ	2020	2021	35.020	Стандарты на продукцию (услуги). Общие требования	Введен в действие ПНСТ 416–2020 Система киберфизическая. Общие положения
3	Система киберфизическая. Дорожная карта стандартов	Разработка ПНСТ	2020	2021	35.020	Общетехнический стандарт	Планируется к разработке
4	Система киберфизическая. Типовая модель для киберфизических управляемых интеллектуальных станкостроительных систем (CPSMT) – Часть 1. Общие положения	Разработка ПНСТ, Модификация МС ISO 23704-1 – MOD	2022	2023	35.020	Стандарты на продукцию (услуги). Общие требования	Срок реализации – 2023 год.
5	Система киберфизическая. Типовая модель для киберфизических управляемых интеллектуальных станкостроительных систем (CPSMT) – Часть 2. Типовая архитектура	Разработка ПНСТ, Модификация МС ISO 23704-2 – MOD	2022	2023	35.020	Общетехнический стандарт	Срок реализации – 2023 год.
6	Система киберфизическая. Онтология верхнего уровня	Разработка ПНСТ	2021	2022	35.020	Общетехнический стандарт	Планируется к разработке
7	Киберфизические системы. Типовая модель для киберфизических управляемых интеллектуальных станкостроительных систем (CPSMT). Часть 3. Типовая архитектура для аддитивного производства	Разработка ПНСТ, Модификация МС ISO 23704-3 – MOD	2023	2024	25.040.01, 25.040.40, 35.240.50	–	Срок реализации – 2024 год.

№	Наименование, вид, категория разрабатываемого / пересматриваемого нормативного документа	Вид работы	Сроки выполнения		ОКС / ОКПД 2	Вид стандарта	Статус реализации
			начало	окончание			
8	Система киберфизическая. Термины и определения	Разработка ГОСТ Р на основе ПНСТ 416–2020	2023	2024	35.020	–	Срок реализации – 2024 год.
9	Система киберфизическая. Общие положения	Разработка ГОСТ Р на основе ПНСТ 417–2020	2023	2024	35.020	–	Срок реализации – 2024 год.

Приложение 4. Перечень национальных стандартов, разработанных по технологиям, смежным с киберфизическими системами

Ниже приведен перечень национальных стандартов и проектов национальных стандартов, разработанных ТК 194 «Кибер-физические системы» по технологиям, смежным с киберфизическими системами:

1. ПНСТ 428–2020 Умное производство. Двойники цифровые производства. Элементы визуализации цифровых двойников производства;
2. ПНСТ 429–2020 Умное производство. Двойники цифровые производства. Часть 1. Общие положения;
3. ПНСТ 430–2020 Умное производство. Двойники цифровые производства. Часть 2. Типовая архитектура;
4. ПНСТ 431–2020 Умное производство. Двойники цифровые производства. Часть 3. Цифровое представление физических производственных элементов;
5. ПНСТ 432–2020 Умное производство. Двойники цифровые производства. Часть 4. Обмен информацией;
6. ПНСТ 434–2020 Умное производство. Интероперабельность единиц возможностей для промышленных прикладных решений. Часть 1. Критерии интероперабельности единиц возможностей согласно требованиям к применению;
7. ПНСТ 435–2020 Умное производство. Интероперабельность единиц возможностей для промышленных прикладных решений. Часть 2. Шаблоны возможностей и каталогизация программных блоков;
8. ПНСТ 436–2020 Умное производство. Интероперабельность единиц возможностей для промышленных прикладных решений. Часть 3. Верификация и валидация интероперабельности единиц возможностей;
9. ПНСТ 758–2022 Умное производство. Интероперабельность единиц возможностей для промышленных прикладных решений. Часть 4. Определение единиц возможностей (введение в действие: 01.01.2023 г.);
10. ПНСТ 437–2020 Умное производство. Интерфейсы для ухода за автоматизированной машиной. Часть 1. Общие положения;
11. ПНСТ 448–2020 Умное производство. Унифицированная архитектура OPC. Часть 1. Общие положения;
12. ПНСТ 795–2022 Умное производство. Каталоги поведения оборудования для виртуальной производственной системы. Часть 1. Общие положения (введение в действие: 01.01.2023 г.);
13. ПНСТ 535–2021 Умное производство. Методы математического моделирования и виртуализации испытаний изделий на тепловые воздействия при проектировании. Общие требования;
14. ПНСТ 536–2021 Умное производство. Методы математического моделирования и виртуализации испытаний изделий на механические воздействия при проектировании. Общие требования;
15. ПНСТ 537–2021 Умное производство. Технология математического моделирования и виртуализации испытаний изделий на внешние воздействующие факторы на всех этапах жизненного цикла. Общие требования;
16. ПНСТ 647–2022 Умное производство. Системы автоматизации производства и их интеграция. Оценка конвергенции информатизации и индустриализации для промышленных предприятий. Часть 1. Структура и типовая модель (введение в действие: 01.01.2023 г.);
17. ПНСТ 648–2022 Умное производство. Системы автоматизации производства и их интеграция. Оценка конвергенции информатизации и индустриализации для промышленных предприятий. Часть 2. Модель зрелости и методология оценки (введение в действие: 01.01.2023 г.);
18. ПНСТ 796–2022 Умное производство. Системы автоматизации производства и их интеграция. Стандартизированные процедуры проектирования производственных систем. Часть 5. Управление производственными изменениями (введение в действие: 01.01.2023 г.);
19. ПНСТ 797–2022 Умное производство. Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 4.2. Интегрированные

- обобщенные ресурсы. Геометрическое и топологическое представление (введение в действие: 01.01.2023 г.);
20. ПНСТ 793–2022 Умное производство. Спецификация формата файла аддитивного производства AMF (введение в действие: 01.01.2023 г.);
 21. ПНСТ 518–2021 Информационные технологии. Интернет вещей. Термины и определения;
 22. ПНСТ 354–2019 Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi);
 23. ПНСТ 419–2020 Информационные технологии. Интернет вещей. Общие положения;
 24. ПНСТ 420–2020 Информационные технологии. Интернет вещей промышленный. Типовая архитектура;
 25. ПНСТ 423–2020 Информационные технологии. Сети сенсорные. Службы и интерфейсы, поддерживающие совместную обработку данных в интеллектуальных сенсорных сетях;
 26. ПНСТ 438–2020 Информационные технологии. Интернет вещей. Типовая архитектура;
 27. ПНСТ 433–2020 Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей;
 28. ПНСТ 644–2022 Информационные технологии. Интернет вещей. Совместимость систем интернета вещей. Часть 1. Структура;
 29. ПНСТ 446–2020 Информационные технологии. Интернет вещей. Совместимость систем интернета вещей. Часть 2. Совместимость на транспортном уровне;
 30. ПНСТ 516–2021 Информационные технологии. Интернет вещей. Спецификация LoRaWAN RU;
 31. ПНСТ 418–2020 Информационные технологии. Интернет вещей. Структура системы интернета вещей реального времени;
 32. ГОСТ Р 70036–2022 Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi);
 33. ПНСТ 421–2020 Информационные технологии. Сети сенсорные. Типовая архитектура сенсорных сетей. Часть 4. Модели сущностей;
 34. ПНСТ 422–2020 Информационные технологии. Сети сенсорные. Сетевой интерфейс прикладного программирования датчика;
 35. ПНСТ 649–2022 Информационные технологии. Сети сенсорные. Типовая архитектура сенсорных сетей. Часть 5. Описание интерфейсов (введение в действие: 01.01.2023 г.);
 36. ПНСТ 650–2022 Информационные технологии. Сети сенсорные. Типовая архитектура сенсорных сетей. Часть 6. Области применения (введение в действие: 01.01.2023 г.);
 37. ПНСТ 651–2022 Информационные технологии. Сенсорные сети. Типовая архитектура сенсорных сетей. Часть 7. Функциональная совместимость (введение в действие: 01.01.2023 г.);
 38. ПНСТ 521–2021 Информационные технологии. Подводная акустическая сенсорная сеть. Часть 1. Общие положения;
 39. ПНСТ 522–2021 Информационные технологии. Подводная акустическая сенсорная сеть. Часть 2. Типовая архитектура;
 40. ПНСТ 652–2022 Информационные технологии. Подводная акустическая сенсорная сеть. Часть 3. Сущности и интерфейсы (введение в действие: 01.01.2023 г.);
 41. ПНСТ 653–2022 Информационные технологии. Подводная акустическая сенсорная сеть. Часть 4. Функциональная совместимость (введение в действие: 01.01.2023 г.);
 42. ПНСТ 642–2022 Информационные технологии. Интернет вещей промышленный. Общие положения;
 43. ПНСТ 643–2022 Информационные технологии. Интернет вещей промышленный. Термины и определения (введение в действие: 31.03.2023 г.);
 44. ПНСТ 439–2020 Информационные технологии. Умный город. Совместимость данных;
 45. ПНСТ 440–2020 Информационные технологии. Умный город. Показатели ИКТ;
 46. ПНСТ 441–2020 Информационные технологии. Умный город. Онтология верхнего уровня для показателей умного города;
 47. ПНСТ 442–2020 Информационные технологии. Умный город. Руководства по обмену и

- совместному использованию данных;
- 48. ПНСТ 443–2020 Информационные технологии. Умный город. Общие положения по интеграции и функционированию инфраструктур умного города;
- 49. ПНСТ 444–2020 Информационные технологии. Умный город. Руководящие указания по переводной практике в области перевозок;
- 50. ПНСТ 445–2020 Информационные технологии. Умный город. Общая схема развития и функционирования;
- 51. ПНСТ 447–2020 Информационные технологии. Умный город. Типовая архитектура ИКТ умного города. Часть 3. Инженерные системы умного города.

Помимо этого, были подготовлены национальные стандарты и предварительные национальные стандарты по технологиям, смежным с киберфизическими системами, в рамках деятельности прочих технических комитетов:

- 1. ГОСТ Р 57700.37–2021 Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения;
- 2. ГОСТ Р 70249–2022 Системы искусственного интеллекта на автомобильном транспорте. Высокоавтоматизированные транспортные средства. Термины и определения (введение в действие: 01.01.2023 г.);
- 3. ГОСТ Р 70290–2022 Системы автоматизированного проектирования электроники. Термины и определения;
- 4. ГОСТ Р ИСО 18828–2–2020 Системы промышленной автоматизации и интеграция. Стандартизированные процедуры проектирования производственных систем. Часть 2. Процесс непрерывного планирования производства;
- 5. ГОСТ Р ИСО 18828–3–2020 Системы промышленной автоматизации и интеграция. Стандартизированные процедуры проектирования производственных систем. Часть 3. Информационные потоки в процессах;
- 6. ГОСТ Р ИСО 18828–4–2020 Системы промышленной автоматизации и интеграция. Стандартизированные процедуры проектирования производственных систем. Часть 4. Ключевые показатели эффективности процессов планирования производства;
- 7. ГОСТ Р ИСО 10303–21–2022 Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 21. Методы реализации. Кодирование открытым текстом структуры обмена (введение в действие: 01.01.2023 г.);
- 8. ГОСТ Р ИСО 10303–41–2022 Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 41. Интегрированный обобщенный ресурс. Основы описания и поддержки изделий (введение в действие: 01.01.2023 г.);
- 9. ГОСТ Р ИСО 10303–43–2022 Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 43. Интегрированный обобщенный ресурс. Структуры представления (введение в действие: 01.01.2023 г.);
- 10. ГОСТ Р ИСО 10303–44–2022 Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 44. Интегрированный обобщенный ресурс. Конфигурация структуры изделия (введение в действие: 01.01.2023 г.);
- 11. ГОСТ Р ИСО 10303–45–2022 Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными. Часть 45. Интегрированный обобщенный ресурс. Материал и другие технические характеристики (введение в действие: 01.01.2023 г.);
- 12. ПНСТ 366.4–2019 Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности;
- 13. ГОСТ Р МЭК 61297–2017 Системы управления промышленным процессом. Классификация адаптивных контроллеров для их оценки;
- 14. ГОСТ Р МЭК 60770–1–2015 Датчики для применения в системах управления промышленным процессом. Часть 1. Методы оценки рабочих характеристик;

15. серия стандартов ГОСТ Р ИСО 15746 «Системы интеграция и промышленной автоматизации»;
16. серия стандартов «Измерение, управление и автоматизация промышленного процесса»;
17. серия стандартов «Информационная технология» и другое.

Приложение 5. Стартапы в сфере киберфизических систем на 2021 год

Таблица 20. Самые успешные стартапы в сфере киберфизических систем на 2021 год

№	Компания	Страна	Сфера деятельности	Продукт / решение	Размер привлеченных инвестиций (млрд долл.)
1	Biosplice Therapeutics	США	Здравоохранение	Передовые компоненты сигнального пути Wnt	12
2	Bitmain Technologies	Китай	Разработка и производство оборудования	Микросхемы интегральных схем для конкретных приложений (Application-specific integrated circuit, ASIC) для майнинга биткоинов	12
3	Bytedance	Китай	Искусственный интеллект, социальные сети	Сервисы для создания и просмотра коротких видео (TikTok, Douyin, Xigua Video), новостные сети, социальные сети, облачный сервис для повышения производительности	140
4	Databricks	США	Разработка ПО	Автоматическое управление кластерами информации, корпоративное программное обеспечение	38
5	Devoted Health	США	Здравоохранение	Передовые технологии в области частного здравоохранения	12,6
6	DJI Innovations	Китай	Разработка и производство оборудования	Создание БПЛА, мультикоптеров, микроконтроллеров, видеооборудования (для стабилизации видеосъемки)	15
7	Faire	США	Искусственный интеллект	Мировая «умная» цепочка поставок	12,4
8	Global Switch	Великобритания	Телекоммуникационные сети	Создание облачных центров данных для большинства пользователей	11,1
9	SenseTime	Китай	Искусственный интеллект	Создание приложений по распознаванию человеческих лиц	12
10	ZongMu Technology	США	Автомобильная промышленность	Создание и разработка ПО для	11,4

№	Компания	Страна	Сфера деятельности	Продукт / решение	Размер привлеченных ин- вестиций (млрд долл.)
				автоматизации транспортных средств	

Источник: Центр НТИ СПбПУ по материалам Visual Capitalists, 2021 [163]

Приложение 6. Дополнительные материалы исследования по направлениям «новые материалы» и «аддитивные технологии»

Стоит отметить важность развития новых «умных» материалов и современных аддитивных технологий. Они не входят в привычную структуру КФС, однако изготовление различных физических элементов, а также аппаратной части вычислительных устройств с использованием инновационных материалов и технологий производства из них конечного изделия является одним из значимых факторов перехода к «умному» производству и Индустрии 4.0.

Новые материалы и технологии аддитивного производства предоставляют возможность создания нового класса изделий со сложной геометрией и улучшенными характеристиками, повышенной устойчивостью и адаптивностью к различным внешним факторам. Основные типы новых материалов, среди которых передовые полимерные материалы, керамические материалы, композиционные материалы и др., активно используются в аддитивном производстве [282].

Новые материалы

Новые материалы включают в себя совокупность технологий создания материалов, которые отличаются особыми эксплуатационными характеристиками и напрямую влияют на свойства конечного изделия, производимого для КФС или изделия для КФС. Данный комплекс технологий обеспечивает реализацию концепции инжиниринга – материал-конструкция (М-К) [190]. Новые материалы могут использоваться на всех этапах жизненного цикла: от создания базовых компонентов, до эксплуатации систем М-К. К главным преимуществам данных материалов можно отнести гибкость и изменчивость свойств (в зависимости от постановки задачи), а также возможность комбинации характеристик различных типов новых материалов путем их совместного использования в одной системе. В настоящее время инновационные материалы широко применяются в авиации, авиакосмической, нефтяной, химической и перерабатывающей промышленности.

Таблица 21. Новые материалы

Новые материалы	
Функции	Корпусирование объектов КФС
	Аддитивное производство
	Биопротезирование и биоинженерия
	Восстановление повреждений/дефектов частично или полностью
	Продление срока эксплуатации изделия
Области применения	Перерабатывающая промышленность
	Строительная сфера
	Транспортная система (морской, речной, железнодорожный транспорт) и логистика
	Авиационная и аэрокосмическая сфера
	Электроэнергетика
	Недропользование
	Медицина и фармацевтика
Технологии/ решения в основе	Деятельность в сфере телекоммуникаций
	Ударопрочные и физически-устойчивые новые материалы (высокотехнологичные сплавы, передовые полимеры, передовые композиционные материалы, передовые керамические материалы и проч.)
	Новые материалы аддитивного производства (металлопорошки, фотополимерные материалы, полимерные материалы и проч.)
	Электропроводные новые материалы (сверхпроводники, передовые магнитные материалы и проч.)
	Новые жаропрочные материалы (перспективные пенные материалы, высокотемпературные композиты, высокотемпературные сплавы и проч.)

Новые материалы	
Эффекты от внедрения	Новые биоматериалы
	Самовосстанавливающиеся материалы
	Суперсплавы
	Повышение устойчивости к внешним физическим, химическим и радиационным угрозам
	Улучшение показателей характеристик (легкость, высокая прочность, жаропрочность, коррозионно- и износоустойчивость, стойкостью к окислению, эффект памяти формы, тепловая изоляция)
	Увеличение диапазона рабочих температур
Средний уровень УГТ	Появление способности восстанавливать механические и геометрические свойства изделий
	Снижение стоимости готовой детали до 30% за счет исключения брака
Компании-разработчики/производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных сетевого журнала «Видеонаука», Ассоциации «Технет», 2016–2022 [190; 283]

Новые материалы являются одним из ключевых технологических направлений, способствующих обновлению существующих производств и формированию новых «умных производств», интегрированных с КФС. Глобальный мегатренд – разработка таких материалов, которые будут способны контролируемо изменять свои собственные характеристики и параметры под внешним воздействием. Применение новых материалов обеспечивает стабильный производственный результат и максимальное качество продукции. Отметим, что технологии новых материалов носят кросс-рыночный характер. В связи с этим они в разной степени могут быть применены в рамках всех высокотехнологичных рынков, в каждом отдельном имея определенную фокусировку.

Развитию рынка производства новых материалов в России способствуют мировые тенденции перехода к Индустрии 4.0, а также государственная политика в отношении импортозамещения зарубежных материалов. В качестве факторов, сдерживающих рост рынка новых материалов в России, можно выделить:

1. высокую стоимость производства и необходимого оборудования для создания новых материалов;
2. сложность запуска производства в промышленных масштабах;
3. токсичность множества композитных материалов;
4. монополизацию рынка производителями традиционных материалов (чугун, полиэтилен, сталь и проч.).

Уровень развития новых материалов варьируется от вида материала и технологии в основе, но в среднем российский уровень ощутимо ниже общемирового. В России на сегодняшний день некоторые новые материалы не производятся или производятся исключительно для научных целей.

Так, инновационный жаропрочный материал, как аэрогель, используется лишь в качестве основы или добавки в различные теплоизоляционные материалы («Almalen», «Ниагара») [284; 285]. В настоящий момент НИОКР на

тем самовосстанавливающихся материалов (полимеров) находится на стадии завершения, готовится запуск производства первой продукции [286].

При этом доля российских производителей сверхпроводников нового поколения составляет около 20% от мирового рынка [287]. Компании наращивают производственные мощности и успешно конкурируют с глобальными лидерами.

Аддитивные технологии

Одним из ключевых элементов Индустрии 4.0, концепции «умного производства» и, как следствие, – КФС, являются аддитивные технологии. Аддитивные технологии – это совокупность методов послойного наращивания и синтеза объекта с помощью компьютерных 3D технологий [288]. На сегодняшний день технологии аддитивного производства в большинстве случаев используются для изготовления трехмерного объекта путем добавления материала слой за слоем и/или путем его сплавления, напыления, затвердевания и проч. Исходная 3D-модель объекта проектируется в системах автоматизированного проектирования и заранее адаптируется под тип печатающего устройства с учетом свойств и характеристик материала, температуры внешней среды и желаемых характеристик конечной продукции.

Таблица 22. Аддитивные технологии

Аддитивные технологии	
Функции	3D-печать конечных объектов (конечных изделий)
	Изготовление пресс-форм
	Цифровое производство
	Прототипирование
Области применения	Строительство
	Сельскохозяйственная промышленность
	Машиностроение
	Судостроение
	Электронная промышленность
	Авиационная промышленность
	Аэрокосмическая отрасль
	Медицина, в том числе стоматология
	Фармацевтика
Технологии/ решения в основе	Энергетика
	Технология послойного построения изделия из расплавленной пластиковой нити (FDM)
	Технология лазерного сплавления металлического порошка (SLM)
	Технология инфузионного напыления материала (SLS)
	Лазерная стереолитография, отверждение жидкого фотополимерного материала под действием лазера (SLA)
	Технология затвердевания фотополимера с помощью цифровой светодиодной проекции (DLP)
Эффекты от внедрения	Технологии быстрого прототипирования (MJM, PolyJet, CJP)
	Улучшение свойств готовой продукции
	Экономия сырья
	Возможность изготовления изделий со сложной геометрией
	Мобильность производства
Средний уровень УГТ	Быстрая скорость обмена данными
	УГТ9 (по миру)
	УГТ7–9 (по России)

Аддитивные технологии	
Компании-разработчики/ производители (примеры)	

Источник: МГУ имени М.В.Ломоносова на основе данных MIT International Journal of Mechanical Engineering, Минпромторга России, Томского политехнического университета, 2016–2021 [102; 289; 290]

Внедрение аддитивных технологий в КФС путем автоматизации процессов настройки параметров печатающего устройства с помощью информационных технологий, в том числе Интернета вещей, методов искусственного интеллекта и проч., и обеспечения сравнения фактических и прогнозируемых результатов «умного» производства в режиме реального времени с меньшим вмешательством человека позволит повысить производительность и эффективность производства [291].

К глобальным трендам аддитивных технологий на 2022–2023 годы относятся:

1. переход к производству конечной продукции (при этом прототипирование по-прежнему остается основным вариантом использования 3D-печати);
2. разработку новых материалов;
3. повышение интегрированности специализированного ПО с иными технологическими и управленческими средствами (системы автоматизированного проектирования и проч.);
4. повышение экологичности аддитивных технологий.

В 2022 году Россия, несмотря на наличие на рынке готовых решений аддитивного производства, находится в высокой степени зависимости от зарубежных решений, и, как следствие, новых материалов. Одними из наиболее важных задач, решение которых может способствовать развитию отечественных разработок новых материалов и аддитивных технологий, являются [190]:

1. разработка базовых и специализированных национальных стандартов;
2. создание центров в сфере новых материалов и аддитивных технологий, а также утверждение системы сертификации на базе данных центров;
3. формирование программ подготовки и переподготовки кадров по направлению новых материалов и аддитивных технологий;
4. субсидирование и государственная поддержка проектов, направленных на развитие отечественных аддитивных технологий и новых материалов.

Совершенствование технологий машинного обучения, искусственный интеллект, Интернет вещей, цифрового моделирования способствует развитию новых материалов и аддитивного производства. Их использование позволяет повысить эффективность процессов прототипирования и создания конечной продукции с определенными заданными свойствами. Это может ускорить процесс перехода к Индустрии 4.0, а также положительным образом сказаться на степени внедрения КФС в производственные и технологические процессы предприятий, в том числе отечественных.

Приложение 7. Результаты библиометрического и патентного анализа

Таблица 23. Результаты библиометрического анализа. Публикации с наибольшим количеством цитирований (2006–2023 годы)

№	Наименование публикации	Авторы	Краткое описание	Год	Кол-во цитирований
Публикации иностранных научных организаций					
1	A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems	Lee, J., Bagheri, B., Kao, H.-A.	Предложено определение КФС, пригодной для эксплуатации на промышленных предприятиях. Описана 5ти-уровневая структура КФС: «умное» подключение, преобразование данных, центральный информационный «узел» системы, уровень преобразования машинных данных в человекочитаемый вид (графики, диаграммы и проч.), цифровые системы управления и самоуправления (системы контроля устойчивости, посредством которого реализуется корректировка работы всей КФС)	2015	2782
2	Cyber physical systems: Design challenges	Lee, E.A.	Представлено определение КФС. Описана проблематика создания и внедрения КФС, в том числе в части обеспечения безопасности используемых в КФС данных и надежности КФС в целом. Описано качественное отличие компонентов КФС от объектно-ориентированных программных компонентов. Рассмотрены проблемы проектирования КФС. Представлена новая концепция объединения физических и вычислительных компонентов, позволяющая реализовать весь потенциал КФС	2008	2335
3	A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications	Lin, J., Yu, W., Zhang, N., Zhang, H., Zhao, W. и другие	Исследована взаимосвязь между КФС и Интернетом вещей. Предложено интегрировать туманные/ граничные вычисления с Интернетом вещей с целью улучшения взаимодействия объектов сети и повышения устойчивости служб в случае сбоев. Предложено несколько способов интеграции Интернета вещей и туманных/ граничных вычислений с системами «умного» города и транспорта	2017	1568
4	Industry 4.0: A survey on technologies, applications and open	Lu, Y.	Проведен всесторонний обзор концепции Индустрии 4.0. Описаны взаимосвязи «умного» производства с технологиями КФС (Интернет вещей, информационно-коммуникационные технологии, системы управления технологическими процессами предприятия и проч.).	2017	1555

№	Наименование публикации	Авторы	Краткое описание	Год	Кол-во цитирований
	research issues		Проанализированы соответствующие предметной области научные работы, проведена их категоризация. Описаны проблемы и тенденции развития Индустрии 4.0		
5	Research directions for the internet of things	Stankovic, J.A.	Реализовано форсайт-исследование рынка решений Интернета вещей и влияния данной технологии на иные аспекты повсеместной цифровизации и интеллектуализации, в том числе на развитие КФС. Определены ключевые направления деятельности в рамках изучения технологии и разработки решений Интернета вещей	2014	1409
Публикации отечественных научных организаций					
1	The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	Ivanov, D., Dolgui, A., Sokolov, B.	Изучено влияние цифровизации и Индустрии 4.0 на процессы аналитики управления рисками в рамках организации цепочек поставок. Описаны перспективы и прогнозы развития КФС управления цепочками поставок	2019	608
2	A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0	Ivanov, D., Dolgui, A., Sokolov, B., Werner, F., Ivanova, M.	Предприятия Индустрии 4.0 на основе совместных КФС представляют собой новую форму промышленных сетей, цепочки поставок в которых будут иметь динамическую структуру, которая может изменяться с течением времени. В данной работе представлены динамическая модель и алгоритм краткосрочного планирования цепочки поставок на умных фабриках Индустрии 4.0. Проведен подробный теоретический анализ временной декомпозиции и вычислительной сложности предложенного метода. Исследованы условия оптимальности, а также структурные свойства модели и алгоритма	2016	356
3	Authentication in cloud-driven IoT-based big data environment:	Wazid, M., Das, A.K., Hussain, R., Succi, G., Rodrigues, J.J.P.C.	Описаны сетевые модели и внешние угрозы в разрезе схем аутентификации пользователей/ устройств в облачной среде на основе Интернета вещей, Больших данных и КФС. Определен блок нерешенных задач разработки специализированных протоколов безопасности в	2019	108

№	Наименование публикации	Авторы	Краткое описание	Год	Кол-во цитирований
	Survey and outlook		рамках организации работы Интернета вещей		
4	Trust management in a blockchain based fog computing platform with trustless smart oracles	Kochovski, P., Gec, S., Stankovski, V., Bajec, M., Drobintsev, P.D.	Обеспечение надежности и безопасности данных является важным аспектом реализации и эксплуатации КФС. В данной работе представлена архитектура управления доверием для DECENTER (платформа туманных вычислений, основным функционалом которой является поддержка Больших данных, в том числе данных, поступающих от устройств Интернета вещей, для последующего анализа), основанная на использовании смарт-контрактов, технологии блокчейн и проч.	2019	92
5	Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems	Challa, S., Das, A.K., Gope, P., Wu, F., Vasilakos, A.V. и другие	Проанализированы схемы аутентификации в облачных КФС. Разработаны новые схемы аутентификации: между пользователем и облачным сервером, между «умным» счетчиком и облачным сервером. Доказана эффективность и безопасность предложенных схем	2020	80

Источник: МГУ имени М.В.Ломоносова на основе данных библиографической и реферативной базы данных Scopus

Таблица 24. Результаты патентного анализа. Наиболее релевантные опубликованные патенты в сфере КФС (2006–2022 годы)

№	МПК	Авторы	Наименование патента	Краткое описание	Год
Патенты, признанные зарубежными патентными ведомствами					
1	C07D-263/32 C07D-417/06 C07D-417/14 G03G-015/00 G05B-019/418 G06F-011/14 G06F-015/177 G06F-030/20 G06F-030/27 H04L-029/08 H04L-041/084 H04L-041/0873	Siemens. Böhm Birthe	System and method for validating system requirements of cyber-physical systems	Изобретение представляет собой систему и метод проверки системных требований к КФС в группе систем. К ним относятся: создание цифрового двойника по меньшей мере для одной КФС, установление системных требований для каждой из КФС, хранение системных требований КФС прямо и/или косвенно в тех цифровых двойниках, которые соответственно закреплены за	2019

№	МПК	Авторы	Наименование патента	Краткое описание	Год
				КФС, установка связи между двумя или более цифровыми двойниками КФС и проч.	
2	G06F-008/41 G06F-011/34	Siemens. Elsner Christoph, Figalist Iris, Schultis Klaus- Benedikt	Method and computer-implemented tool for optimizing a cyber-physical system in terms of system artifacts and cyber-physical system	Для оптимизации КФС с точки зрения системных артефактов, предложен метод, включающий: мониторинг использования пользовательского интерфейса для сбора данных об использовании КФС, анализ данных об использовании КФС и данных об артефактах системы, поиск хотя бы одной оптимизации артефактов системы на основе анализа соответствующей информации о состоянии КФС, создание по крайней мере одного улучшенного артефакта на основе предполагаемой оптимизации, проверка работоспособности КФС с новыми вводными, формирование оптимизированной КФС на основе сборки улучшенного системного артефакта, развертывание оптимизированной КФС в операционной среде	2020
3	G06F-021/55 G06N-003/04 G06N-003/08 G06N-020/00 H04L-009/40 H04L-012/22	Battelle Memorial Institute. Edgar Thomas, Vrabie Draguna, Hofer William, Nowak Kathleen	High-fidelity model-driven deception platform for cyber-physical systems	Описана система защиты КФС от потенциального злоумышленника. Данная система включает в себя по меньшей мере один процессор, сконфигурированный для сбора исторической информации о КФС и обученный с применением методов машинного обучения для прогнозирования будущих состояний по меньшей мере одной части КФС. При обнаружении входного сигнала в КФС система конфигурируется для вывода предупреждения об атаке на КФС, указывающего на потенциальную киберугрозу	2018– 2022
4	H04L-009/40 H04L-029/06	Siemens. Schenk Tim,	Computer-implemented method and	Для выявления угроз КФС, в том числе киберугроз,	2021

№	МПК	Авторы	Наименование патента	Краткое описание	Год
	H04L-029/08	Botero Halblaub Andrés, Patzlaff Heiko, Obradovic Dragan, Knorn Steffi, Patel Abhi Himmatbhai	surveillance arrangement for identifying manipulations of cyber-physical-systems as well as computer-implemented-tool and cyber-physical-system	предложен метод их идентификации в режиме реального времени с целью предотвращения ущерба и изменения работы КФС. Данный метод актуален для КФС, введенных в эксплуатацию параллельно с цифровым двойником исследуемой КФС, что позволяет обнаружить отклонения в поведении КФС путем сравнения реальных параметров КФС с параметрами реплицированной модели и, таким образом, обнаружить источник отклонения, если оно превышает заданное пороговое значение	
5	G06F-008/41 G06F-011/36	Chungbuk National University Industry Academic Cooperation Foundation. HONG JangEui, YoonYou-Sang	System and method for writing interaction specification and for verifying safety of collaborating cyber-physical systems	Представлена система спецификации взаимодействия КФС и для проверки стабильности взаимодействия между ними. Система написания спецификации взаимодействия КФС и проверки стабильности взаимодействия между ними включает: модуль ввода модели анализа угроз для получения результатов анализа режима и последствий отказа каждой КФС, модуль ввода функциональной спецификации, модуль генерирования интегрированной спецификации для реализации взаимодействия нескольких КФС, модуль определения сценария и модуль выполнения сценария	2019
Патенты, признанные российским патентным ведомством					
1	C07D-263/32 C07D-417/06 C07D-417/14 G03G-015/00 G05B-019/418 G06F-011/14 G06F-015/177 G06F-030/20 G06F-030/27 H04L-029/08	Siemens. Böhm Birthe	System and method for validating system requirements of cyber-physical systems	Изобретение представляет собой систему и метод проверки системных требований к КФС в группе систем. К ним относятся: создание цифрового двойника по меньшей мере для одной КФС, установление системных требований для каждой из КФС, хранение системных требований КФС	2019

№	МПК	Авторы	Наименование патента	Краткое описание	Год
	H04L-041/084 H04L-041/0873			прямо и/ или косвенно в тех цифровых двойниках, которые соответственно закреплены за КФС, установка связи между двумя или более цифровыми двойниками КФС и проч.	
2	G06F-011/00 G06F-011/07 G06F-016/901 G06F-021/00 G06N-003/08	АО «Лаборатория Касперского». Лаврентьев Андрей, Воронцов Артем, Филонов Павел, Шалыга Дмитрий, Шкулев Вячеслав, Демидов Николай, Иванов Дмитрий	System and method of generating data for monitoring of a cyber-physical system for early determination of anomalies	Представлены системы и способы раннего определения аномалий в работе КФС с использованием графического пользовательского интерфейса, включая: методы получения информации об одном или нескольких параметрах КФС, получения информации о периоде времени наблюдения за одним или несколькими параметрами, создания прогноза значений одного или нескольких параметров КФС. Реализован вывод информации в графическом пользовательском интерфейсе, о том, что найденная аномалия превышает заданные пороговые значения и идентифицируется как ошибка	2018
3	G06F-011/00 G06F-011/07 G06F-011/34 G06F-021/50 G06K-009/62 G06N-020/00	АО «Лаборатория Касперского». Лаврентьев Андрей, Воронцов Артем, Филонов Павел, Шалыга Дмитрий, Шкулев Вячеслав, Демидов Николай, Иванов Дмитрий	System and method for detecting anomalies in cyber-physical system with determined characteristics	Представлены система и метод определения источника аномалии в КФС. Разработанный инструмент идентификации аномалий может определять ошибку прогноза для множества параметров КФС, а также идентифицировать аномалию тогда, когда «общая» ошибка прогноза превышает пороговое значение и идентификация по меньшей мере одного параметра КФС как основного источника аномалии становится возможной	2018
4	B60R-025/04 B60R-025/24 G06F-021/55 G06F-021/57	АО «Лаборатория Касперского». Зорин Сергей,	System and method for controlling access to a cyber-physical system	Разработан инструмент контроля безопасности в момент авторизации пользователей в системе. В системе	2019

№	МПК	Авторы	Наименование патента	Краткое описание	Год
	H04L-029/06	Шадрин Александр		реализуется мониторинг сообщений, отправленных через КФС для подтверждения санкционированного доступа к системе, и фиксируются «фиктивные» отправленные данные для входа. Инструмент контроля доступа может обнаружить изменение в функциональном модуле КФС, связанное с несанкционированным доступом к КФС, и изменить его состояние/ правила мониторинга	
5	G06F-011/30 G06F-021/00	АО «Лаборатория Касперского». Лаврентьев Андрей, Воронцов Артем, Филонов Павел, Шалыга Дмитрий, Шкулев Вячеслав, Демидов Николай, Иванов Дмитрий	Способ определения источников аномалии в киберфизической системе	Изобретение относится к способу и системе определения источников аномалии в КФС. Технический результат заключается в определении источников аномалии в КФС. С помощью средств прогнозирования и определения аномалий может быть определен по меньшей мере один признак КФС, являющийся источником аномалии, если вклад ошибки прогноза упомянутого по меньшей мере одного признака КФС в общую ошибку прогноза выше, чем вклад по меньшей мере одного другого признака КФС в общую ошибку прогноза	2020

Источник: МГУ имени М.В.Ломоносова на основе данных международной патентной базы данных Questel Orbit

Приложение 8. Описание продуктов и услуг по отдельному направлению НТИ

Таблица 25. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части робототехнического оборудования и устройств

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	ООО «Промобот»	Робот для исполнения операций: Robo-C и Promobot V.4	Сервисный робот для бизнеса	Робот автоматизировано перемещается по помещению, консультирует посетителей, воспринимая их речь и вопросы [292; 293]
2	ООО «МАКРОСОЛЮШНС»	Многофункциональный роботизированный комплекс	Производство электроники и приборостроение	Робототехнический комплекс при помощи сервоприводных манипуляторов осуществляет перемещение в пространстве и ряд операций: укладка, нанесение лазерной маркировки, формирование проводящего рисунка, сверление, лазерная резка, нанесение лакировки, сборка корпусов, установка крепежа, DIP-пайка, визуальный контроль требуемых параметров [294]
3	ООО «ГОРНЫЙ-ЦОТ»	Система контроля запыленности	Оперативный контроль запыленности воздуха, дисперсионного состава, параметров атмосферы и вычисление количества отложившейся пыли	Принцип действия системы основан на регистрации рассеянного ИК-излучения частиц, попадающих в пространство измерительной камеры. Регистрация рассеянного излучения осуществляется кремниевым фотоприемником, после чего полученные данные анализируются и на основе них включается обдув помещения при помощи вентилятора, осуществляющего вентиляцию через фильтр очистки воздуха [295]
4	ООО «ИНСПАИР»	Робот для исполнения процессов на производстве	Автоматизация процесса нанесения этикеток и контроля геометрических параметров рулонов биаксиально-ориентированной полипропиленовой пленки	Робот осуществляет манипулирование мелкими деталями, продукцией и инструментами на производстве при помощи антропоморфных манипуляторов [296]

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
5	ООО «НЬЮ ЛАЙН ИНЖИНИРИНГ»	Роботизированная линия термообработки деталей	Автоматизация управления линиями термообработки	По линии осуществляется перемещение детали. По очереди деталь попадает в камеры промышленных установок, в которых она закаляется, охлаждается и передается на следующий вид обработки, после чего попадает на стол-накопитель для обработанных деталей [297]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Таблица 26. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части средств сбора и / или обработки информации из внешней среды

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	ООО «ВИДЕОМАТ-РИКС»	ПО контроля процессов по видео (искусственный интеллект)	Контроль качества технологического процесса и сокращение издержек за счет уменьшения времени простоя оборудования и оперативного реагирования на нештатные ситуации в узлах технологического процесса	Система получает изображение с видеокамеры и на основе технологии искусственного интеллекта и машинного зрения выявляет характерные инциденты, подсвечивая их на системе мониторов ответственным за безопасность сотрудникам. Также на основании видео отслеживается наличие брака в продукции. В случае обнаружения брака система может остановить конвейер или подать звуковой сигнал ответственному работнику [298]
2	ООО «НВИАЙ СОЛЮШЕНС»	Система распознавания данных на основе искусственного интеллекта	Распознавание документов, QR-кодов и карт в видеопотоке	Система использует методы компьютерного зрения для автоматизированного получения данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени [299]
3	ООО «НИЛАР»	Система локального позиционирования	Выявление угроз и инцидентов, связанных с исполнением требований техники	По периметру рабочей области устанавливаются сверхширокополосные

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
			безопасности производственных предприятий и объектов критической инфраструктуры	радиомаяки. В бортовой компьютер робота устанавливается приемник и навигационное ПО, позволяющее свободно работать сотрудникам в помещении и снаружи [300]
4	ООО «ПАВЛИН ТЕХНО»	Система автоматизированной дефектоскопии на производстве	Поиск дефектов на продукции на конвейерном производстве	Устройство на основании методов машинного зрения анализирует продукцию и выявляет дефекты, сигнализируя о них и / или останавливая конвейер [301]
5	ООО «ЦАПК»	Автоматизированная система инвентаризации	Автоматизация и сокращение временных издержек при инвентаризации	Устройство с датчиками устанавливается на форклифт или рич-трак и собирает данные о паллетах с продукцией на складе. Информация автоматически заносится в базу данных в режиме реального времени. Основные параметры мониторинга при сканировании: заполненность паллетоместа, высота паллета, штрихкоды продукции и другие [302]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Таблица 27. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных продуктов компаний НТИ в части технологий проектирования и моделирования

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	ООО «ЭТТОН ГРУП»	Цифровой двойник	Моделирование производственных ситуаций, тестирование параметров эксплуатации в сферах добычи и переработки полезных ископаемых, медицине, образовании, ритейле, сельском хозяйстве, спорте, строительстве, транспорте и логистике, энергетике	На основе технологий виртуальной реальности и специального ПО система создает цифровой двойник предприятия / объекта / системы, после чего осуществляет имитационное моделирование с целью прогнозирования [303]
2	ООО «ЭТТОН ГРУП»	Система предиктивной аналитики	Сокращение расходов на замену или ремонт	Система осуществляет предиктивную аналитику

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
		ремонта	оборудования, а также повышение производительного времени работы на нефтегазодобывающем объекте	состояния нефтегазового комплекса при помощи технологий искусственного интеллекта, собирая данные о состоянии оборудования [304]
3	АО «ТЕРРА ТЕХ»	Система создания цифровой копии объектов и территорий в 3D	Создания точной цифровой копии объектов и территорий Земли в 3D-формате	Система работает на основе данных дистанционного зондирования Земли, далее методами пространственного анализа создаются цифровые модели местности и рельефа, ортофотопланы и 3D-модели объектов и территорий в различных форматах (obj, 3ds, vrml, dxf, collada, pdf) [305]
4	ООО «ВИДЕОМАТ-РИКС»	Система конвейерного отслеживания продукта	Повышение качества контроля на производстве и упрощение учета продуктов и сырья, повышение уровня экономической безопасности	Система прослеживает путь каждого продукта от начала до конца жизненного цикла на производстве. В базу данных автоматически записываются время, место и действия с изделием, такие как: снятие, установка или модификация. Записанные данные содержат стоп-кадр с камеры, если в этот момент зафиксировано нарушение. Система ведет учет, сколько изделий с производственной линии дошло до склада, а сколько нет. В случае выявления брака собранные данные позволяют выявить причину его возникновения [306]
5	ООО ИЦ «СТАНКО-СЕРВИС»	Система контроля работы и энергоэффективности промышленного оборудования	Непрерывный мониторинг и контроль промышленного оборудования	Система осуществляет мониторинг работы оборудования станков с ЧПУ и универсального оборудования, выполняет анализ и классификацию причин простоя оборудования, ведет контроль

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
				энергопотребления оборудования, информирует цеховые службы предприятия о простое оборудования, формирует отчеты [307]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Таблица 28. Перечень и описание продукции компаний НТИ в части систем Интернета вещей

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	ООО «ИНТЕЛЛИДЖЕНТ АЙДИАС»	Цифровой шлем для удаленной технической поддержки	Оказание удаленной технической поддержки по настройке, тестированию и оценке производительности оборудования	VR / AR гарнитура на удаленном техническом специалисте с помощью пространственных камер у конечного клиента создает визуальное 3D пространство для более удобной работы специалиста с оборудованием [308]
2	ООО «ИРИДИУМ»	Система автоматизации домов и прочих зданий	Управление системами «Умный дом» с помощью интуитивно понятного интерфейса	Система собирает данные о статусе устройств «Умный дом» и осуществляет управление их работой (освещение, бытовая техника, системы кондиционирования и т.д.) при помощи мобильного приложения [309]
3	ООО «МГБОТ»	Набор «Умная теплица ЙоТик М2»	Творческий набор для выращивания растений и обучения работы с технологиями интернета вещей	На основе датчиков интернета вещей, включенных в набор, осуществляется сбор данных о макете теплицы. Данные с датчиков поступают в хаб, также включенный в набор, и проходят процесс вычислительной обработки, после чего на устройства полива и освещения могут подаваться сигналы о начале работы [310]
4	ООО «НЕОХОУМ»	«Умный холодильник»	Первый в России «Умный холодильник»	В холодильник внедрен электронный блок с выходом в Интернет через WiFi. Помимо сбора телеметрической информации

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
				о состоянии самого холодильника, осуществляется анализ использования холодильника (продукции внутри) для целей экономики и анализа пищевых привычек [311]
5	ООО «СОФТ М»	Система управления генерацией и распределением тепловой энергии «Аврора»	Управление генерацией и распределением тепловой энергии с обеспечением наибольшего КПД и наименьших потерь	В рамках системы посредством сети датчиков и устройств интернета вещей собираются данные о генерации тепловой энергии и ее распределении в здании. Далее полученные данные обрабатываются классическими методами, в том числе с помощью искусственного интеллекта, после чего могут активироваться другие устройства или осуществляться диспетчерское управление. Система также может учитывать финансовые затраты и счета оплаты энергии [219]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Таблица 29. Перечень и описание продукции компаний НТИ в части облачных вычислений

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	АО «ИНФОВОТЧ»	Система предотвращения утечек информации и контроля информационных потоков	DLP-система для предотвращения утечек конфиденциальной информации, повышения уровня автоматизации работы систем информационной безопасности	Система осуществляет контроль каналов передачи данных и проверяет исходящую информацию, в том числе текстовые и графические объекты, на предмет конфиденциальности, вычисляя утечку данных даже в случае видоизменения / маркировки исходящих данных [312]
2	АО «ИНФОВОТЧ»	Промышленный межсетевой экран	Предотвращение утечек информации в промышленных сетях и контроль информационных потоков	Система осуществляет контроль действий пользователей, ограничивает промышленный трафик на

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
				уровне отдельных промышленных протоколов и контролирует недопустимые операции с программируемым логистическим контроллером [313]
3	АО «ИНФОВОТЧ»	Система выявления нелояльных сотрудников InfoWatch Employee Monitoring	Мониторинг эффективности работы персонала и выявление рисков в действиях сотрудников	Система осуществляет анализ цифрового следа сотрудников для выявления утечек конфиденциальной информации и фиксирует факт присутствия сотрудников на рабочем месте и время, проведенное за работой. Система формирует картину действий каждого сотрудника, записывая изображения экрана и звуки с микрофона и динамиков, осуществляя мониторинг мессенджеров и почтовых ящиков, фиксируя операции с документами, анализирует полученные данные и предотвращает утечку конфиденциальных данных из организации, блокируя определенные действия сотрудника [220]
4	ООО «АЛАН-ИТ»	Сервис бизнес-аналитики	Построение прогнозов для повышения экономической эффективности деятельности компании	Сервис собирает данные о потреблении электроэнергии из таких источников, как счетчики интернета вещей, метеорологические сводки, ГИС ЖКХ, открытые данные регионального правительства, выстраивает исторические тренды и составляет прогнозные экстраполяции в режиме реального времени. За счет автоматизации коммерческого учета энергии, сбора и хранения данных система выявляет хищения электроэнергии

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
				и расхождения по плану / факту потребления [314]
5	ООО «СИСОРТ»	Система мониторинга и управления работой сети фотосепараторов	Мониторинг и управление работой сети фотосепараторов	Система собирает данные онлайн о технических параметрах фотосепараторов и параметрах сортировки, обновляет ПО и рецепты сортировки [315]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Таблица 30. Перечень и описание продукции компаний НТИ в части Больших данных

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
1	ООО «7ТЕК»	Система проактивного мониторинга бизнес-сервисов	Оперативное определение, предупреждение и устранение инцидентов	Система накапливает данные, анализирует их, заранее оповещает о возможных сбоях и реагирует на них, используя стек технологий Zabbix, Prometheus, GrayLog и Grafana [316]
2	ООО «ЭТТОН ГРУП»	ПО автоматизации управления жизненным циклом продукции	Автоматизация отслеживания и управления жизненным циклом продукции, объединение всех участников снабжения и производства в единой системе	Система определяет время и место изготовления оборудования и его комплектующих с помощью сканирования установленной на него метки, что, в том числе, позволяет свести к минимуму количество готовых изделий, подлежащих ремонту [317]
3	ООО «КВАНТОР»	«Умная» система контроля телеметрии грузовых автомобилей и автобусов	Мониторинг текущего состояния автомобиля, дистанционный анализ неисправностей, сигнал к проведению своевременной профилактики транспортного средства	Приложение осуществляет сбор и анализ около 200 технических параметров транспортного средства, предоставляет наглядные графики и гибкую систему отчетов, связь с водителем прямо из приложения, настраиваемые уведомления пользователя [318]
4	ООО «САТЕЛ ПРО»	Система мониторинга и предиктивного анализа работы оборудования промышленных объектов с	Мониторинг состояния промышленных объектов в режиме реального времени для раннего выявления возможных аварий и других негативных событий	Система собирает данные с множества объектов посредством сети промышленного интернета вещей. Большие данные обрабатываются на локальном

№	Наименование компании	Наименование продукции	Назначение продукции	Механизм работы продукции
		использованием технологий интернета вещей		вычислительном сервере, на основе проведенной аналитики могут активироваться другие устройства для регулировки деятельности предприятия [319]
5	ООО «АУРА 365»	Комплексная инфраструктурная цифровая платформа для беспроводного автоматизированного контроля и учета коммунальных ресурсов	Обеспечение передачи данных для контроля и учета коммунальных ресурсов	Осуществляет прием данных от различных приборов учета (электричества, воды, газа, тепла) и датчиков (протечки, давления, температуры, контроля доступа и т.д.), а также передает на них команды управления (отключение / включение реле электросчетчика, запрос текущих показаний счетчика) и другую служебную информацию. Работает на расстоянии от 300 м до 1 км в зависимости от рельефа местности и плотности застройки, работает в частотном диапазоне 868,7–869,2 МГц [320]

Источник: МГУ имени М.В.Ломоносова, 2022 год

Приложение 9. Реализуемые проекты по отдельному направлению НТИ

Таблица 31. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части робототехнического оборудования и устройств

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «НТК «МОРО-БОТСИСТЕМ»	Морская безэкипажная платформа	7	Сбор и передача данных в морской среде для промышленного, экологического мониторинга, поиска биоресурсов, проведения геофизических исследований в транзитных зонах и т.п.	Платформа находится в открытых водных пространствах и при помощи установленных на нее датчиков осуществляет сбор данных. Также возможна установка прочих устройств на платформу для реализации необходимых сценариев. Генерация энергии для перемещения, сбора и обмена данными происходит с помощью систем солнечных панелей и ветрогенераторов [242]
2	ООО «ЦР»	Безлюдные технологии транспортировки и добычи руды	7	Транспортировка и добыча руды	На шахтный локомотив устанавливается оборудование для его дистанционного управления (системы связи, микропроцессорные системы управления), затем посредством дистанционного управления осуществляются операции по добыче и транспортировке руды [321]
3	ООО «НИИ УРАЛ-МЕТ»	Разработка семейства ветроэнергетических установок, а также интеллектуальной системы управления к ним	7	Генерация электричества из возобновляемых источников энергии и автоматизация управления этими источниками	Традиционные ветро- и солнечные генераторы электроэнергии мощностью до 100кВт управляются интеллектуальной системой на основе технологий сенсорики и Искусственного интеллекта для достижения наиболее эффективных результатов [322]
4	ООО «ОБРАЗОВАТЕЛЬНАЯ РОБОТОТЕХНИКА»	Роботизированная ячейка по финишной полировке (адаптивная)	5	Автоматизированная финишная полировка деталей	Роботизированная рука осуществляет управление полировочной установкой, осуществляя контакт с деталью и обрабатывая

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
					ее до нужного состояния [323]
5	АО «НПО «АНДРОИДНАЯ ТЕХНИКА»	Комплекс антропоморфных робототехнических устройств	5	Автоматизация циклических производственных процессов при взаимодействии с человеком в пределах рабочего пространства	Робот состоит из манипуляторного модуля, захватного модуля, блока управления и комплекта ПО. Используя технологии искусственного интеллекта, робот анализирует окружающее пространство и выполняет такие операции, как обслуживание и ремонт станков, сборка и сортировка товаров и т.д. [324]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

Таблица 32. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части средств сбора и / или обработки информации из внешней среды

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «А1»	Автоматизированное измерение температуры людей в потоке	8	Повышение общественной безопасности путем выявления людей с повышенной температурой	Прибор измеряет температуру тела каждого человека в потоке благодаря инфракрасной камере и определяет повышена ли она, издает звуковой сигнал при выявлении установленных факторов. Также прибор определяет в каком месте на теле человека находится запрещенный к проносу металлический предмет на основе использования комплектов датчиков [325]
2	ООО «ДИАМАНТ»	Нейтронный анализатор сырья конвейера	8	Контроль качества сырья, управление потоками, сортировка, управление расходом сырьевых компонентов и осуществление управляющего воздействия	Анализатор в режиме реального времени с помощью потока нейтронов собирает и анализирует данные об элементном состоянии сырья, идущего по конвейеру, на основе чего может

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
					осуществлять управление потоком (сортировка, изменение расхода сырьевых компонентов и т.п.) [326]
3	ООО «ПАВЛИН ТЕХНО»	Автономный гаджет видео-аналитики	8	Сбор данных для проведения маркетинговых исследований и повышения эффективности бизнеса	Система подсчитывает количество посетителей в магазинах, торговых, выставочных центрах и других местах массового скопления людей посредством технологии машинного зрения [327]
4	ООО «ПАВЛИН ТЕХНО»	Система контроля дыхания при лучевых процедурах пациента	8	Повышение эффективности конусно-лучевой терапии во время дыхания пациента	Система посредством обработки сигналов с ультразвуковых сканеров отслеживает дыхание пациента и определяет, в какой момент можно проводить облучение пациента в наиболее удобном положении [327]
5	ООО «ИНТЭК»	Биометрический браслет	6	Отслеживание биометрических показателей жизни, а также определение физиологического состояния человека (стресс, сердечные отклонения и т.п.)	Устройство измеряет пульс, температуру, определяет падения с помощью акселератора и при помощи телекоммуникационного модуля осуществляет сбор и передачу информации о состоянии пользователя посредством мобильного интернета. В случае экстренной ситуации информация о пользователе и его местонахождении направляется родственникам / врачам / экстренным службам и т.д. [328]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

Таблица 33. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов

компаний НТИ в части технологий проектирования и моделирования

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «НМТ»	Аппаратно-программный комплекс управления судами	8	Автоматизация управления судовыми системами	Сервис осуществляет аналитику и прокладывание маршрута, исходя из статистических и прогнозируемых расчетов на основе нейронных сетей, метеорологической ситуации на маршруте следования, а также ведение статистической отчетности состояния судна на всем пути следования [329]
2	АО «ФЭСКОМ»	Программный комплекс для мониторинга, диагностики, прогнозирования, управления работой электротехнического оборудования и систем электропитания оборудования (объектов)	6	Мониторинг, диагностика, прогнозирование, управление работой электротехнического оборудования и систем электропитания оборудования	Система содержит интегрированный пакет инструментов для создания и внедрения цифровых технологий в управление электротехническим оборудованием в различных инфраструктурах. В набор инструментов включено ПО, позволяющее автоматизировать такие функции, как конструирование приложений, обработка Больших данных, интеллектуальное управление распределенными энергетическими ресурсами, управление ролевой моделью и т.д. [330]
3	ООО «ГАР-ПИКС»	Система проектирования и мониторинга электрооборудования	6	Проектирование электрооборудования, обеспечивающего оптимальные параметры энергосистем	Система рассчитывает оптимальные параметры энергосистем, используя методы имитационного моделирования, в том числе с помощью цифровых двойников и физических цепей [331]
4	ООО «ЭТТОН ГРУП»	АИС «Месторождение»	6	Автоматизация бизнес-процессов на месторождении, включая автоматизацию контроля проведения и учета результатов интерпретации исследований	Система собирает данные с множества датчиков и других систем учета, агрегирует их, обрабатывает и может совершать ряд установленных действий на основании полученных результатов [332]
5	ПАО «ОДК-САТУРН»	Умная фабрика – испытательный полигон для создания промышленного предприятия в рамках	6	Автоматизация процессов управления производственными предприятиями (автоматизация проектирования и	Модель фабрики представляет собой совокупность элементов (производственного оборудования, цифровых технологий, кадров), объединенных в единую цифровую сеть на базе

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
		Индустрии 4.0		моделирования изделий, управления оборудованием, инфраструктурой и процессами, развития человеческого капитала)	технологий цифровых двойников, что позволяет осуществлять непрерывный контроль за всеми процессами, управлять ими в режиме реального времени, корректировать производственные нагрузки на основе аналитики данных [233]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

Таблица 34. Перечень и описание наиболее релевантных, высокотехнологичных и востребованных проектов компаний НТИ в части систем Интернета вещей

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «СЕРВИССОФТ ИНЖИНИРИНГ»	ПАК сбора и обработки данных об объектах	8	Обработка данных от территориально распределенного промышленного оборудования	Промышленное оборудование при помощи промышленных сенсоров собирает набор данных и отправляет их по сети промышленного интернета в общий центр обработки данных. Полученные данные обрабатываются искусственным интеллектом, на основе этих данных формируется аналитика и могут активироваться другие устройства [333]
2	ООО «СЛУЖБА МОНИТОРИНГА. ТЮМЕНЬ»	Система контроля работы инженерного оборудования	8	Противопожарная система снижения влияния человеческого фактора при эксплуатации инженерного оборудования	Система при помощи набора датчиков Интернета вещей собирает всевозможные данные об объекте и контролирует работоспособность всех систем, в том числе систему вентиляции, водоснабжения и противопожарную систему. В случае необходимости система направляет вызов инженерам [334]
3	ООО «НЕОХОУМ»	Мониторинг холодильного оборудования («умный»)	8	Онлайн мониторинг температур в технике и помещениях	Система при помощи датчиков Интернета вещей осуществляет контроль температуры в помещении. При необходимости датчиками Интернета

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
					вещей оснащаются устройства (например, сервера). В целях поддержания необходимой температуры система может регулировать работу холодильного оборудования, увеличивая или уменьшая интенсивность его охлаждения [311]
4	ООО «МОДУЛЬНЫЕ СИСТЕМЫ ТОРНАДО»	Архитектура Доверенной Открытой Распределенной Системы Управления на основе Промышленного Интернета (ДОРСУ-ПИ)	6	Управление устройствами промышленного интернета	Система включает проектно-масштабируемый мультипроцессорный суперкомпьютер, который получает и отправляет данные по сети Ethernet, осуществляя управление устройствами промышленного интернета [335]
5	ООО «ДИЛИБРИУМ»	ПАК для выращивания ценных пород рыб	2	Автоматизация производства по выращиванию ценных пород рыб в установках замкнутого водоснабжения	Система включает в себя комплекс технологических решений в виде датчиков контроля параметров искусственной среды обитания гидробионтов и управляющего ПО с алгоритмами машинного обучения, на основании чего системой осуществляются определенные действия (регулировка освещения, температуры, подача корма и т.д.) для наиболее эффективного выращивания рыбы [336]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

Таблица 35. Описание проекта компании НТИ в части облачных вычислений

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «ИНТЭК»	Автоматизированная система видеонаблюдения высокого разрешения	4	Повышение автономности систем видеонаблюдения	В камеры системы видеонаблюдения встроена высокопроизводительная система, позволяющая проводить вычисления непосредственно на камере, что снижает требования к пропускной способности

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
					сети и мощности серверов обработки данных [239]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

Таблица 36. Описание проекта компании НТИ в части Больших данных

№	Наименование компании	Наименование проекта	УГТ	Назначение проекта	Механизм работы устройства в проекте
1	ООО «7ТЕК»	Цифровая платформа трейсинга алмазов	5	Подтверждение факты добычи алмазов на месторождениях	В открытых источниках отсутствуют данные, позволяющие сделать какой-либо вывод о механизме работы устройства в составе данного проекта [241]

Источник: МГУ имени М.В.Ломоносова по материалам реестра «НТИ 1000», 2022 год

БИБЛИОГРАФИЯ

1. Scopus - Document search | Signed in [Электронный ресурс]. – URL: <https://www.scopus.com/search/form.uri?display=basic#basic> (дата обращения: 22.12.2022).
2. Lee J. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems / J. Lee, B. Bagheri, H.-A. Kao // Manufacturing Letters. – 2015. – Vol. 3. – P. 18-23.
3. ChatGPT: Optimizing Language Models for Dialogue [Электронный ресурс]. – URL: <https://openai.com/blog/chatgpt/> (дата обращения: 27.12.2022).
4. Editor C.C. cyber-physical system(s) - Glossary | CSRC [Электронный ресурс]. – URL: https://csrc.nist.gov/glossary/term/cyber_physical_systems (дата обращения: 22.12.2022).
5. Cyber-Physical Systems and Internet of Things / C. Greer [et al.] // NIST. – 2019.
6. The 12 Flavors of Cyberphysical Systems | IEEE Journals & Magazine | IEEE Xplore [Электронный ресурс]. – URL: <https://ieeexplore.ieee.org/document/9622310> (дата обращения: 12.12.2022).
7. Тематическое моделирование с использованием эмбедингов BERT [Электронный ресурс] : NewTechAudit / Хабр. – 2022. – URL: <https://habr.com/ru/post/653443/> (дата обращения: 06.07.2022).
8. Дорожная карта «Технет 4.0» [Электронный ресурс]. – URL: https://technet-nti.ru/article/roadmap_new (дата обращения: 28.12.2022).
9. Digital Twins and Cyber-Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison / F. Tao [et al.] // Engineering. – 2019. – Vol. 5. – Digital Twins and Cyber-Physical Systems toward Smart Manufacturing and Industry 4.0. – № 4. – P. 653-661.
10. Itd R. and M. Cyber-Physical Systems Market Size, Market Share, Application Analysis, Regional Outlook, Growth Trends, Key Players, Competitive Strategies and Forecasts, 2021 To 2029 [Электронный ресурс]. – URL: <https://www.researchandmarkets.com/reports/5614637/cyber-physical-systems-market-size-market-share> (дата обращения: 19.12.2022).
11. Cyber-Physical System Market [Электронный ресурс]. – URL: <https://www.futuremarketinsights.com/reports/cyber-physical-systems-market> (дата обращения: 19.12.2022).
12. Industrial Robots Market Size, Share & Growth Report [2029] [Электронный ресурс]. – URL: <https://www.fortunebusinessinsights.com/industry-reports/industrial-robots-market-100360> (дата обращения: 22.12.2022).
13. Industrial Robotics Market Share, Growth, Forecast by 2030 [Электронный ресурс]. – URL: <https://www.alliedmarketresearch.com/industrial-robotics-market> (дата обращения: 21.12.2022).
14. Industrial Sensors Market Size, Share, Trends and Industry Analysis 2022 - 2030 [Электронный ресурс]. – URL: <https://www.marketsandmarkets.com/Market-Reports/industrial-sensor-market-108042398.html> (дата обращения: 22.12.2022).
15. Industrial IoT Market Size To Surpass USD 1742.8 Bn By 2030 [Электронный ресурс]. – URL: <https://www.precedenceresearch.com/industrial-iot-market> (дата обращения: 21.12.2022).
16. Markets R. and. Global CAD Software Market (2020 to 2030) - by Technology, Model, Deployment, Level and Application [Электронный ресурс]. – URL: <https://www.globenewswire.com/news-release/2020/11/19/2130084/28124/en/Global-CAD-Software-Market-2020-to-2030-by-Technology-Model-Deployment-Level-and-Application.html> (дата обращения: 29.12.2022).
17. Robotics Technology Market Size, Trends, Growth, Report 2030 [Электронный ресурс]. – URL: <https://www.precedenceresearch.com/robotics-technology-market> (дата обращения: 21.12.2022).
18. Itd R. and M. Computer Aided Engineering (CAE) - Global Market Trajectory & Analytics [Электронный ресурс]. – URL: <https://www.researchandmarkets.com/reports/5139748/computer-aided-engineering-cae-global-market> (дата обращения: 22.12.2022).
19. Hype Cycle for the Internet of Things, 2017 [Электронный ресурс]. – URL: https://www.gartner.com/resources/314200/314298/314298_0001.gif (дата обращения: 28.12.2022).

20. Hype Cycle for the Internet of Things, 2019 [Электронный ресурс]. – URL: <https://www.gartner.com/en/documents/3947474> (дата обращения: 07.12.2022).
21. PricewaterhouseCoopers. Digital Factory Transformation Survey 2022 [Электронный ресурс]. – URL: <https://www.pwc.de/en/strategy-organisation-processes-systems/operations/digital-factory-transformation-survey-2022.html> (дата обращения: 25.12.2022).
22. Sedik T.S. Pandemics and Automation: Will the Lost Jobs Come Back? [Электронный ресурс]. – URL: <https://www.imf.org/en/Publications/WP/Issues/2021/01/15/Pandemics-and-Automation-Will-the-Lost-Jobs-Come-Back-50000> (дата обращения: 25.12.2022).
23. 10 IoT technology trends to watch in 2022. – 2022.
24. Worldwide CAD Trends 2022 in Manufacturing Survey Results [Электронный ресурс]. – URL: https://business-advantage.com/landing_page_CAD_Trends_2022_MFG.php (дата обращения: 26.12.2022).
25. Jay A. 11 Big Data Trends for 2022/2023: Current Predictions You Should Know [Электронный ресурс]. – URL: <https://financesonline.com/big-data-trends/> (дата обращения: 25.12.2022).
26. The State of Industrial Robotics: Emerging Technologies, Challenges, and Key Research Directions [Электронный ресурс]. – URL: <https://workofthefuture.mit.edu/research-post/the-state-of-industrial-robotics-emerging-technologies-challenges-and-key-research-directions/> (дата обращения: 25.12.2022).
27. Больше всего роботов в России покупает автопром [Электронный ресурс]. – URL: <https://www.vedomosti.ru/technology/articles/2019/09/19/811579-bolshe-vsego-robot> (дата обращения: 26.12.2022).
28. Big Data Market Share, Size, Trends – [2021-2026] [Электронный ресурс]. – URL: <https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html> (дата обращения: 14.12.2022).
29. Cyber-Physical Systems (CPS) [Электронный ресурс]. – URL: <https://beta.nsf.gov/funding/opportunities/cyber-physical-systems-cps> (дата обращения: 27.12.2022).
30. The Cyber-Physical Systems Virtual Organization | CPS-VO [Электронный ресурс]. – URL: <https://cps-vo.org/> (дата обращения: 27.12.2022).
31. Cyber-Physical Systems (CPS) (nsf21551) | NSF - National Science Foundation [Электронный ресурс]. – URL: <https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm> (дата обращения: 27.12.2022).
32. Science and Technology Directorate | Homeland Security [Электронный ресурс]. – URL: <https://www.dhs.gov/science-and-technology> (дата обращения: 27.12.2022).
33. CPSSEC | Homeland Security [Электронный ресурс]. – URL: <https://www.dhs.gov/science-and-technology/cpssec> (дата обращения: 27.12.2022).
34. Federal Highway Administration [Электронный ресурс]. – URL: <https://highways.dot.gov/> (дата обращения: 27.12.2022).
35. National Institutes of Health (NIH) [Электронный ресурс]. – URL: <https://www.nih.gov/> (дата обращения: 27.12.2022).
36. National Institute of Biomedical Imaging and Bioengineering | [Электронный ресурс]. – URL: <https://www.nibib.nih.gov/> (дата обращения: 27.12.2022).
37. Comprehensive Cancer Information - NCI [Электронный ресурс] : cgvHomeLanding. – URL: <https://www.cancer.gov/> (дата обращения: 27.12.2022).
38. Office of Behavioral and Social Sciences Research [Электронный ресурс]. – URL: <https://obssr.od.nih.gov/> (дата обращения: 27.12.2022).
39. National Center for Advancing Translational Sciences | [Электронный ресурс]. – URL: <https://ncats.nih.gov/> (дата обращения: 27.12.2022).
40. Cyber-Physical Systems (CPS) (Joint NSF) Competitive Grants Program [Электронный ресурс]. – URL: <http://www.nifa.usda.gov/grants/funding-opportunities/cyber-physical-systems-cps-joint-nsf-competitive-grants-program> (дата обращения: 27.12.2022).

41. Horizon Europe [Электронный ресурс]. – URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (дата обращения: 27.12.2022).
42. DIGITAL INNOVATION HUBS AND COLLABORATIVE PLATFORM FOR CYBER-PHYSICAL SYSTEMS | HUBCAP Project | Fact Sheet | H2020 | CORDIS | European Commission [Электронный ресурс]. – URL: <https://cordis.europa.eu/project/id/872698> (дата обращения: 27.12.2022).
43. CPS4EU [Электронный ресурс]. – URL: <https://cps4eu.eu/> (дата обращения: 27.12.2022).
44. Cyber Physical Systems for Europe | CPS4EU Project | Fact Sheet | H2020 | CORDIS | European Commission [Электронный ресурс]. – URL: <https://cordis.europa.eu/project/id/826276> (дата обращения: 27.12.2022).
45. Documents | KDT JU [Электронный ресурс]. – URL: <https://www.kdt-ju.europa.eu/documents?data=refresh> (дата обращения: 27.12.2022).
46. ECSEL-JU [Электронный ресурс]. – URL: <https://artemis-ia.eu/article/ecsel-ju.html> (дата обращения: 27.12.2022).
47. EPoSS - The Product Driven Platform | EPoSS [Электронный ресурс]. – URL: <https://www.smart-systems-integration.org/> (дата обращения: 27.12.2022).
48. Key Digital Technologies : Aeneas [Электронный ресурс]. – URL: <https://aeneas-office.org/funding/kdt/> (дата обращения: 27.12.2022).
49. Inside Industry Association. Key Technologies [Электронный ресурс]. – URL: <https://www.inside-association.eu/key-technologies> (дата обращения: 27.12.2022).
50. ECS SRIA| Strategic Research and Innovation Agenda 2023 [Электронный ресурс]. – URL: <https://ecssria.eu/> (дата обращения: 28.12.2022).
51. Editor. Publication of the ECS SRIA 2022 [Электронный ресурс]. – URL: <https://aeneas-office.org/2022/01/17/publication-of-ecs-sria-2022/> (дата обращения: 28.12.2022).
52. What we do | KDT JU [Электронный ресурс]. – URL: <https://www.kdt-ju.europa.eu/what-we-do> (дата обращения: 28.12.2022).
53. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance). Vol. 166. – 2021.
54. National Cyber Strategy 2022 [Электронный ресурс]. – URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022> (дата обращения: 28.12.2022).
55. UK's Digital Strategy [Электронный ресурс]. – URL: <https://www.gov.uk/government/publications/uks-digital-strategy> (дата обращения: 28.12.2022).
56. UK Innovation Strategy: leading the future by creating it [Электронный ресурс]. – URL: <https://www.gov.uk/government/publications/uk-innovation-strategy-leading-the-future-by-creating-it> (дата обращения: 28.12.2022).
57. Enabling a national Cyber-Physical Infrastructure to catalyse innovation: consultation document (accessible webpage) [Электронный ресурс]. – URL: <https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage> (дата обращения: 28.12.2022).
58. What is Industrie 4.0? [Электронный ресурс]. – URL: <https://www.plattform-i40.de/IP/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html> (дата обращения: 28.12.2022).
59. Kagermann H. Ten Years of Industrie 4.0 / H. Kagermann, W. Wahlster // Sci. – 2022. – Vol. 4. – № 3. – P. 26.
60. Results [Электронный ресурс]. – URL: <https://www.plattform-i40.de/IP/Navigation/EN/Services-Results/Results/results.html> (дата обращения: 28.12.2022).

61. 2030 Vision for Industrie 4.0 [Электронный ресурс]. – URL: <https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Vision-2030-for-Industrie-4.0.html> (дата обращения: 28.12.2022).
62. 2030 Vision for Industrie 4.0. Shaping Digital Ecosystems Globally [Электронный ресурс]. – URL: <https://www.plattform-i40.de/IP/Navigation/EN/Industrie40/Vision/vision.html> (дата обращения: 28.12.2022).
63. Der deutsche Gaia-X Hub [Электронный ресурс]. – URL: <https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html> (дата обращения: 28.12.2022).
64. Gaia-X: A Federated Secure Data Infrastructure [Электронный ресурс]. – URL: <https://gaia-x.eu/> (дата обращения: 28.12.2022).
65. Winter J. Towards the Next Decade of Industrie 4.0 – Current State in Research and Adoption and Promising Development Paths from a German Perspective / J. Winter, A. Frey, J. Biehler // Sci. – 2022. – Vol. 4. – № 3. – P. 31.
66. 中国制造2025 (Made in China 2025) [Электронный ресурс]. – URL: http://mp.weixin.qq.com/s?__biz=MzUzODAxMjA0OQ==&mid=2247496764&idx=1&sn=69edafcff965c8b48b3820fea5bad2a5&chksm=fadc84c2cdab0dd43bcd5efda4edb59018872c87ca9d18475e8ba2f636fc9b6a7d119f96b963#rd (дата обращения: 28.12.2022).
67. Made in China-2025. IoT-ONE [Электронный ресурс]. – URL: <http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf> (дата обращения: 28.12.2022).
68. China's 14th Five-Year Plan (2021-2025) Report [Электронный ресурс]. – URL: <https://www.hkstrategies.com/en/chinas-14th-five-year-plan-2021-2025-report/> (дата обращения: 28.12.2022).
69. China issues guideline on expanding domestic demand-Xinhua [Электронный ресурс]. – URL: <https://english.news.cn/20221215/ce17156e641844a85c51fa3356e94e9/c.html> (дата обращения: 28.12.2022).
70. В Китае опубликовано руководство по расширению внутреннего спроса - Российская газета [Электронный ресурс]. – URL: <https://rg.ru/2022/12/16/v-kitae-opublikovano-rukovodstvo-po-rasshireniiu-vnutrennego-sprosa.html> (дата обращения: 28.12.2022).
71. (全文) 中共中央 国务院印发《扩大内需战略规划纲要 (2022—2035年)》(The Outline of the Strategic Plan for Expanding Domestic Demand (2022-2035)) [Электронный ресурс]. – URL: <http://www.stcn.com/article/detail/755021.html> (дата обращения: 28.12.2022).
72. Программа «Цифровая экономика Российской Федерации» (Распоряжение от 28 июля 2017 г. № 1632-р) [Электронный ресурс]. – URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf> (дата обращения: 28.12.2022).
73. Распоряжение Правительства Российской Федерации от 12.02.2019 № 195-р · Официальное опубликование правовых актов · Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/Document/View/0001201902190011> (дата обращения: 28.12.2022).
74. Цифровая экономика РФ [Электронный ресурс] : Направления деятельности. – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 2022. – URL: <https://digital.gov.ru/ru/activity/directions/858/> (дата обращения: 12.12.2022).
75. Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: <http://government.ru/info/35568/> (дата обращения: 28.12.2022).
76. Паспорт национальной программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: <http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf> (дата обращения: 28.12.2022).
77. Федеральный проект «Цифровые технологии» национальной программы «Цифровая экономика». Меры поддержки/Технологии. [Электронный ресурс]. – URL: <https://digital.ac.gov.ru/support#technology> (дата обращения: 11.11.2019).

78. Федеральный проект «Искусственный интеллект» [Электронный ресурс]. – URL: <https://digital.gov.ru/ru/activity/directions/1046/> (дата обращения: 28.12.2022).
79. Развитие отдельных высокотехнологичных направлений. Белая книга / А.М. Абакумов [и др.]; ред. Т.Л. Броницкий [и др.]. – Национальный исследовательский университет «Высшая школа экономики», 2022.
80. Нормативное регулирование цифровой среды | Министерство экономического развития Российской Федерации [Электронный ресурс]. – URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/ (дата обращения: 28.12.2022).
81. Федеральный проект «Информационная безопасность» [Электронный ресурс]. – URL: <https://digital.gov.ru/ru/activity/directions/874/> (дата обращения: 28.12.2022).
82. На базе Санкт-Петербургского университета Бонч-Бруевича открылся киберполигон : [Электронный ресурс]. – URL: <https://digital.gov.ru/ru/events/41426/> (дата обращения: 28.12.2022).
83. Подписаны соглашения о намерениях между Правительством и крупнейшими компаниями о развитии отдельных высокотехнологичных направлений [Электронный ресурс]. – URL: <http://kremlin.ru/events/president/news/60971> (дата обращения: 16.11.2020).
84. Утверждены «дорожные карты» «Новое индустриальное программное обеспечение» и «Новое общестемное программное обеспечение» [Электронный ресурс]. – URL: <http://government.ru/news/47353/> (дата обращения: 28.12.2022).
85. Уткин Н. Значение стандартизации киберфизических систем для экономики России [Электронный ресурс]. – URL: https://metrob.ru/html/Stati/stand/kiberphysical_sistems.html (дата обращения: 23.12.2022).
86. IoT Devices and Infrastructures Group | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructures-group> (дата обращения: 23.12.2022).
87. Cyber Physical Systems | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/itl/ssd/cyber-physical-systems> (дата обращения: 23.12.2022).
88. Ross Jr. W.L. NIST SP 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview / W.L. Ross Jr., K. Rochford. – NIST, 2017.
89. NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things / C. Greer [и др.]. – NIST, 2019.
90. IoT-Enabled Smart City Framework [Электронный ресурс]. – URL: <https://pages.nist.gov/smartcitiesarchitecture/> (дата обращения: 23.12.2022).
91. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0 [Электронный ресурс]. – URL: <https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40> (дата обращения: 23.12.2022).
92. Framework for Cyber-Physical Systems: Volume 3, Timing Annex [Электронный ресурс]. – URL: <https://www.nist.gov/publications/framework-cyber-physical-systems-volume-3-timing-annex> (дата обращения: 23.12.2022).
93. Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems [Электронный ресурс]. – URL: <https://www.nist.gov/publications/ontology-based-reasoning-about-trustworthiness-cyber-physical-systems> (дата обращения: 23.12.2022).
94. A Standards-Based Approach for Linking As-Planned to As-Fabricated Product Data [Электронный ресурс]. – URL: <https://www.nist.gov/publications/standards-based-approach-linking-planned-fabricated-product-data> (дата обращения: 23.12.2022).
95. Cyber-Physical Systems Public Working Group [Электронный ресурс]. – URL: <https://pages.nist.gov/cpspwg/> (дата обращения: 23.12.2022).
96. UCEF: Universal CPS Environment for Federation | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructures-group/ucef-universal-cps> (дата обращения: 23.12.2022).

97. The UCEF Approach to Tool Integration for HLA Co-Simulations | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/publications/ucef-approach-tool-integration-hla-co-simulations> (дата обращения: 23.12.2022).
98. Universal CPS Environment for Federation (UCEF) | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/publications/universal-cps-environment-federation-ucef> (дата обращения: 23.12.2022).
99. Standards.gov | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/standardsgov> (дата обращения: 23.12.2022).
100. ISO - Cyber-physical systems [Электронный ресурс]. – URL: <https://www.iso.org/foresight/cyber-physical-systems.html> (дата обращения: 23.12.2022).
101. Cyber security | IEC [Электронный ресурс]. – URL: <https://www.iec.ch/cyber-security> (дата обращения: 23.12.2022).
102. Современные технологии. Киберфизические системы: учебное пособие. – Томский политехнический университет. – Томск: Издательство Томского политехнического университета, 2021. – 166 с.
103. ISO 23704-1:2022(en) General requirements for cyber-physically controlled smart machine tool systems (CPSMT) — Part 1: Overview and fundamental principles. – 2022.
104. Turovets Y. Standardization in digital manufacturing: implications for Russia and the EAEU / Y. Turovets, K. Vishnevskiy // Business Informatics. – 2019. – Т. 13. – № 3. – С. 78-96.
105. A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing / A.J.C. Trappey [и др.] // IEEE Access. – 2016. – № 4. – С. 7356-7382.
106. Развитие законодательства о робототехнике и киберфизических системах. Отчет по результатам исследования / А. Незнамов [и др.]. – Дентонс Юроп, 2018.
107. Understanding Canadian Cybersecurity Laws: Measuring up — Outlining existing federal cybersecurity legislation in Canada, the UK, Australia, and the US [Электронный ресурс]. – URL: <https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-measuring-up-outlining-existing-federal-cybersecurity-legislation-in-canada-the-uk-australia-and-the-us-article-8/440343> (дата обращения: 23.12.2022).
108. ЦСР. Оценка потенциала российских решений в области кибербезопасности на международном рынке [Электронный ресурс]. – URL: <https://www.csr.ru/upload/iblock/a6d/h9lkrjgaawtho0hg7sy7ofgur7p9anx1.pdf> (дата обращения: 23.12.2022).
109. Cybersecurity 2022 - Germany | Global Practice Guides | Chambers and Partners [Электронный ресурс]. – URL: <https://practiceguides.chambers.com/practice-guides/cybersecurity-2022/germany> (дата обращения: 23.12.2022).
110. Analysis of Cyber Laws in USA, UAE and Germany - Enhelion Blogs [Электронный ресурс]. – URL: <https://enhelion.com/blogs/2020/11/24/analysis-of-cyber-laws-in-usa-uae-and-germany/> (дата обращения: 23.12.2022).
111. China's Emerging Cyber Governance System | Center for Strategic and International Studies [Электронный ресурс]. – URL: <https://www.csis.org/programs/strategic-technologies-program/other-projects-cybersecurity/chinas-emerging-cyber> (дата обращения: 26.12.2022).
112. Приказ от 27 марта 2017 года № 642 "О создании технического комитета по стандартизации «Киберфизические системы» [Электронный ресурс]. – URL: <https://docs.cntd.ru/document/456055018> (дата обращения: 23.12.2022).
113. Распоряжение Правительства Российской Федерации от 19.08.2020 г. № 2129-р [Электронный ресурс]. – URL: <http://government.ru/docs/all/129505/> (дата обращения: 23.12.2022).
114. ТК 194 Кибер-физические системы [Электронный ресурс]. – URL: <http://tc194.ru/> (дата обращения: 23.12.2022).
115. Распоряжение Правительства Российской Федерации от 23.03.2018 г. № 482-р [Электронный ресурс]. – URL: <http://government.ru/docs/all/115963/> (дата обращения: 23.12.2022).

116. Перспективный план стандартизации в области передовых производственных технологий на 2018 – 2025 годы [Электронный ресурс]. – URL: <https://nti2035.ru/upload/iblock/41c/41cb2bc4c3bad4a7b6a2d99486abfdad.pdf> (дата обращения: 23.12.2022).
117. Минпромторг и Росстандарт обновили Перспективный план стандартизации технологий Индустрии 4.0 [Электронный ресурс]. – URL: https://minpromtorg.gov.ru/press-centre/news/#!minpromtorg_i_rosstandart_obnovili_perspektivnyy_plan_standartizacii_tehnologiy_industrii_40 (дата обращения: 23.12.2022).
118. О продолжении В России работы над регулированием технологий индустрии 4.0 – ФГБУ «Институт стандартизации» [Электронный ресурс]. – URL: <https://www.gostinfo.ru/InformationOfStandardization/Details/2909> (дата обращения: 23.12.2022).
119. В России продолжат работу над регулированием технологий Индустрии 4.0 [Электронный ресурс]. – URL: https://minpromtorg.gov.ru/press-centre/news/#!v_rossii_prodolzhat_rabotu_nad_regulirovaniem_tehnologiy_industrii_40 (дата обращения: 23.12.2022).
120. Российская венчурная компания передана в управление РФПИ [Электронный ресурс]. – URL: <https://www.interfax.ru/russia/738266> (дата обращения: 26.12.2022).
121. Никита Уткин: «Стандартизация – не про стены, а про мосты» - Connect-WIT [Электронный ресурс]. – URL: <https://www.connect-wit.ru/nikita-utkin-standartizatsiya-ne-pro-steny-a-pro-mosty.html> (дата обращения: 23.12.2022).
122. Технический комитет «Кибер-физические системы» получил статус соредатора международного стандарта IoT ISO/IEC [Электронный ресурс]. – URL: <https://iot.ru/promyshlennost/tekhnicheskii-komitet-kiber-fizicheskie-sistemy-poluchil-status-soredatora-mezhdunarodnogo-standart> (дата обращения: 23.12.2022).
123. Быкова Н. ТК 194 «Кибер-физические системы» / Н. Быкова // Стандарты и качество. – 2021. – № 5. – С. 50–51.
124. Технический комитет по стандартизации 141 «Робототехника» [Электронный ресурс]. – URL: <https://tk141.rtc.ru/> (дата обращения: 23.12.2022).
125. Стандарты ТК 141 [Электронный ресурс]. – URL: <https://tk141.rtc.ru/index.php/dokumenty/standarty-tk-141> (дата обращения: 23.12.2022).
126. Cyber Physical Systems and Internet of Things Program | NIST [Электронный ресурс]. – URL: <https://www.nist.gov/programs-projects/cyber-physical-systems-and-internet-things-program> (дата обращения: 23.12.2022).
127. The Lens [Электронный ресурс] : Free & Open Patent and Scholarly Search. – URL: <https://www.lens.org/lens> (дата обращения: 20.12.2022).
128. Companies ranked by Market Cap [Электронный ресурс]. – URL: <https://companiesmarketcap.com/> (дата обращения: 20.12.2022).
129. Encoding system for incremental redundancy for hybrid ARQ for wireless networks [Электронный ресурс] : Patent No.: US – 11184117 B2. – Nokia Technologies Oy, 2021. – URL: https://www.lens.org/images/patent/US/11184117/B2/US_11184117_B2.pdf (дата обращения: 20.12.2022).
130. Transmission of network slicing constraints in 5G wireless networks [Электронный ресурс] : Patent No.: US – 10959225 B2. – Nokia Technologies Oy, 2020. – URL: https://www.lens.org/images/patent/US/10638356/B2/US_10638356_B2.pdf (дата обращения: 20.12.2022).
131. Techniques for handling semi-persistent scheduling collisions for wireless networks [Электронный ресурс] : Patent No.: US – 10959225 B2. – Nokia Technologies Oy, 2021. – URL: https://www.lens.org/images/patent/US/10959225/B2/US_10959225_B2.pdf (дата обращения: 20.12.2022).
132. Network Slice Configuration [Электронный ресурс] : Patent No.: US – 0306215 A1. – Nokia Solutions & Networks Oy, 2021. – URL: https://www.lens.org/images/patent/US/10959225/B2/US_10959225_B2.pdf (дата обращения: 20.12.2022).

133. Doppler Compensation in Non-Terrestrial Networks [Электронный ресурс] : Patent No.: US – 0091276 A1. – Nokia Technologies Oy, 2022. – URL: https://www.lens.org/images/patent/US/20220091276/A1/US_2022_0091276_A1.pdf (дата обращения: 20.12.2022).
134. Systems and methods for skyline prediction for cyber-physical photovoltaic array control [Электронный ресурс] : Patent No.: US – 11132551 B2. – Arizona Board of Regents on Behalf of Arizona State University, 2021. – URL: https://www.lens.org/images/patent/US/11132551/B2/US_11132551_B2.pdf (дата обращения: 20.12.2022).
135. Systems Implementing Hierarchical Levels of Security [Электронный ресурс] : Patent No.: US – 0346644 A1. – Arizona Board of Regents on Behalf of Northern Arizona University, 2019. – URL: https://www.lens.org/images/patent/US/20170346644/A1/US_2017_0346644_A1.pdf (дата обращения: 20.12.2022).
136. Systems, Methods, and Apparatuses for Utilizing Co-Simulation of a Physical Model and a Self-Adaptive Predictive Controller Using Hybrid Automata [Электронный ресурс] : Patent No.: US – 0108203 A1. – Arizona Board of Regents on Behalf of Arizona State University, 2022. – URL: https://www.lens.org/images/patent/US/20200108203/A1/US_2020_0108203_A1.pdf (дата обращения: 20.12.2022).
137. Securing physically unclonable functions with additional random ternary states [Электронный ресурс] : Patent No.: US – 11310062 B2. – Arizona Board of Regents on Behalf of Northern Arizona University, 2022. – URL: https://www.lens.org/images/patent/US/11310062/B2/US_11310062_B2.pdf (дата обращения: 20.12.2022).
138. Support vector machine enhanced models for short-term wind farm generation forecasting [Электронный ресурс] : Patent No.: US – 10181101 B2. – Arizona Board of Regents on Behalf of Arizona State University, 2019. – URL: https://www.lens.org/images/patent/US/10181101/B2/US_10181101_B2.pdf (дата обращения: 20.12.2022).
139. Framework to develop cyber-physical system behavior-based monitoring [Электронный ресурс] : Patent No.: US – 11005870 B2. – General Electric Company, 2021. – URL: https://www.lens.org/images/patent/US/11005870/B2/US_11005870_B2.pdf (дата обращения: 20.12.2022).
140. Detection and protection against mode switching attacks in cyber-physical systems [Электронный ресурс] : Patent No.: US – 11170314 B2. – General Electric Company, 2021. – URL: https://www.lens.org/images/patent/US/11170314/B2/US_11170314_B2.pdf (дата обращения: 20.12.2022).
141. Dynamic Physical Watermarking For Attack Detection In Cyber-Physical Systems [Электронный ресурс] : Patent No.: US – 0106785 A1. – General Electric Company, 2021. – URL: https://www.lens.org/images/patent/US/20200106785/A1/US_2020_0106785_A1.pdf (дата обращения: 20.12.2022).
142. System and method for anomaly and cyber-threat detection in a wind turbine [Электронный ресурс] : Patent No.: US – 11113395 B2. – General Electric Company, 2021. – URL: https://www.lens.org/images/patent/US/11113395/B2/US_11113395_B2.pdf.
143. Cyber-attack detection, localization, and neutralization for unmanned aerial vehicles [Электронный ресурс] : Patent No.: US – 10931687 B2. – General Electric Company, 2021. – URL: https://www.lens.org/images/patent/US/10931687/B2/US_10931687_B2.pdf (дата обращения: 20.12.2022).
144. Method for classifying and correlating simulation components to functional models [Электронный ресурс] : Patent No.: US – 9778636 B2. – Siemens Industry Software Inc, 2017. – URL: https://www.lens.org/images/patent/US/9778636/B2/US_9778636_B2.pdf (дата обращения: 20.12.2022).
145. Production Module for Performing a Production Function on a Product [Электронный ресурс] : Patent No.: US – 0322542 A1. – Siemens Aktiengesellschaft, 2019. – URL: https://www.lens.org/images/patent/US/20170322542/A1/US_2017_0322542_A1.pdf (дата обращения: 20.12.2022).
146. Method for planning the manufacture of a product and production module having self-description information [Электронный ресурс] : Patent No.: US – 11003174 B2. – Siemens Aktiengesellschaft, 2021. – URL: https://www.lens.org/images/patent/US/11003174/B2/US_11003174_B2.pdf (дата обращения: 20.12.2022).
147. Method and Apparatus for Providing a Safe Operation of a Technical System [Электронный ресурс] : Patent No.: US – 0344673 A1. – Siemens Aktiengesellschaft, 2019. – URL: https://www.lens.org/images/patent/US/20170344673/A1/US_2017_0344673_A1.pdf (дата обращения: 20.12.2022).

148. Context-Based Synthesis Of Simulation Models From Functional Models Of Cyber-Physical Systems [Электронный ресурс] : Patent No.: US – 0019104 A1. – Siemens Aktiengesellschaft, 2017. – URL: https://www.lens.org/images/patent/US/20140019104/A1/US_2014_0019104_A1.pdf (дата обращения: 20.12.2022).
149. Cyber-physical systems [Электронный ресурс] : Robotics, Autonomous vehicles, Internet of things, Smart cities. – ISO, 2021. – URL: <https://www.iso.org/foresight/cyber-physical-systems.html> (дата обращения: 22.12.2022).
150. Cyber Security Statistics Trends & Data [Электронный ресурс] : Cost Of Cyber Security. / PurpleSec. – 2022. – URL: <https://purplesec.us/resources/cyber-security-statistics/> (дата обращения: 22.12.2022).
151. Nokia launches first off-the-shelf, mission-critical Industrial Edge to accelerate the enterprise journey to Industry 4.0 [Электронный ресурс] : Press Release. – Nokia, 2021. – URL: <https://www.nokia.com/about-us/news/releases/2021/10/06/nokia-launches-first-off-the-shelf-mission-critical-industrial-edge-to-accelerate-the-enterprise-journey-to-industry-40/> (дата обращения: 22.12.2022).
152. IUDX: Partnerships [Электронный ресурс] : India Urban Data Exchange. – IUDX, 2020. – URL: <https://iudx.org.in/partnerships/> (дата обращения: 22.12.2022).
153. “Indian Urban Data Exchange” for Smart Cities [Электронный ресурс] : An overview of the rationale, architecture and methodology. – RBCCPS, 2018. – URL: <https://cps.iisc.ac.in/iudx/> (дата обращения: 22.12.2022).
154. IUDX: Platform [Электронный ресурс] : India Urban Data Exchange. – IUDX, 2020. – URL: <https://iudx.org.in/platform/> (дата обращения: 22.12.2022).
155. IUDX: Cities [Электронный ресурс] : India Urban Data Exchange. – IUDX, 2020. – URL: <https://iudx.org.in/cities/> (дата обращения: 22.12.2022).
156. MX Industrial Edge [Электронный ресурс] : Accelerate digitalization for mission critical industrial OT. – Nokia, 2021. – URL: <https://www.nokia.com/networks/industry-solutions/mx-industrial-edge/> (дата обращения: 22.12.2022).
157. Cybersecurity for Defense: Strengthening our nation’s cyber protection [Электронный ресурс] : Digitalization for Defense. – Siemens Government Technologies, 2021. – URL: <https://www.siemensgovt.com/solutions/digitalization-for-defense> (дата обращения: 22.12.2022).
158. Cantrell W. Cyber-Physical Protection Platforms Safeguard Critical Operations [Электронный ресурс] : By coupling threat detection systems with intelligent actions, organizations can better protect their processes from internal and external threats. – Siemens Government Technologies, 2021. – URL: <https://www.siemensgovt.com/insights/white-papers/wp-energy-savings-performance-contracts> (дата обращения: 22.12.2022).
159. Nokia in 2021 [Электронный ресурс] : Annual Report. – Nokia, 2021. – URL: <https://www.nokia.com/system/files/2022-03/nokia-ar21-en.pdf> (дата обращения: 26.12.2022).
160. Bosch in 2021 [Электронный ресурс] : Annual Report. – Bosch, 2021. – URL: https://assets.bosch.com/media/global/bosch_group/our_figures/pdf/bosch-annual-report-2021.pdf (дата обращения: 26.12.2022).
161. Microsoft in 2021 [Электронный ресурс] : Annual Report. – Microsoft, 2021. – URL: <https://www.microsoft.com/investor/reports/ar21/index.html> (дата обращения: 26.12.2022).
162. Siemens in 2021 [Электронный ресурс] : Annual Report. – Siemens, 2021. – URL: https://new.siemens.com/content/dam/internet/siemens-com/global/company/investor-relations/application-pages/report/report4you_en/assets/pdfs/Siemens_Report_FY2021.pdf?ste_sid=782dce6e2b4bd4da2d58837a9fc73284 (дата обращения: 26.12.2022).
163. Wallach O. The World’s Biggest Startups [Электронный ресурс] : Top Unicorns of 2021. / Visual Capitalist. – 2021. – URL: <https://www.visualcapitalist.com/the-worlds-biggest-startups-top-unicorns-of-2021/> (дата обращения: 26.12.2022).
164. Nokia completes acquisition of Elenion Technologies [Электронный ресурс] : Nokia today announced the successful completion of its acquisition of Elenion Technologies. – Nokia, 2020. – URL: <https://www.nokia.com/about-us/news/releases/2020/03/25/nokia-completes-acquisition-of-elenion-technologies/> (дата обращения: 23.12.2022).
165. ItoM – Semiconductor Ideas to the Market [Электронный ресурс] : ItoM is now part of the Bosch Group. – ItoM, 2022. – URL: <https://www.itom.nl/> (дата обращения: 26.12.2022).

166. Bosch plans acquisition of the MoTeC Group [Электронный ресурс] : Portfolio and market expansion for Bosch Motorsport. – Bosch Presse, 2022. – URL: <https://www.bosch-presse.de/pressportal/de/en/bosch-plans-acquisition-of-the-motec-group-242496.html> (дата обращения: 26.12.2022).
167. Acquisitions by Bosch [Электронный ресурс] : Overview of Bosch's Acquisitions. / Tracxn. – 2022. – URL: <https://tracxn.com/d/acquisitions/acquisitionsbyBosch/> (дата обращения: 26.12.2022).
168. Accenture, Microsoft and Avanade expand partnership [Электронный ресурс] : Helping organizations tackle their greatest sustainability challenges. – Microsoft, 2022. – URL: <https://news.microsoft.com/2022/06/02/accenture-microsoft-and-avanade-expand-partnership-to-help-organizations-tackle-their-greatest-sustainability-challenges/> (дата обращения: 26.12.2022).
169. Sokol Flex OS [Электронный ресурс] : Digital Industries Software. – Siemens, 2022. – URL: <https://static.sw.cdn.siemens.com/siemens-disw-assets/public/60tq0h1PnTjNqTEJfENAIL/en-US/Siemens-SW-Sokol-Flex-OS-FS-82900-D0.pdf> (дата обращения: 29.12.2022).
170. Siemens in 2022 [Электронный ресурс] : Annual Report. – Siemens, 2022. – URL: https://www.siemens.com/applications/b09c49eb-3a14-73b3-9f71-e30e3c2dfdbd/assets/pdfs/en/Siemens_Report_FY2022.pdf (дата обращения: 29.12.2022).
171. Publicly funded projects [Электронный ресурс] : Top publicly funded projects Bosch Research is involved in. – Bosch, 2022. – URL: <https://www.bosch.com/research/meet-bosch-research/collaboration/publicly-funded-projects/> (дата обращения: 29.12.2022).
172. ATTENTION [Электронный ресурс] : Project to improve road safety. – University of Stuttgart, 2022. – URL: <https://www.simtech.uni-stuttgart.de/press/ATTENTION-project-to-improve-road-safety/> (дата обращения: 29.12.2022).
173. Hexa-X [Электронный ресурс] : A flagship for 6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds. – Hexa-X, 2022. – URL: <https://hexa-x.eu/> (дата обращения: 29.12.2022).
174. Consortium [Электронный ресурс] : Member list. – Hexa-X, 2022. – URL: <https://hexa-x.eu/consortium/> (дата обращения: 29.12.2022).
175. Hexa-X Project [Электронный ресурс] : A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds. – European Commission, 2022. – URL: <https://cordis.europa.eu/project/id/101015956> (дата обращения: 29.12.2022).
176. Objectives [Электронный ресурс] : Project overview structure. – Hexa-X, 2022. – URL: <https://hexa-x.eu/objectives/> (дата обращения: 29.12.2022).
177. Kim E. Amazon is cutting some robotics projects [Электронный ресурс] : Reorganization inside Amazon. / Business Insider. – 2022. – URL: <https://www.businessinsider.com/amazon-cuts-robotics-projects-canvas-warehouse-robots-scout-2022-10> (дата обращения: 30.12.2022).
178. Korosec K. Ford, VW-backed Argo AI is shutting down [Электронный ресурс] : Another project shutted down. / Techcrunch – 2022. – URL: <https://techcrunch.com/2022/10/26/ford-vw-backed-argo-ai-is-shutting-down/> (дата обращения: 30.12.2022).
179. Koetsier J. 9 Things We Lost When Google Canceled Its Smart Cities Project In Toronto [Электронный ресурс] : Three years ago Google subsidiary Sidewalk Labs. / Forbes. – 2020. – URL: <https://www.forbes.com/sites/johnkoetsier/2020/05/13/9-things-we-lost-when-google-canceled-its-smart-cities-project-in-toronto/> (дата обращения: 30.12.2022).
180. Киберфизические системы. [Электронный ресурс]. – URL: <https://www.iso.org/foresight/cyber-physical-systems.html> (дата обращения: 29.11.2022).
181. Перспективные направления применения робототехники в бизнесе [Электронный ресурс] : Официальный портал Росконгресса. – URL: <https://roscongress.org/materials/perspektivnye-napravleniya-primeneniya-robototekhniki-v-biznese/>.
182. Варшавский А.Е. Мировые тенденции и направления развития промышленных роботов / А.Е. Варшавский, В.В. Дубинина // МИР (Модернизация. Инновации. Развитие). – 2020. – Т. 11. – № 3. – С. 294–319.

183. Технологии робототехники 2020 [Электронный ресурс] : Официальный портал Агентства промышленного развития Москвы. – URL: <https://apr.moscow/content/data/4/Технологии робототехники.pdf>.
184. CNews Analytics выпускает первый обзор рынка промышленной робототехники [Электронный ресурс]. – URL: https://www.cnews.ru/news/top/2021-07-26_snews_analytics_vypuskaet_pervyj (дата обращения: 08.12.2022).
185. How smart sensors are driving Industry 4.0 forward [Электронный ресурс]. – URL: https://www.ey.com/en_ch/industrial-products/how-smart-sensors-are-driving-industry-4-0-forward (дата обращения: 11.12.2022).
186. Top 7 Sensor Technology Companies In The Global Market [Электронный ресурс]. – URL: <https://straitresearch.com/blog/top-7-sensor-technology-companies-in-the-global-market> (дата обращения: 11.12.2022).
187. Brien Posey. What is a Smart Sensor and How Does It Work? [Электронный ресурс]. – URL: <https://www.techtarget.com/iotagenda/definition/smart-sensor> (дата обращения: 11.12.2022).
188. Липкин Е. ИНДУСТРИЯ 4.0: Умные технологии – ключевой элемент в промышленной конкуренции [Электронный ресурс]. – URL: <https://www.soel.ru/online/kniga-industriya-4-0-umnye-tehnologii-klyuchevoe-element-v-promyshlennoy-konkurentsii-chast-6-goriz/> (дата обращения: 11.12.2022).
189. Развитие IoT-рынка [Электронный ресурс]. – URL: <https://lib.itsec.ru/articles2/internet-of-things/razvitie-iot-rynka>.
190. Дорожная карта развития «сквозной» цифровой технологии «Новые производственные технологии». – Министерство цифрового развития, связи и массовых коммуникаций РФ, .
191. ГОСТ Р 57700.37-2021 «Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения».
192. Байдаров Д.Ю. Программное обеспечение «тяжелого» класса: возможности импортозамещения / Д.Ю. Байдаров, Е.М. Абакумов, Д.Ю. Файков // Russian Journal of Innovation Economics. – 2022. – Т. 12. – Программное обеспечение «тяжелого» класса. – № 1. – С. 295-316.
193. Что такое Интернет вещей и как он работает? | SAP Insights [Электронный ресурс]. – URL: <https://www.sap.com/cis/insights/what-is-iot-internet-of-things.html> (дата обращения: 14.12.2022).
194. Промышленный Интернет вещей. Цифровая трансформация [Электронный ресурс]. – URL: <https://aws.amazon.com/ru/iot/solutions/industrial-iot/> (дата обращения: 14.12.2022).
195. Городнова Н.В. Индустриальный интернет вещей в России: сущность и перспективы / Н.В. Городнова // Russian Journal of Innovation Economics. – 2022. – Т. 12. – Индустриальный интернет вещей в России. – № 3. – С. 1503-1522.
196. Top Suppliers of Internet of Things (IoT) Services in the USA [Электронный ресурс]. – URL: <https://www.thomasnet.com/articles/top-suppliers/internet-of-things-iot-companies/> (дата обращения: 14.12.2022).
197. Интернет вещей: сегодняшние лидеры [Электронный ресурс]. – URL: <https://spbspecials.rbc.ru/iot-leading-industries> (дата обращения: 14.12.2022).
198. Where and how to capture accelerating IoT value [Электронный ресурс]. – URL: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it> (дата обращения: 14.12.2022).
199. Объем рынка интернета вещей в России вырос на 18,3% [Электронный ресурс]. – URL: <https://rg.ru/2021/07/28/obem-rynka-interneta-veshchej-v-rossii-vyros-na-183.html> (дата обращения: 14.12.2022).
200. Рынок «Интернета вещей» России на современном этапе [Электронный ресурс]. – URL: <https://www.it-world.ru/it-news/reviews/183872.html> (дата обращения: 14.12.2022).
201. Что такое «Индустрия 4.0»? Определение, технологии, преимущества [Электронный ресурс]. – URL: <https://www.sap.com/cis/insights/what-is-industry-4-0.html> (дата обращения: 13.12.2022).
202. ГОСТ ISO/IEC 17788-2016. Облачные вычисления. Общие положения и терминология.

203. Cloud Computing [Электронный ресурс]. – URL: <https://www.bcg.com/capabilities/digital-technology-data/cloud-computing> (дата обращения: 13.12.2022).
204. Обзор облачных систем от российских компаний [Электронный ресурс]. – URL: <https://vc.ru/services/103351-obzor-oblachnyh-sistem-ot-rossiyskih-kompaniy> (дата обращения: 13.12.2022).
205. Felix Richter. Amazon, Microsoft & Google Dominate Cloud Market [Электронный ресурс]. – URL: <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/> (дата обращения: 13.12.2022).
206. Bailin J. Cloud computing trends 2023: Top predictions, stats, and growth drivers [Электронный ресурс]. – URL: <https://www.the-future-of-commerce.com/2022/11/09/cloud-computing-trends-2023/> (дата обращения: 13.12.2022).
207. 12 Cloud Computing Risks & Challenges Businesses Are Facing In These Days [Электронный ресурс]. – URL: <https://www.datapine.com/blog/cloud-computing-risks-and-challenges/> (дата обращения: 13.12.2022).
208. ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь».
209. Что такое Big Data и почему их называют «новой нефтью» [Электронный ресурс]. – URL: <https://trends.rbc.ru/trends/innovation/5d6c020b9a7947a740fea65c> (дата обращения: 14.12.2022).
210. Big Data: перспективы развития, тренды и объемы рынка больших данных [Электронный ресурс]. – URL: <https://delprof.ru/download/pub/big-data-perspektivy-razvitiya-trendy-i-obemy-rynka-bolshikh-dannykh/>.
211. Big Data Analytics [Электронный ресурс]. – URL: <https://www.ibm.com/analytics/big-data-analytics> (дата обращения: 14.12.2022).
212. Пандемия ускорила развитие рынка больших данных [Электронный ресурс]. – URL: <https://rg.ru/2021/01/26/pandemiia-uskorila-razvitie-rynka-bolshih-dannyh.html> (дата обращения: 14.12.2022).
213. Amy Robotics, AMY-A3 Multifunctional Service Robot [Электронный ресурс]. – URL: <https://global.amyrobotics.com/indexpdetailsen?id=30&seriesid=4> (дата обращения: 15.12.2022).
214. Canbot, UU - U05 Humanoid service robot for commercial use [Электронный ресурс]. – URL: <http://www.uurobot.com/en/index.html> (дата обращения: 15.12.2022).
215. Chuangze Intelligent, Сервисный робот [Электронный ресурс]. – URL: <http://www.chuangze.com.cn/daping.asp> (дата обращения: 15.12.2022).
216. Hancom, The Next Generation of AI Robot «Toki2» [Электронный ресурс]. – URL: http://www.hancomrobotics.com/robotics_en/index (дата обращения: 15.12.2022).
217. LG, CLOi GuideBot [Электронный ресурс]. – URL: <https://www.lg.com/global/business/cloi/lg-cloi-guidebot> (дата обращения: 15.12.2022).
218. Danfoss, Energy metering [Электронный ресурс]. – URL: <https://www.danfoss.com/en/markets/buildings-commercial/dhs/energy-metering/> (дата обращения: 15.12.2022).
219. Soft M, Энергоконтроль [Электронный ресурс]. – URL: <http://softm.tv/energy/> (дата обращения: 15.12.2022).
220. INFOWATCH, INFOWATCH EMPLOYEE MONITORING [Электронный ресурс]. – URL: <https://www.infowatch.ru/products/employee-monitoring> (дата обращения: 15.12.2022).
221. Kickidler, Employee Monitoring Software [Электронный ресурс]. – URL: <https://www.kickidler.com/> (дата обращения: 15.12.2022).
222. Deloitte, Industry 4.0 and the digital twin Manufacturing meets its match [Электронный ресурс]. – URL: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html?id=us:2sm:3tw:4dup3833:5awa:6DUPress:20170523:4ir:du_press&linkId=37860070 (дата обращения: 15.12.2022).
223. BIM based cyber-physical systems for intelligent disaster prevention / Y. Lei [et al.] // Journal of Industrial Information Integration. – 2020. – Vol. 20. – P. 100171.

224. РБК, Какие передовые технологии экспортирует Россия. Инфографика [Электронный ресурс]. – URL: <https://www.rbc.ru/specials/13/04/2021/607549af9a7947665097a07c> (дата обращения: 15.12.2022).
225. Федеральная служба по интеллектуальной собственности, Годовой отчет 2021 [Электронный ресурс]. – URL: <https://rospatent.gov.ru/content/uploadfiles/otchet-2021-ru.pdf>.
226. Электронный фонд правовых и нормативно-технических документов, CNTD [Электронный ресурс]. – URL: <https://docs.cntd.ru/document/1200158331> (дата обращения: 16.12.2022).
227. Anybus, Electric Mining Locomotive [Электронный ресурс]. – URL: <https://www.anybus.com/about-us/case-studies/electric-mining-locomotive> (дата обращения: 15.12.2022).
228. MNU, Tying multiple power systems together with intelligent controls [Электронный ресурс]. – URL: <https://www.mtu-solutions.com/au/en/technical-articles/2020/tying-multiple-power-systems-together-with-intelligent-controls.html> (дата обращения: 15.12.2022).
229. PushCorp, Robotic Polishing [Электронный ресурс]. – URL: <https://pushcorp.com/application/robotic-polishing/> (дата обращения: 15.12.2022).
230. Информационный портал Pharmaceutical Technology, Automated Temperature Monitoring for the Healthcare and Pharmaceutical Industries [Электронный ресурс]. – URL: <https://www.pharmaceutical-technology.com/contractors/supply-chain/kelsius-automated-temperature-monitoring/> (дата обращения: 15.12.2022).
231. Thermo Scientific, CB Omni™ Fusion Online Elemental Analyzer [Электронный ресурс]. – URL: <https://www.thermofisher.com/order/catalog/product/CBOMNIFUSION> (дата обращения: 15.12.2022).
232. Empatica, Empatica Health Monitoring Platform for Clinical Trials [Электронный ресурс]. – URL: <https://www.empatica.com/platform/clinical-trials> (дата обращения: 15.12.2022).
233. Реестр «НТИ 1000», ПАО «ОДК-КАТУРН» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7610052644/> (дата обращения: 15.12.2022).
234. Prime Marine, Ship Management Software SIMPLIFIED [Электронный ресурс]. – URL: <https://www.primemarine.com/> (дата обращения: 15.12.2022).
235. Eaton, Foreseer electrical power monitoring system [Электронный ресурс]. – URL: <https://www.eaton.com/ph/en-us/catalog/services/foreseer.html> (дата обращения: 15.12.2022).
236. Schneider Electric, EcoStruxure IT Expert [Электронный ресурс]. – URL: <https://www.se.com/ww/en/product-range/65972-ecostruxure-it-expert/> (дата обращения: 15.12.2022).
237. Biz Intellia, IoT-Based Smart Factory and Machine Monitoring Solution [Электронный ресурс]. – URL: <https://www.biz4intellia.com/machine-monitoring-solution/> (дата обращения: 15.12.2022).
238. Danfoss, Smart refrigeration case control [Электронный ресурс]. – URL: <https://www.danfoss.com/en/markets/food-and-beverage/dcs/case-controls/#tab-overview> (дата обращения: 15.12.2022).
239. INTEC, SMARTCAM [Электронный ресурс]. – URL: <https://intecgroup.ru/smartcam> (дата обращения: 15.12.2022).
240. Dahua, IPC-HFW3441DG-AS-4G-EAU-B [Электронный ресурс]. – URL: <https://www.dahuasecurity.com/products/All-Products/Network-Cameras/Wireless-Series/4G-Camera/IPC-HFW3441DG-AS-4G-EAU-B> (дата обращения: 15.12.2022).
241. Реестр «НТИ 1000», ООО «7ТЕК» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/9705113553/> (дата обращения: 15.12.2022).
242. Сколково, НТК МОПРОБОТСИСТЕМ [Электронный ресурс]. – URL: <https://navigator.sk.ru/orn/1123032> (дата обращения: 15.12.2022).
243. Промобот, Promobot V.4 [Электронный ресурс]. – URL: <https://promo-bot.ru/production/promobot-v4/> (дата обращения: 15.12.2022).
244. MGBOT, Набор «Динамика ЙоТик М1» [Электронный ресурс]. – URL: https://mgbot.ru/catalog/uchebnaya_robototekhnika/nabor_dinamika_yotik_m1/ (дата обращения: 15.12.2022).

245. NASA - Cyber-Physical Systems Modeling and Analysis (CPSMA) Initiative [Электронный ресурс]. – URL: https://www.nasa.gov/centers/ames/cct/office/studies/cyber-physical_systems.html (дата обращения: 23.12.2022).
246. DRAFT Robotics, Tele-Robotics and Autonomous Systems Roadmap. Technology Area 04 / R. Ambrose [и др.]. – NASA, 2010.
247. DRAFT Modeling, Simulation, Information Technology & Processing Roadmap. Technology Area 11 / M. Shafto [и др.]. – NASA, 2010.
248. National Cyber Strategy of the United States of America - UNT Digital Library [Электронный ресурс]. – URL: <https://digital.library.unt.edu/ark:/67531/metadc1259394/> (дата обращения: 23.12.2022).
249. Smart Grid Research: Cyber Security - IEEE Cyber Security for the Smart Grid / K. Bhat [и др.] // IEEE. – 2013.
250. IEEE C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. – 2014.
251. ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels. – 2013.
252. GAO-19-332 Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid [Электронный ресурс]. – URL: <https://www.gao.gov/products/gao-19-332> (дата обращения: 23.12.2022).
253. NERC CIP Compliance Consultants, Services & Solutions - RSI Security [Электронный ресурс]. – URL: <https://www.rsisecurity.com/compliance-advisory-services/nerc/> (дата обращения: 23.12.2022).
254. Common Security Advisory Framework Version 2.0 [Электронный ресурс]. – URL: <https://docs.oasis-open.org/csaf/csaf/v2.0/cs02/csaf-v2.0-cs02.html> (дата обращения: 23.12.2022).
255. Cardenas A. Cyber-Physical Systems Security. Knowledge Area. Version 1.0.1 / A. Cardenas. – University of California Santa Cruz, 2021.
256. Cardenas A. Cyber-Physical Systems Security. Knowledge Area. Issue 1.0 / A. Cardenas. – University of California Santa Cruz, 2019.
257. Protecting Critical Cyber Systems - Canada.ca [Электронный ресурс]. – URL: <https://www.canada.ca/en/public-safety-canada/news/2022/06/protecting-critical-cyber-systems.html> (дата обращения: 23.12.2022).
258. Fundamentals of Cyber Security for Canada's CI Community. – Public Safety Canada, 2016.
259. Canada's Cyber Security Strategy. – Government of Canada, 2010.
260. The Cyber-Physical Infrastructure. – Robotics Growth Partnership, 2022.
261. UK Government Minimum Cyber Security Standard | IT Governance Ltd [Электронный ресурс]. – URL: <https://www.itgovernance.co.uk/uk-government-minimum-cyber-security-standard> (дата обращения: 23.12.2022).
262. Cyber Security Standards | IT Governance UK [Электронный ресурс]. – URL: <https://www.itgovernance.co.uk/cybersecurity-standards> (дата обращения: 23.12.2022).
263. Cyber-pHysical European Roadmap & Strategy - Research Agenda and Recommendations for Action / B. Schätz [и др.]. – 2015.
264. Directive on Security of Network and Information Systems [Электронный ресурс]. – URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2422 (дата обращения: 23.12.2022).
265. Woensel L.V. Ethical Aspects of Cyber-Physical Systems: Scientific Foresight study / L.V. Woensel, C. Kurrer, M. Kritikos. – European Parliamentary Research Service, 2016.
266. German Standardization Roadmap Industrie 4.0. Version 4. – DIN e. V., DKE Deutsche Kommission Elektrotechnik, 2020.
267. ETSI TS 103 645 V1.1.1 (2019-02) Cyber Security for Consumer Internet of Things. – ETSI, 2019.
268. ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI, 2020.

269. ETSI industry standard based on the Code of Practice - GOV.UK [Электронный ресурс]. – URL: <https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice> (дата обращения: 23.12.2022).
270. ISO/IEC TS 27100:2020(en) Information technology — Cybersecurity — Overview and concepts. – 2020.
271. ISO/IEC TS 27110:2021(en) Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines. – 2021.
272. ITU-T X.1060 (06/2021) Framework for the creation and operation of a cyber defence centre [Электронный ресурс]. – URL: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14721&lang=en> (дата обращения: 23.12.2022).
273. Strategy 2030. – CEN, CENELEC, 2021.
274. Schoitsch E. Strategic Agenda on Standardization for Cyber-Physical Systems / E. Schoitsch, J. Niehaus. – AIT Austrian Institute of Technology, 2017.
275. GB/T 41262-2022 Technical requirements of cyber-physical fusion anomaly detection system for industrial control system [Электронный ресурс]. – URL: https://gbstandards.org/GB_standard_english.asp?code=GB/T%2041262-2022 (дата обращения: 23.12.2022).
276. China as a “Cyber Great Power”: Beijing’s two voices in tele-communications / R. Doshi [и др.]. – The Brookings Institution, 2021.
277. Китай выпустил официальный документ по стандартизации кибербезопасности 5G - China Justice Observer [Электронный ресурс]. – URL: <https://ru.chinajusticeobserver.com/a/china-releases-white-paper-on-5g-cybersecurity-standardization> (дата обращения: 23.12.2022).
278. Cybersecurity 2022 - China | Global Practice Guides | Chambers and Partners [Электронный ресурс]. – URL: <https://practiceguides.chambers.com/practice-guides/cybersecurity-2022/china> (дата обращения: 23.12.2022).
279. The Cyber/Physical Security Framework. – Japanese Ministry of Economy, Trade and Industry, 2019.
280. National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS) [Электронный ресурс]. – URL: <https://www.serbonline.in/ICPS/HomePage> (дата обращения: 23.12.2022).
281. National Mission on Interdisciplinary Cyber-Physical Systems | UPSC - IAS [Электронный ресурс]. – URL: <https://digitallylearn.com/national-mission-on-interdisciplinary-cyber-physical-systems-upsc-ias/> (дата обращения: 23.12.2022).
282. Современные материалы для аддитивного производства [Электронный ресурс]. – URL: <https://viam.ru/review/5942> (дата обращения: 14.12.2022).
283. Кокцинская Е.М. «Умные» материалы и их применение (обзор) / Е.М. Кокцинская // Видеонаука: сетевой журнал. – 2016. – Т. 1.
284. Что такое Аэрогель? Виды, производство, применение [Электронный ресурс]. – URL: <https://xn--b1agyekgek.xn--p1ai/articles/chto-takoe-aerogel/> (дата обращения: 14.12.2022).
285. В Московской области запустили производство высокоэффективных теплоизоляционных материалов из российского сырья [Электронный ресурс]. – URL: https://www.ruscable.ru/news/2019/10/28/V_Moskovskoj_oblasti_zapustili_proizvodstvo_vysoko/ (дата обращения: 14.12.2022).
286. В России создали самовосстанавливающийся полимер для дорожного покрытия [Электронный ресурс]. – URL: <https://nauka.tass.ru/nauka/15366785> (дата обращения: 14.12.2022).
287. Чудеса проводимости [Электронный ресурс]. – URL: <https://www.kommersant.ru/doc/4769633> (дата обращения: 14.12.2022).
288. Аддитивные технологии – что это такое и где применяются [Электронный ресурс]. – URL: https://old.sk.ru/news/b/press/archive/2019/09/18/additivnye-tehnologii-_1320_-chto-eto-takoe-i-gde-primenyayutsya.aspx (дата обращения: 14.12.2022).
289. Abhishek S.A. Comprehensive Study on 3D Printing Technology / S.A. Abhishek // MIT International Journal of Mechanical Engineering. – 2016. – Т. 6. – № 2. – С. 63-69.

290. Каталог аддитивного оборудования, производимого на территории Российской Федерации. – Минпромторг России, .
291. A Cloud-Based Cyber-Physical System with Industry 4.0: Remote and Digitized Additive Manufacturing / M.A. Rahman [et al.] // Automation. – 2022. – Vol. 3. – A Cloud-Based Cyber-Physical System with Industry 4.0. – № 3. – P. 400–425.
292. Promobot, Robo-C2 [Электронный ресурс]. – URL: <https://promo-bot.ru/production/robo-c/>.
293. Promobot, Promobot V.4 [Электронный ресурс]. – URL: <https://promo-bot.ru/production/promobot-v4/> (дата обращения: 14.12.2022).
294. Макро Групп, Разработки промышленных робототехнических решений [Электронный ресурс]. – URL: <https://solutions.macrogroup.ru> (дата обращения: 15.12.2022).
295. Горный-ЦОТ, Продукция [Электронный ресурс]. – URL: <http://indsafe.ru/products.html> (дата обращения: 15.12.2022).
296. Инспайр, Мы разрабатываем роботизированные комплексы — автоматизируем производственный процесс или целую производственную линию [Электронный ресурс]. – URL: <https://www.inspair.ru/services/business> (дата обращения: 15.12.2022).
297. Союз машиностроителей России, «Протон-ПМ» ввел в эксплуатацию автоматизированный комплекс термообработки [Электронный ресурс]. – URL: <https://soyuzmash.ru/news/companies-news/proton-pm-vvye-l-v-ekspluatatsiyu-avtomatizirovannyi-kompleks-termoobrabotki/> (дата обращения: 16.12.2022).
298. Video Matrix, Vmx Dequs [Электронный ресурс]. – URL: <https://videomatrix.ru/vmx-dequs/> (дата обращения: 15.12.2022).
299. NVI Research — разработчик наукоемких программных решений для цифровой трансформации. [Электронный ресурс]. – URL: <https://nvi-research.ru> (дата обращения: 15.12.2022).
300. Neelar, PEERS [Электронный ресурс]. – URL: <http://2020.openinnovations.ru/> (дата обращения: 15.12.2022).
301. Pawlin Technologies, Искусственный Интеллект для медоборудования [Электронный ресурс]. – URL: <https://www.pawlin.ru/uslugi> (дата обращения: 15.12.2022).
302. ЦАПК, Inventory Viewer 2.0 [Электронный ресурс]. – URL: <https://tsuru.su/project/iv/> (дата обращения: 15.12.2022).
303. Эттон: Цифровой двойник [Электронный ресурс]. – URL: <https://etton.ru/solution/cifrovoj-dvojnik> (дата обращения: 15.12.2022).
304. Эттон: Предиктивная аналитика ремонта [Электронный ресурс]. – URL: <https://etton.ru/solution/prediktivnaya-analitika-remonta> (дата обращения: 15.12.2022).
305. TerraTex, ATLAS VR [Электронный ресурс]. – URL: <https://terratech.ru/services/atlas-vr/> (дата обращения: 15.12.2022).
306. Video Matrix, Vmx Qualex [Электронный ресурс]. – URL: <https://videomatrix.ru/vmx-qualex/> (дата обращения: 15.12.2022).
307. Диспетчер, Надежный инструмент объективного контроля производства [Электронный ресурс]. – URL: <https://soyuzmash.ru/docs/prez/prez-klkp-060917-2.pdf>.
308. Intelligent Ideas, Digital Helmet [Электронный ресурс]. – URL: <https://intelligentideas.ru/portfolio-posts/digital-helmet/> (дата обращения: 15.12.2022).
309. iRidi lite — система управления (визуализация + сервер) для простых и типовых проектов автоматизации [Электронный ресурс]. – URL: <https://iridi.com/ru/lite/> (дата обращения: 15.12.2022).
310. MGBOT, Набор «Умная теплица ЙоТик М2 [Электронный ресурс]. – URL: https://mgbot.ru/catalog/obrazovatelnye_nabory_iot/nabor_umnaya_teplitsa_yotik_m2/ (дата обращения: 15.12.2022).
311. Реестр «НТИ 1000», ООО «НЕОХОУМ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/3906369480/> (дата обращения: 15.12.2022).

312. INFOWATCH, INFOWATCH TRAFFIC MONITOR [Электронный ресурс]. – URL: <https://www.infowatch.ru/products/traffic-monitor> (дата обращения: 15.12.2022).
313. INFOWATCH, INFOWATCH VISION [Электронный ресурс]. – URL: <https://www.infowatch.ru/products/vision> (дата обращения: 15.12.2022).
314. Реестр «НТИ 1000», ООО АЛАН-ИТ [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7606074282/> (дата обращения: 15.12.2022).
315. CSort Smart Cloud — платформа для повышения производительности сортировки [Электронный ресурс]. – URL: <https://csort.ru/csortcloud/> (дата обращения: 15.12.2022).
316. 7TECH, Проактивный мониторинг бизнес-сервисов [Электронный ресурс]. – URL: <https://solutions/proaktivnyy-monitoring-biznes-servisov/> (дата обращения: 15.12.2022).
317. Эттон: Прослеживаемость товаров и комплектующих [Электронный ресурс]. – URL: <https://etton.ru/solution/proslezhivayemost-tovarov> (дата обращения: 15.12.2022).
318. Geostron, Комплексные системы телематики [Электронный ресурс]. – URL: <https://geostron.ru/> (дата обращения: 15.12.2022).
319. ECOSOFT, Аналитика Больших данных [Электронный ресурс]. – URL: <https://ecosoft.pro/projects/sova/> (дата обращения: 15.12.2022).
320. Aura, LPWAN IoT-платформа АУРА [Электронный ресурс]. – URL: <https://aura365.tech/lpwan-iot/index.php> (дата обращения: 15.12.2022).
321. Реестр «НТИ 1000», ООО «ЦР» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/5905950880/> (дата обращения: 15.12.2022).
322. Реестр «НТИ 1000», ООО НИИ «УРАЛМЕТ [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7453273400/> (дата обращения: 15.12.2022).
323. Реестр «НТИ-1000», ООО «Образовательная робототехника» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7813502881/> (дата обращения: 15.12.2022).
324. Реестр «НТИ 1000», АО «НПО «АНДРОИДНАЯ ТЕХНИКА» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7723738378/> (дата обращения: 15.12.2022).
325. Реестр «НТИ 1000», ООО «А1» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7802639362/> (дата обращения: 15.12.2022).
326. Реестр «НТИ 1000», ООО «Диамант» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/5010048900/> (дата обращения: 15.12.2022).
327. Реестр «НТИ 1000», ООО «ПАВЛИН ТЕХНО» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/5010032762/> (дата обращения: 15.12.2022).
328. Реестр «НТИ 1000», ООО «ИНТЭК» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7017236286/> (дата обращения: 15.12.2022).
329. Реестр «НТИ 1000», ООО «НМТ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/9731032759/> (дата обращения: 15.12.2022).
330. Реестр «НТИ 1000», АО «ФЭСКОМ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/9731032759/> (дата обращения: 16.12.2022).
331. Реестр «НТИ 1000», ООО «ГАРПИКС» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/3702648341/> (дата обращения: 15.12.2022).
332. Реестр «НТИ 1000», ООО «ЭТТОН ГРУП» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/1615009497/> (дата обращения: 15.12.2022).
333. Реестр «НТИ 1000», ООО «СЕРВИССОФТ ИНЖИНИРИНГ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7610052644/> (дата обращения: 15.12.2022).
334. Реестр «НТИ 1000», ООО «СЛУЖБА МОНИТОРИНГА. ТЮМЕНЬ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7204160319/> (дата обращения: 15.12.2022).

335. Реестр «НТИ 1000», ООО «МОДУЛЬНЫЕ СИСТЕМЫ ТОРНАДО» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/5408005710/> (дата обращения: 15.12.2022).
336. Реестр «НТИ 1000», ООО «ДИЛИБРИУМ» [Электронный ресурс]. – URL: <https://nti1000.leader-id.ru/companies/7820306775/> (дата обращения: 15.12.2022).