ЭКСПРЕСС-ИНФОРМАЦИЯ

ЦИФРОВАЯ ЭКОНОМИКА

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Институт статистических исследований и экономики знаний

Дата выпуска
24.12.2024

DeepTech для экономики и общества: безопасность превыше всего

Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ изучил влияние кибербезопасности на рынок технологий диптеха (DeepTech) и их приоритетность для государственных и частных инвестиций.

Справочно: Под DeepTech понимают целый ряд наиболее наукоемких и капиталоемких направлений, в основе которых лежат результаты исследований, связанных с физическими элементами продукта, включая материалы, оборудование, аппаратное обеспечение, и нацеленных, как правило, на решение актуальных социально-экономических задач. Последующие разработка и коммерциализация результатов таких исследований требуют больше времени и ресурсов и сопряжены с большими рисками. Но и отдача от использования полученных решений, включая рост ВВП, повышение производительности труда, совокупной факторной производительности, кратно выше и дольше по периоду действия. В настоящем исследовании к диптеху отнесены квантовые технологии, фотоника, искусственный интеллект, робототехника, космические технологии, биотехнологии, новые материалы.

DeepTech как драйвер венчурного рынка

В середине 2010-х гг. драйвером венчурного рынка были цифровые технологии и сервисы (в большинстве своем софтверные), стремительно набиравшие популярность среди населения. В последние годы значимый вклад в развитие венчурного рынка стали вносить глубокие технологии (DeepTech). Согласно расчетам ИСИЭЗ НИУ ВШЭ по данным Crunchbase за 2020–2023 гг., всего по указанным направлениям в мире действуют порядка 32 тыс. технологических компаний и стартапов.

Мировой рынок технологий в целом претерпевает ряд кардинальных изменений, которые влияют на приоритеты инвесторов, а в последние несколько лет привели к снижению инвестиционной активности. В 2023 г. вложения в стартапы сократились почти на 40% от уровня предыдущего года и составили 285 млрд долл. (в 2022 г. – 462 млрд долл.). Эти тенденции продолжились и в текущем году: в третьем квартале рынок не смог выйти на уровень 70 млрд долл. (наименьший показатель с 2017 г.). Такой сдвиг вызван комплексом различных факторов, включая фрагментацию глобального рынка, замедление темпов экономического роста, снижение спроса, сокращение доступных финансовых ресурсов, ослабление в результате санкционной политики международных торгово-экономических институтов.

Среди очевидных драйверов развития рынка технологий в последние годы – стремление к созданию устойчивых промышленных экосистем, развитие новых транспортно-логистических маршрутов с минимальным антропогенным воздействием, а также физическая и цифровая безопасность на фоне острейших геополитических изменений. В I полугодии 2024 г. инвестиции в стартапы в области кибербеза как отдельную индустрию превысили 7 млрд долл. (более чем наполовину выше показателя за тот же период 2023 г.). Несмотря на снижение числа финансируемых проектов, вложения в них наращивают как западные игроки, так и представители БРИКС+.

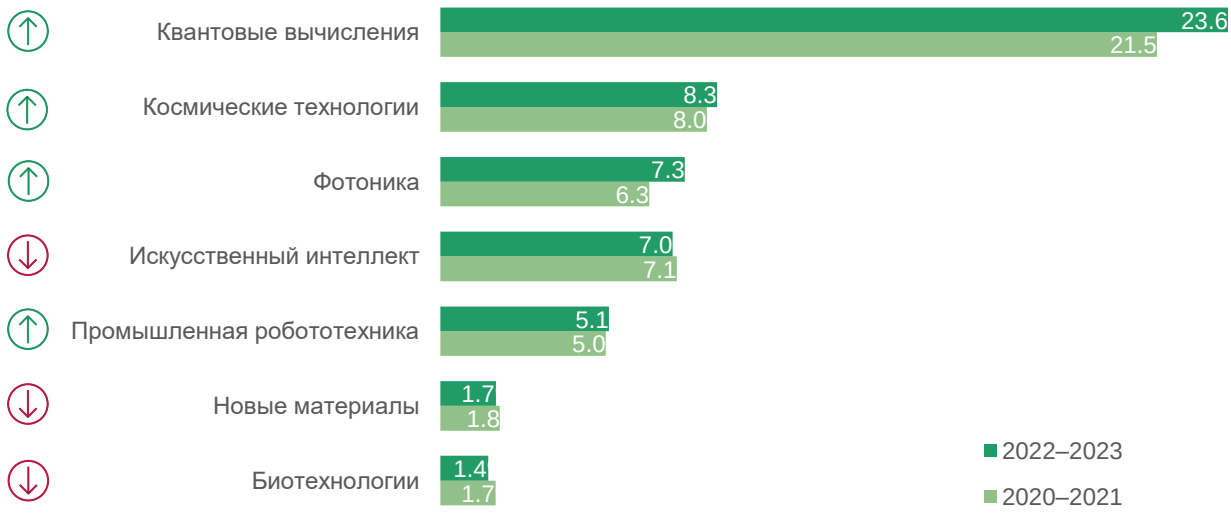
Справочно: Летом 2024 г. сорвалась самая крупная в истории Google сделка на 23 млрд долл. по покупке единорога в сфере облачной кибербезопасности Wiz (основан выпускниками элитного израильского подразделения радиотехнической разведки). В 2022 г. Google уже приобрел крупную киберкомпанию Mandiant за 5.4 млрд долл. В Индии под эгидой министерства информационных технологий действуют центр превосходства и инкубатор, среди задач которого – развитие национальной экосистемы кибербеза и поддержка собственных стартапов в этой области. В КНР реализуется еще более масштабная государственно-частная инициатива такого рода: Национальный центр кибербезопасности Китая в Ухане включает частные и государственные лаборатории, центр подготовки специалистов, Национальную школу кибербезопасности (2.5 тыс. выпускников ежегодно), а также инкубатор, насчитывающий 200 стартапов. Все они получают помощь не только для коммерциализации исследований, но и на протяжении всего жизненного цикла компании.

Безопасность в DeepTech

Тематика цифровой безопасности сквозным образом «зашита» в технологиях диптеха. В 2022–2023 гг. более 5% всех диптех-компаний так или иначе разрабатывали решения в этой области, в области **квантовых технологий** – почти каждая четвертая компания (23.6% в 2022–2023 гг.) (рис. 1). Появление квантовых компьютеров с огромными вычислительными мощностями кардинально изменит архитектуру цифровых коммуникаций: так, практически любое зашифрованное с помощью текущих средств сообщение может быть моментально раскодировано. Многие ведущие организации в различных странах, включая финансовые и государственные учреждения, уже начали модернизировать свою цифровую инфраструктуру и в инициативном порядке разрабатывают новые виды защиты данных с помощью протоколов квантовой и постквантовой криптографии (*см. подробнее о технологиях квантовой связи*).

Справочно: Летом 2024 г. первые стандарты постквантового шифрования представил Национальный институт стандартов и технологий США (NIST), призвав организации переходить на них в ускоренном порядке. Отбор алгоритмов для них начат еще в 2015 г. в сотрудничестве с бизнесом и международными партнерами: из 85 решений, предложенных Radical Semiconductor (США), PQShield (Великобритания) и другими компаниями, были выбраны 15 лучших алгоритмов, которые далее применили в ходе отработки процессов миграции на постквантовую криптографию. В эксперименте приняли участие 12 игроков из сектора ИТ, телекома, обороны США (Amazon Web Services, Microsoft, Cisco Systems, VMware, Thales DIS CPL USA и др.).

Рис. 1. Доля компаний в мире, связанных с разработками в области кибербезопасности, по сегментам диптеха, %



Источник: расчеты ИСИЭЗ НИУ ВШЭ на основе данных Crunchbase.

Методологический комментарий: Для определения количества компаний в базе данных Crunchbase взяты два периода финансирования: 01.01.2020 – 31.12.2021 и 01.01.2022 – 31.12.2023 гг. Число организаций по каждому из семи направлений (квантовые технологии, фотоника, космические технологии, ИИ, робототехника, новые материалы, биотехнологии) определялось в соответствии с заданным в базе классификатором индустрий, за исключением фотоники (сформировано на основе ключевых слов). Далее поиск внутри отдельного направления ограничивался с помощью единого набора ключевых слов, характеризующих область кибербезопасности. Устранены повторы одной и той же организации при сопоставлении результатов поиска по разным ключевым словам.

С квантовыми технологиями тесно связана **фотоника**. Специализирующиеся в области фотоники компании занимают **3-е место** с долей в 2022–2023 гг. более 7% среди организаций диптеха, развивающих решения для кибербезопасности.

Справочно: Относительно новый инструмент – фотонные нейросети, в реальном времени проверяющие трафик с целью обнаружения DDoS-атак (типа «отказ в обслуживании», когда злоумышленники перегружают страницу запросами, что делает невозможным обработку запросов от настоящих пользователей). Перспективное применение фотоники для кибербезопасности – гомоморфное шифрование, при котором зашифрованные данные обрабатываются без их расшифровки, что позволяет сохранить конфиденциальность самих данных в процессе их передачи. Для обеспечения полностью гомоморфного шифрования используется, например, недавно интегрированная в инструменты Google технология фотонной обработки.

Космические технологии занимают **2-ю позицию** по доле технологических компаний, связанных с задачами кибербезопасности (8.3% в 2022–2023 гг.). Круг игроков космической индустрии в последние годы существенно расширился благодаря удешевлению технологий и повышению их доступности. Это привело к обострению конкуренции, появлению новых продуктов и сервисов, объектов на орбите Земли и вместе с тем – к росту числа физических и цифровых угроз. Крупные компании в области авиационного и космического машиностроения (для гражданских и оборонных задач) рассматривают кибербезопасность как перспективное направление для диверсификации своей деятельности, которое в ближайшие годы будет расти высокими темпами. Так, собственные компетенции в этой области намерен развивать авиастроительный концерн Airbus, который для этого в 2024 г. приобрел немецкого вендора Infodas. Итальянская компания Leonardo планирует укрепить позиции в сфере кибербеза путем приобретения профильных компаний-разработчиков.

Справочно: Первый зафиксированный кибериндидент со взломом системы спутника датируется 1986 г.: в результате атаки была нарушена работа одного из крупнейших американских телеканалов HBO. Из числа недавних кейсов – экспериментальная атака на внутреннюю сеть SpaceX. С помощью сбоя напряжения и самодельного чипа стоимостью 25 долл. была практически продемонстрирована уязвимость спутников Starlink перед киберугрозами. После инцидента был запущен проект по поиску ошибок в системе за денежное вознаграждение. Национальный институт стандартов и технологий США (NIST) выпустил в 2023 г. доклад-справочник по управлению рисками кибербезопасности коммерческих спутников.

Искусственный интеллект – лидер среди направлений DeepTech (более 17.5 тыс. в 2020–2023 гг., по данным Crunchbase), при этом доля связанных с кибербезопасностью технологических компаний составляет 7%. Это значение в силу методологических ограничений на практике может оказаться выше: ИИ-решения все чаще применяются для защиты ИКТ-инфраструктуры, в то же время сами ИИ-решения нуждаются в защите на протяжении всего своего жизненного цикла.

Разработками в области кибербезопасности в 2022–2023 гг. занимались более 5% компаний **промышленной робототехники**. Они сталкиваются с серьезными вызовами в свете все более массового характера роботизации, необходимости обеспечить безопасную работу с физическими объектами, сложным и нередко опасным для человека механическим инструментарием. Даже в тех процессах, где человек лишь контролирует робота и не работает рядом с ним (т. е. исключается возможность нанесения вреда здоровью и жизни человека), кибератака может привести к остановке всей производственной линии, выходу из строя других систем и оборудования и в конечном итоге – финансовым и репутационным потерям от срыва заказов. На защищенность работы с роботами влияет еще целый ряд факторов, включая «стык» между физической и цифровой средами, адаптацию роботов под специфику отдельного предприятия-пользователя, уровень автоматизации процессов. А главная проблема состоит в том, что развитие инструментария кибербезопасности промышленных роботов не успевает за темпами их внедрения. Все это кратно повышает риски для пользователей, масштабы и ущерб от кибератак. Дальнейший тренд на создание мультифункциональных, гибких, способных адаптироваться под разные задачи роботов потребует еще более сложных инструментов их цифровой и физической защиты.

Справочно: Ключевые инструменты защиты роботизированных систем строятся по принципу нулевого доверия (Zero Trust), т. е. отсутствия доверия к пользователям на всех этапах работы при выполнении любой операции, что требует аутентификации и авторизации для получения доступа к каждому отдельному ресурсу или устройству, а также перепроверки статуса прав доступа в ходе работы. Все чаще задействуют ИИ-решения, позволяющие мониторить и фиксировать в режиме реального времени аномальные характеристики работы робота.

Комментирует Юлия Туровец, заведующий отделом исследований цифровых технологий Института статистических исследований и экономики знаний НИУ ВШЭ:

Ранее успех проектов, особенно в области цифровых технологий, доминировавших среди предпочтений инвесторов, измеряли в скорости распространения нового продукта, которая стремительно сокращалась. Однако темпы внедрения не всегда говорят о востребованности или трансформационном потенциале новшества. К примеру, сервис ChatGPT после запуска в ноябре 2022 г. за пять дней привлек более 100 млн пользователей (на данный момент – рекордное время привлечения пользовательской аудитории). Но уже через пару лет его популярность начала снижаться: к осени 2024 г. показатель вернулся на исходные позиции в 133 млн пользователей (при 1.8 млрд посещений весной текущего года). В случае сетей связи 5G количество подключений к ним лишь к концу 2023 г. превысило 1.5 млрд, т.е. спустя четыре года после появления. Большинство глубоких технологий требуют времени на разработку и апробацию, развитие инфраструктуры, адаптацию решений и потребителей, но спустя время приносят больший выигрыш для экономики.

До конца десятилетия и далее диптех-направления останутся ключевым приоритетом для стран и компаний, при этом государство сохранит статус крупнейшего инвестора. В мире из топ-100 перспективных стартапов почти треть получают поддержку от различных государственных институтов. При этом чаще всего она реализуется в форме постоянных программ. Но и для частного капитала глубокие технологии обеспечивают долгосрочные выгоды: при значительных инвестициях (100 млн долл. и более) проекты диптеха показывают большую норму доходности и меньше подвержены колебаниям при смене инвестиционных циклов. Многие венчурные фонды перестраиваются под специфику этих направлений, увеличивая срок окупаемости своих проектов до семи-десяти лет.

Кибербезопасность – намного более широкое понятие. Сегодня сложно провести четкую границу между цифровой и физической средой: защищенность цифровых систем напрямую влияет на безопасность людей, промышленных, инфраструктурных и иных объектов. Цифровой компонент встроен практически во все современные высокотехнологичные решения. С этой позиции актуальная для России задача по роботизации промышленности должна сопровождаться обеспечением аппаратной и программной безопасности еще на этапе проектирования отечественных решений, в диалоге между пользователями, разработчиками и производителями.

Источники: результаты проекта «Определение технологических приоритетов в период глобальных трансформаций» тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ на 2024 год; результаты проекта «Экспертно-аналитическое сопровождение деятельности по развитию высокотехнологичных направлений в 2024 г., включая подготовку ежегодного доклада ("белой книги") о развитии отдельных высокотехнологичных направлений» тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ.

■ Материал подготовили **А. И. Фокина, Ю. В. Туровец**