ФИНТЕХ
— РАДАР

ФИНТЕХ АССОЦИАЦИЯ

ТЕХНОЛОГИИ ГОДА

Целью финтех-радара является обзор актуальных технологий и новых трендов финтеха

По вопросам радара и с обратной связью, пожалуйста, обращайтесь к команде исследований и аналитики Ассоциации ФинТех

research.analytics@fintechru.org

АССОЦИАЦИЯ ФИНТЕХ ИНФОРМАЦИОННЫЕ СЕРВИСЫ

В рамках трека «Информационный сервис» аналитики Ассоциации ФинТех реализуют следующие проекты:

1 **«Дайджест зарубежных СМИ»** – сбор актуальных новостей и обзор событий в области финансовых технологий на еженедельной основе по 7 основным направлениям:
- Блокчейн и криптоактивы,
- Платежи,
- Open Finance,
- Биометрия,
- Облачные сервисы,
- CBDC,
- Технологии,
- «Эхо финтеха» - резонансные новости по общей финтех-тематике.

2 **Финтех-радар** – периодический информацион--ный материал, целью которого является информирование таргетной аудитории об актуальных событиях в области технологий, зарождающихся трендах для принятия оперативных решений. Материал состоит из инсайтов Управления исследований и аналитики Ассоциации ФинТех, описания технологии месяца, дополнительных материалов по теме выпуска, а также дайджеста ключевых технологических событий.

МАРИАННА ДАНИЛИНА

Руководитель Управления исследований и аналитики

Опыт более 15 лет в финансовом секторе и консалтинге Big4. Профессиональный фокус на корпоративной стратегии, операционной эффективности, IT и цифровой трансформации.

Окончила МГУ имени М.В.Ломоносова и бизнес-школу Colorado Heights University (MBA)

m.danilina@fintechru.org

ДАРЬЯ ПЕТРОВА

Ведущий бизнес-аналитик по исследовательской деятельности

Ведущий бизнес-аналитик по исследовательской деятельности. Специализируется на метавселенных, CBDC, цифровой идентификации и трендах в криптовалютах.

Окончила Northumbria University (бакалавр) и Frankfurt School of Finance & Management (магистратура).

d.petrova@fintechru.org

ГРИГОРИЙ КАРУНАС

Бизнес-аналитик по информационным сервисам

Специализируется на машинном обучении, искусственном интеллекте, безопасной разработке и токенизированных активах.

Окончил МГТУ им. Н.Э. Баумана (бакалавр).

g.karunas@fintechru.org

О РАДАРЕ

Финтех-радар – периодический информационный продукт, направленный на обеспечение целевой аудитории актуальной информацией о трендах с фокусом на технологиях в финансовой сфере.

GPT-4
выпуск №1

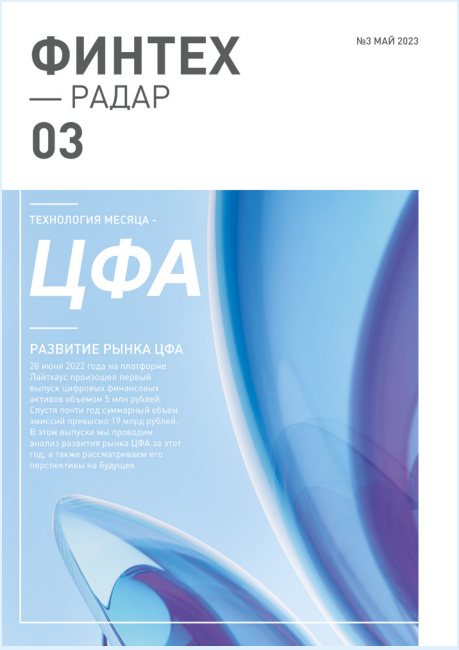
март 2023

Выпуск посвящен большим языковым моделям, в частности функциональным аспектам нашумевшей технологии GPT-4.

Федеративное обучение
выпуск №2

апрель 2023

Выпуск посвящен федеративному обучению – подходу к обучению систем ИИ, позволяющему проводить обучение одновременно на большом количестве децентрализованных источников данных без необходимости передавать их в централизованное хранилище.



ЦФА
выпуск №3

май 2023

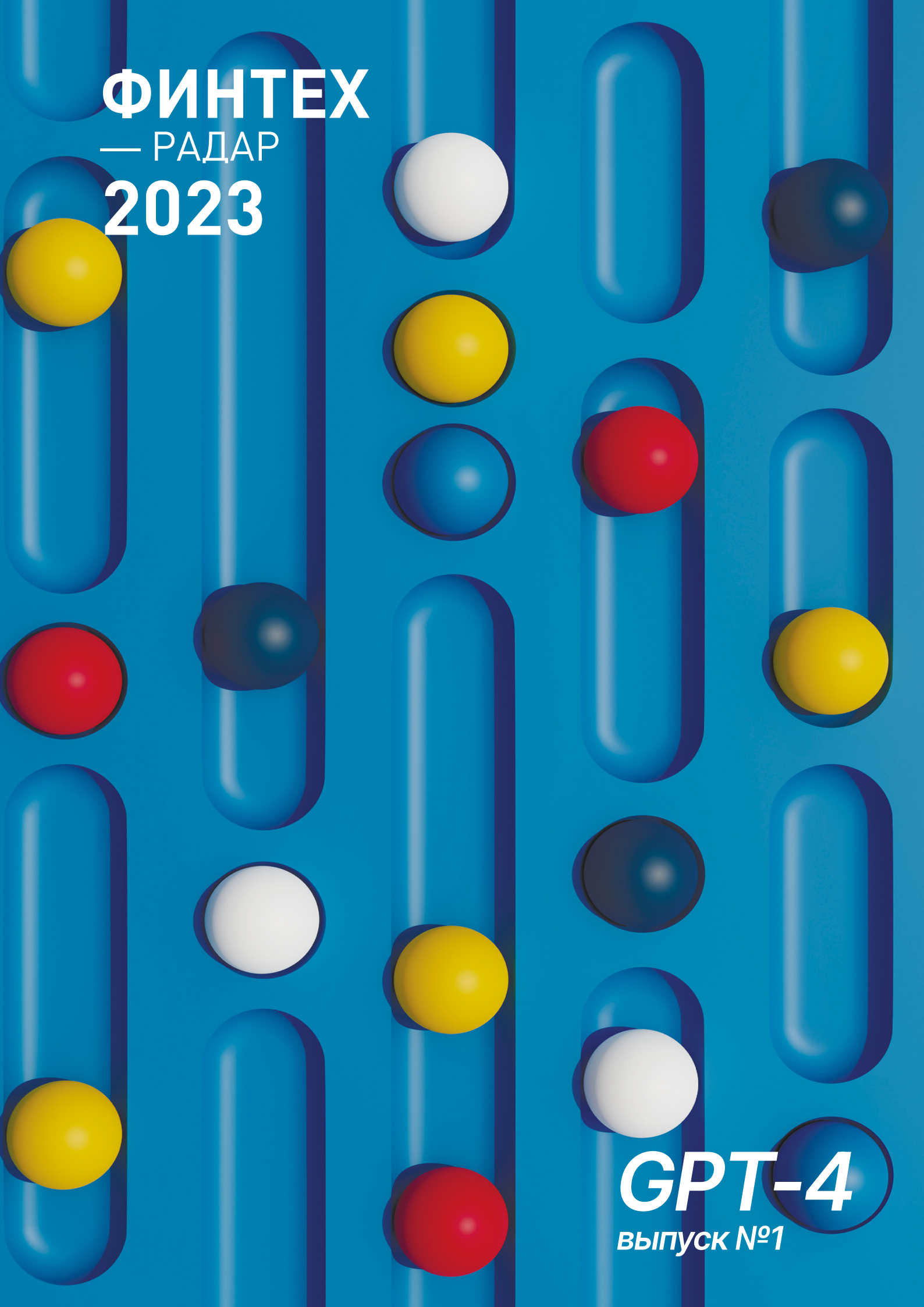
Выпуск посвящен цифровым финансовым активам и дальнейшим перспективам развития рынка ЦФА.

DevSecOps
выпуск №4

июль 2023

Выпуск посвящен безопасной разработке и решениям с открытым исходным кодом, а также обеспечению долгосрочного безопасного развития корпоративных ИТ-решений.

ФИНТЕХ
— РАДАР
2023



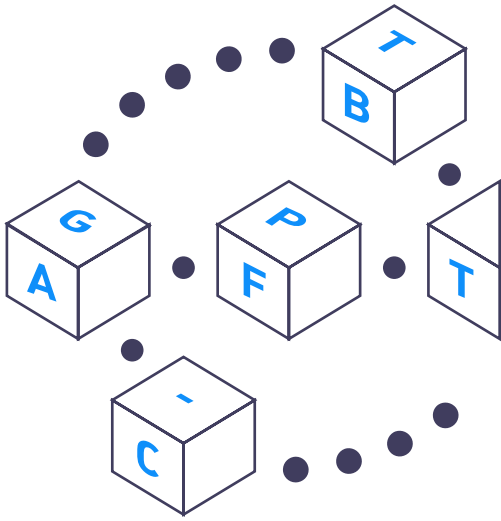
GPT-4

выпуск №1

Генеративные предобученные трансформеры

Данные в статье актуальны на март 2023 года

GPT-4 Generative Pre-trained Transformer 4



GPT-4 — (Generative Pre-trained Transformer 4) — это большая мультимодальная языковая модель компании OpenAI, которая генерирует текст на основе текстового фрагмента, введенного пользователем, или предложенного графического объекта. GPT-4 может решать более сложные задачи, чем предыдущие модели GPT. Она демонстрирует результаты на уровне человека во многих профессиональных и академических местах, включая международные олимпиады по биологии.

ПОЯВЛЕНИЕ И ЭВОЛЮЦИЯ ТЕХНОЛОГИИ

GPT-4 – технология, которую ученые приписывают к «языковым моделям» (Language Models). На самом деле, упрощенно, их основной функционал – угадывать, какое следующее слово должно идти за уже имеющимся текстом. Современные модели гораздо больше предшественников. Под большими моделями (Large Language Models, LLM) понимаются модели, имеющие огромное количество параметров, на сегодняшний день речь идет о сотнях миллиардов.

Как ранее было сказано, GPT расшифровывается как Generative Pre-trained Transformer, или «генеративный предобученный трансформер». Трансформер – это разработанный Google в 2017 году тип нейросетей[1], направленный на создание последовательностей с эффективной обработкой взаимосвязей между отдельными элементами. Например, словами в тексте. На сегодня это самая продвинутая техника в области обработки естественного языка (NLP).

Прорыв состоял в том, что был создан алгоритм, в котором не использовались привычные сверточные (CNN) и рекуррентные (RNN) нейронные сети, справлявшиеся с задачами лучше, чем иные решения на тот момент. Это достигается радикальным использованием «механизма внимания», который определяет, какая часть данных важнее другой, в зависимости от контекста. Взаимосвязи находятся не только среди введенных данных, но и среди тех, которые создает трансформер. Профессиональное сообщество оценило то, насколько хорошо передается информация между многочисленными этапами работы и функциональными блоками в архитектуре модели, насколько легко ее оптимизировать под конкретные задачи и насколько она эффективна в сравнении с аналогами.

Трансформеры до того легко масштабируются и универсальны, что во всех областях искусственного интеллекта начали активно их адаптировать и применять – от обработки текстов и изображений до звуков и видео, а также понимания устройства мира. Модель GPT-1, основанная на архитектуре трансформера, была выпущена в 2018 году и доказала, что нейросеть может генерировать тексты. У GPT-1 было 117 млн параметров. В 2019 году была выпущена модель GPT-2, которая превосходила предшественника по объему тренировочных данных и была в объеме больше в 10 раз (1,5 млрд параметров). К тому же она обучалась качественно новым навыкам, таким как написание связных эссе и решение сложных задач, требующих понимания устройства мира.

GPT-3 образца 2020 года была в 100 раз больше GPT-2 по количеству параметров (175 млрд) и в 10 раз – по объему тренировочных данных. Рост снова привел к значительному скачку в качестве: модель стала еще более универсальной, научилась переводу с других языков, арифметике, базовому программированию, пошаговым рассуждениям и прочим навыкам.

[1]Искусственная нейронная сеть — математическая модель, а также ее программные или аппаратные реализации, построенная в некотором смысле по образу сетей нервных клеток живого организма.

В ноябре 2022 года OpenAI сделала еще один интересный шаг: запустила чат-бот, позволяющий общаться с ИИ на основе GPT-3 – ChatGPT. Это стало очередным прорывом в развитии и популяризации технологии. С технической точки зрения значительных нововведений не проводилось. Однако появились удобный интерфейс взаимодействия и открытый публичный доступ. 23 марта OpenAI добавила поддержку плагинов для ChatGPT — расширений, которые интегрируют его со сторонними сервисами и позволяют получать доступ к актуальной информации. К примеру, добавили расширение Wolfram, которое позволяет пользоваться вычислительным, математическим и аналитическим функционалом Wolfram|Alpha в реальном времени.

14 марта 2023 года вышла модель GPT-4. На данный момент она уже подключена к ChatGPT. OpenAI не раскрывает количество параметров в этой итерации. Как утверждают разработчики, она может принимать на вход изображения и текст, работает на «уровне компетенций человека» в различных профессиональных и академических тестах. Так, на экзаменах Uniform Bar Exam, LSAT, SAT Math и SAT Evidence-Based Reading & Writing GPT-4 входит в топ-10% сдавших экзамены.

OpenAI в анонсе технологии отмечает, что при обычном диалоге разница между GPT-4 и предыдущими моделями может быть едва уловимой. Разница проявляется, когда сложность задачи достигает достаточного порога — GPT-4 более надежен, креативен и способен обрабатывать гораздо более тонкие инструкции.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ

На март 2023 года всеобщего открытого доступа к GPT-4 нет, потому стоит переключиться на применение технологий, которые можно использовать уже сейчас, а именно ChatGPT.

ChatGPT способен выполнять следующий набор действий:
- генерировать и помогать улучшать разработку текстов и кода,
- резюмировать текст,
- классифицировать контент,
- отвечать на вопросы,
- переводить и преобразовывать язык (включая языки программирования).

Существует четыре основных способа применения технологии ChatGPT:
1. Как есть (AS-IS): ввод запросов и получение результатов через веб-интерфейс.
На сегодняшний день это наиболее популярный подход.
2. Инжиниринг запросов без API[1]: инжиниринг запросов – это использование сервиса, подобного ChatGPT, в сочетании с другими технологиями, как часть рабочего процесса. Этот рабочий процесс возможно создать вручную или с помощью технологий экранного скрейпинга и роботизированной автоматизации процессов (RPA).
3. Проектирование с использованием API: Используя API, можно напрямую общаться с технологией и более свободно использовать ее широкий функционал. К тому же только таким образом можно легально использовать ChatGPT в собственных приложениях. OpenAI дает возможность пользоваться API по тарифу $0,002 за 1 тыс. токенов[2].
4. Пользовательская сборка: существует возможность под собственные нужды собрать новую генеративную модель, использующую GPT-3, GPT-2, их модификации или аналоги. Однако это будет уже не ChatGPT, поэтому будет теряться фильтрация запросов, взаимодействие с собеседником и другие полезные функции.

Ассоциация ФинТех подготовила аналитическую справку по технологии GPT, и этот материал был создан с помощью самой технологии.

ИИ рассказал о себе сам.

[1]API – Application Programming Interface, что значит программный интерфейс приложения. Интерфейс можно рассматривать как сервисный контракт между двумя приложениями. Этот контракт определяет, как они взаимодействуют друг с другом, используя запросы и ответы.

[2]Токены можно представить как фрагменты слов, прошедшие кодировку. Количество токенов, созданных для англоязычного текста, значительно меньше, чем для текстов на иных языках. Например, из «Ассоциация ФинТех» создастся 22 токена, а из «FinTech Association» - только 3. Таким образом, обработка названия организации на русском выйдет в 7 раз дороже, чем на английском.

КАКОВЫ ТЕКУЩИЕ ОГРАНИЧЕНИЯ GPT-4?

• Нет гарантий конфиденциальности данных.
• Модель не может генерировать изображения, но в будущем технологию можно будет использовать в сочетании с визуальными генеративными моделями искусственного интеллекта.
• Полноценные протоколы безопасности в отношении ИИ еще не выработаны и не стандартизированы.

ВЛИЯНИЕ ТЕХНОЛОГИИ НА ОБЩЕСТВО

Согласно совместному исследованию OpenAI и экспертов Университета Пенсильвании (GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models), большие языковые модели, вроде GPT, могут затронуть до 80% рабочей силы в США, а 19% работников рискуют потерять от 50% рабочих задач. Из наиболее уязвимых профессий выделяются следующие: писатели, веб-дизайнеры, финансовые аналитики и ИТ-разработчики.

В отличие от предыдущих волн автоматизации, больше всего могут пострадать профессии с высоким уровнем дохода. Если применение технологий LLM и, в частности, GPT-4 будет направлено только на автоматизацию труда и замещение людей, это будет приводить к еще более сильной концентрации власти, богатства и ресурсов. У людей, которые на данный момент ими не обладают, не будет адекватной возможности улучшать свои результаты. Такой феномен Эрик Бринолфссон в статье «The Turing Trap: The Promise & Peril of Human-Like Artificial Intelligence» называет «ловушкой Тьюринга».

Есть и более благоприятный сценарий развития событий: ИИ чат-боты станут мощными инструментами для работников, дополняющими или «аугментирующими» человеческую деятельность. С их помощью сотрудники компаний приобретут новые навыки и повысят собственную квалификацию. Этот феномен даст толчок развитию экономики в целом. Но данный сценарий предполагает целенаправленное усилие общества и государства на смену фокуса с автоматизации на аугментацию.

Опасения вокруг рынка труда вкупе с непроработанными протоколами безопасности в отношении ИИ вылились в петицию под названием «Приостановить гигантские эксперименты с искусственным интеллектом: открытое письмо», в которой содержится призыв приостановить как минимум на полгода обучение различных передовых систем ИИ. Обращение подписали Илон Маск, Стив Возняк и ещё около 3000 экспертов в области ИИ.

ИНЫЕ ЯЗЫКОВЫЕ МОДЕЛИ[1]

Все модели GPT были созданы компанией OpenAI. Существуют и другие большие языковые модели, которые активно развивают мировые технологические лидеры. Так, помимо анонса GPT-4 14 марта, компания Google открыла сторонним разработчикам доступ к API нейросети PaLM.

В конце февраля 2023 компания Meta (организация запрещена на территории РФ) представила модель LLaMA. Как пишет The Verge, LLaMA представляет собой не единую систему, а «квартет моделей» разного размера, которые будут доступны по некоммерческой лицензии, «ориентированной на исследовательские варианты использования». Аудитория пользователей — это университеты, НПО и отраслевые лаборатории.

Наиболее значимая для индустрии российская большая языковая модель на данный момент — YaLM от «Яндекса» на 100 млрд параметров. Сейчас разрабатывается YaLM 2.0 — новая версия генеративной сети. Предполагается, что она станет частью «Поиска», «Алисы», «Почты» и других сервисов компании. «Яндекс» уже частично использует генеративные нейронные сети при формировании поисковой выдачи, но сейчас у них скорее вспомогательная роль — они помогают сориентироваться, но не генерируют связные ответы.

Также Sber Cloud разработал собственную большую языковую модель ruGPT-3. На данный момент самая крупная ее версия ruGPT-3 XL имеет 1.3 млрд параметров.

[1]Данные в статье актуальны на март 2023 года.

ЧТО ДЕЛАТЬ ДАЛЬШЕ?

Действовать разумно. Проект находится на очень ранней стадии и многое из того, что появляется в публичном пространстве, может оказаться субъективным мнением отдельного человека. Тем не менее, потенциал технологии значителен.

Изучить другие виды генеративного ИИ. Не стоит ограничиваться только моделями, генерирующими текст.

Экспериментировать. Необходимо изучить существующие угрозы и возможности этой технологии, составить дорожную карту для их выявления для конкретной компании, определить необходимые навыки и требуемые инвестиции.

ЗАКЛЮЧЕНИЕ

Искусственный интеллект уже заведомо включили в список потенциальных технологий общего назначения (general purpose technology), способных стать причиной технологической революции, радикально изменить общество и технологические уклады благодаря своему воздействию на существующие экономические и социальные структуры. К таким, например, относят паровой двигатель, электричество и компьютер.

С появлением GPT-4 и других современных LLM общественности стало понятно, что искусственный интеллект в каждом доме и устройстве – не только плод воображения писателей-фантастов, но довольно реалистичный сценарий развития человечества. Следить за этим со стороны – идея не лучшая, в адаптации к потенциальным радикальным изменениям необходимо принимать активное участие.

ПОЧИТАТЬ ДОПОЛНИТЕЛЬНО ПО ТЕМЕ:

BCG:

Руководство CEO относительно революции в области генеративного ИИ

IOT ANALYTICS:

Отчет о тенденциях в области генеративного ИИ: общие сведения,тенденции , кейсы и возможные сценарии использования

GARTNER:

Помимо ChatGPT: Будущее генеративного ИИ для бизнеса. Кейсы, риски, иные технологии.

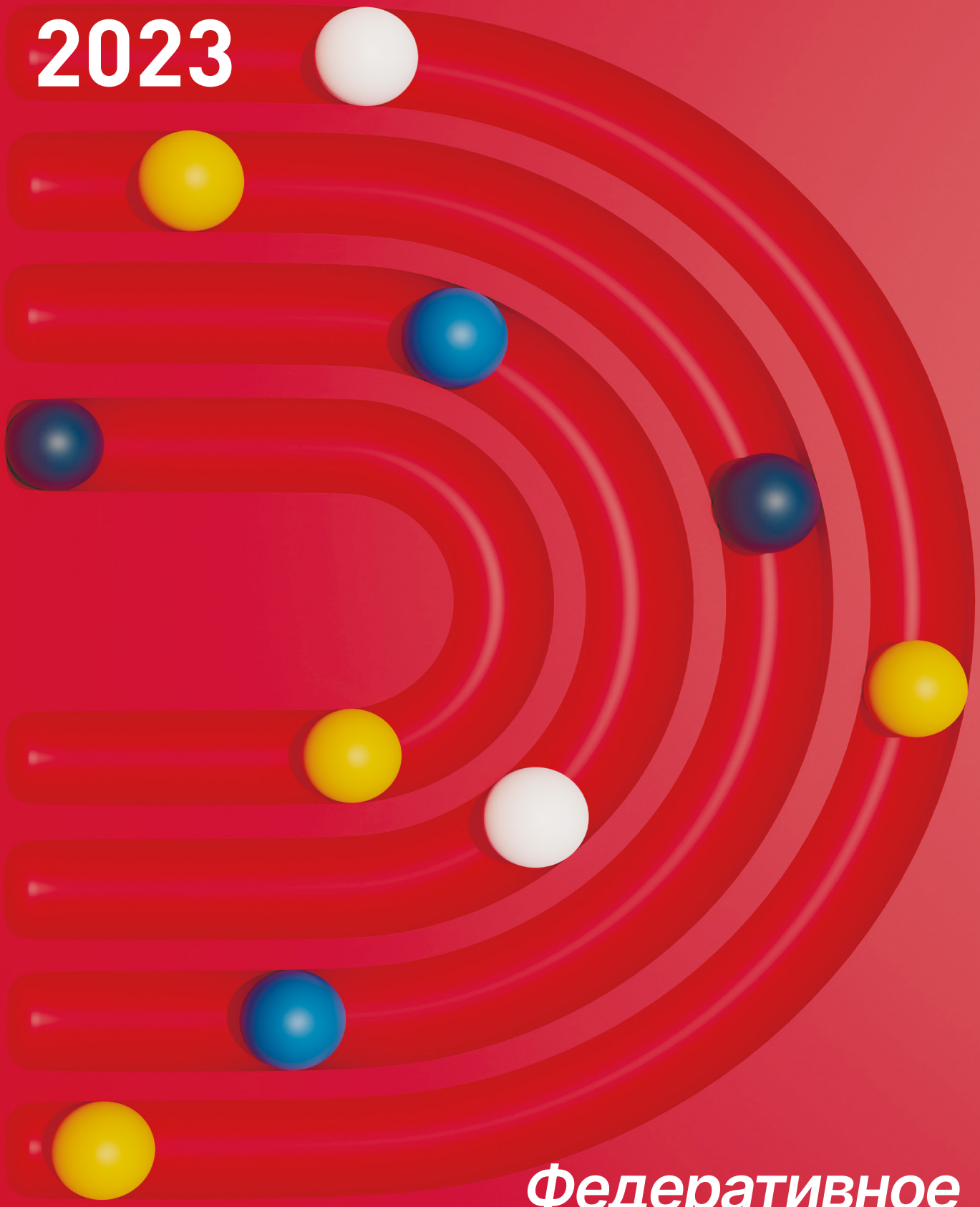
MCKINSEY:

Генеративный искусственный интеллект уже здесь: как такие инструменты, как ChatGPT, могут изменить ваш бизнес

ЭРИК БРИНОЛФССОН

Ловушка Тьюринга: Перспективы и угрозы развития человекоподобного ИИ

ФИНТЕХ
— РАДАР
2023



Федеративное обучение

выпуск №2

Федеративное обучение

Данные в статье актуальны на апрель 2023 года

Одна из ключевых проблем, с которыми сталкиваются компании в процессе широкого внедрения технологий искусственного интеллекта, это вопрос обеспечения конфиденциальных данных. Проблема заключается в том, что при передаче данных на центральный сервер они могут быть скомпрометированы или украдены злоумышленниками. Это может привести к серьезным последствиям, таким как утечка личной информации клиентов или риск финансовых потерь. Кроме того, некоторые данные могут быть чувствительными и требуют особой защиты, например, медицинские данные или данные о финансовых операциях. Раскрытие такой информации может привести к нарушению закона или этических норм, а также к серьезным последствиям для людей, чьи данные были скомпрометированы. Для решения этой проблемы используется технология федеративного обучения.

Федеративное обучение – это подход к обучению систем ИИ, который позволяет проводить его одновременно на большом количестве децентрализованных источников данных, к примеру на смартфонах или ноутбуках, без необходимости передачи данных в централизованное хранилище.

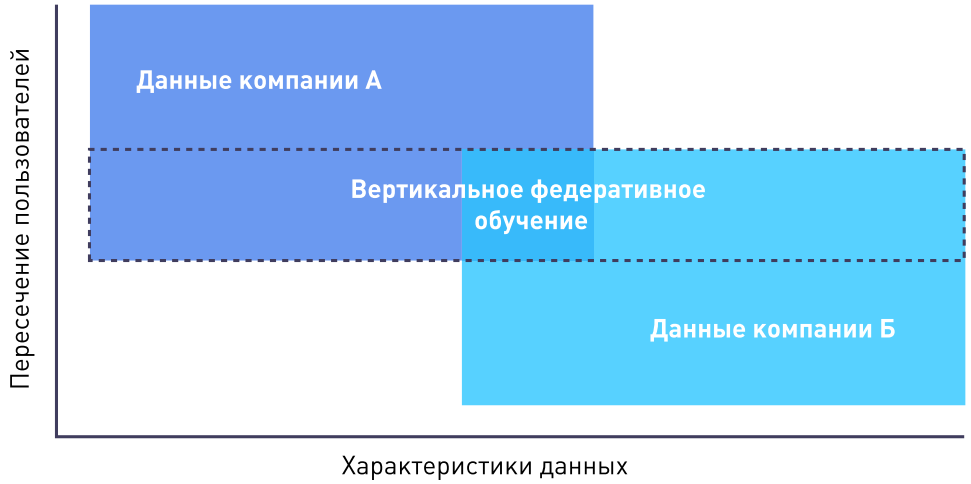
Федеративное обучение позволяет обрабатывать конфиденциальную информацию в соответствии с законодательными нормами по защите данных и обеспечению приватности пользователей, т. к. информация в процессе обработки не передается третьим лицам. Кроме того, эта технология позволяет использовать необработанные данные, поступающие от датчиков на спутниках, мостах, машинах и растущем числе умных устройств в рамках Интернета вещей (IoT) за счет того, что их обработка может происходить непосредственно на конечном устройстве.

ПРИНЦИП РАБОТЫ

При федеративном обучении несколько сторон удаленно участвуют в обучении одной модели, последовательно ее совершенствуя, подобно совместной презентации или докладу.

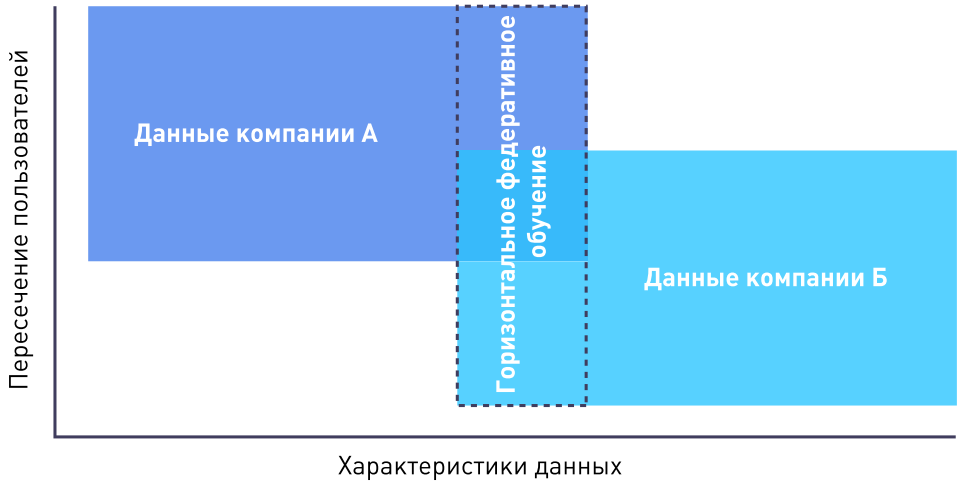
Принцип работы федеративного обучения

Отличия в подходах к федеративному обучению заключаются в том, по каким именно данным происходит пересечение между участниками процесса. Так, между сторонами могут быть данные об одних и тех же сущностях (например, физических и юридических лицах), но разные по структуре. Рассмотрим две компании в одном городе, одна из которых банк, а другая – маркетплейс с доставкой на дом. Пересечение по пользователям у двух организаций значительное. Однако банк регистрирует доходы, расходы и кредитную историю клиентов, а маркетплейс хранит просмотренные товары и покупки пользователя – параметры их данных сильно отличаются. В этом случае применяется вертикальное федеративное обучение (VFL) для объединения различных параметров с сохранением конфиденциальности. Таким образом, чем более детализированной является информация, тем точнее будут прогнозы модели.



Вертикальное федеративное обучение

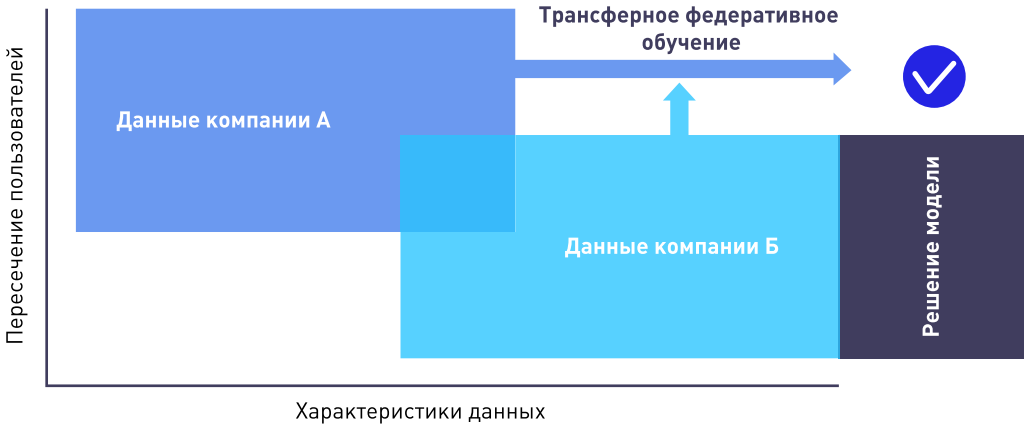
При горизонтальном федеративном обучении (HFL) модель тренируется на аналогичных наборах данных. Например, банки в Москве и в Тюмени предлагают аналогичные финансовые услуги, но имеют непересекающиеся группы пользователей из-за разницы в местоположении.



Горизонтальное федеративное обучение

Характеристики данных почти идентичны, а пересечение пользователей незначительно. В этом случае каждый банк обучает модели на своем объеме данных и на выходе получается модель, обученная на объеме данных двух или более организаций.

Трансферное федеративное обучение (FTL) подходит в случаях, когда у сторон почти нет пересекающихся пользователей, поскольку они работают в разных доменах и регионах.



Трансферное федеративное обучение

Данный тип федеративного обучения заполняет недостающие метки из предварительно обученной модели, чтобы расширить масштаб доступных данных и, по сути, представляет собой комбинацию вертикального и горизонтального обучений.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

«Согласно совместному исследованию группы пакистанских и корейских ученых Applications of Federated Learning; Taxonomy, Challenges, and Research Trends[1], наибольшая доля исследований, в которых реализуется федеративное обучение, зафиксирована в области здравоохранения (30%). За ними следуют исследования по Интернету вещей (IoT) и периферийным вычислениям (edge computing) – 25%. На исследования по обработке естественного языка (NLP), автономным транспортным средствам, мобильным сервисам и рекомендательным системам пришлось 10%. 5% исследований посвящены финтеху».

Денис Афанасьев,
Эксперт по искусственному интеллекту
и работе с данными, Ассоциация ФинТех

Частое появление федеративного обучения в публикациях в области здравоохранения объясняется тем, что в большинстве случае медицинские данные пациентов хранятся на серверах отдельных больниц или иных медицинских учреждений и являются наиболее чувствительными данными для конечного пользователя. Ввиду того, что передача их в единое хранилище не соответствует законодательству многих стран, то для решения задачи применения ИИ в медицине стали активно применять подходы федеративного обучения, которые выступают лучшей альтернативой сбору огромной единой базы знаний.

[1]https://www.mdpi.com/2079-9292/11/4/670

Подход уже использовался для сегментации мозга и опухолей в медицинской томографии, а также позволил моделям работать с чувствительными данными фМРТ[1]-изображений для выявления биомаркеров заболеваний в рамках Международной инициативы по обмену данными при нейровизуализации (ABIDE).

Федеративное обучение (FL) – один из основных подходов при работе с периферийными вычислениями (edge computing) и Интернетом вещей (IoT). Он хорошо подходит для них в связи с быстрорастущей вычислительной мощностью устройств, а также необходимостью хранить и обрабатывать данные локально, соблюдая необходимые правила конфиденциальности.

Подход эффективен и при разработке рекомендательных систем, к которым относятся рекомендации товаров в интернет-магазинах, музыки или фильмов в стриминговых сервисах, а также персонализация клиентского опыта в целом. Федеративное обучение позволяет создавать системы персонализированных рекомендаций, не опасаясь утечки данных. Среди прочих FL решает проблему «холодного старта»[2]. В случае с федеративным обучением система распознает, какой продукт или услугу предложить пользователю – профиль предпочтений нового пользователя X схож с профилем существующего пользователя Y.

ПРИМЕНЕНИЕ В БАНКАХ И ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

Федеративное обучение тесно связано с концепцией Открытого банкинга (Open Banking), Открытых финансов (Open Finance) и Открытых данных (Open Data).

Ассоциация ФинТех в 2022 году провела исследование по Открытым API в России. В нем команда аналитиков АФТ более глубоко рассматривает направления Open Banking и Open Finance, а именно изучает мировые и российские практики и проводит связь с концепцией Open Data.

Открытый банкинг — это модель бизнеса, которая предполагает открытый доступ к банковским данным и сервисам через стандартизированные интерфейсы. Основными особенностями являются:

- открытый доступ к данным о клиентах, таким как история транзакций, информация о счетах,
- появление новых сервисов, таких как аналитика расходов, персональные финансовые менеджеры и т. д.

Основные сценарии федеративного обучения в открытом банкинге за счет совместного обучения моделей ИИ без потери конфиденциальности данных отдельных клиентов могут быть по следующим направлениям:

1. Обнаружение мошенничества: подход может использоваться для выявления мошеннических операций путем анализа закономерностей в нескольких банках.
2. Персонализированные финансовые рекомендации: в данном случае федеративное обучение может использоваться для предоставления персонализированных финансовых рекомендаций клиентам на основе истории операций и других финансовых данных.
3. Кредитный скоринг: для разработки более точных моделей, основывающихся на данных множества банков.
4. Управление рисками: для анализа рисков и разработки более эффективных стратегий управления ими.
5. Сегментация клиентов: для сегментации клиентов на основе их финансового поведения и предпочтений, что позволяет банкам предлагать более подходящие продукты и услуги.

[1]Функциональная магнитно-резонансная томография

[2]«Холодный старт» — это ситуация, когда модели не хватает данных для корректной работы и предоставления точных рекомендаций. Она может возникнуть в трех случаях: при запуске новой системы, когда нет достаточного количества пользователей и их взаимодействий с объектами; для новых пользователей, которые еще не совершили достаточно действий для формирования их профиля; и для новых объектов, которые еще не привлекли достаточное количество интереса пользователей для формирования предсказаний.

ЭТАПЫ СОЗДАНИЯ ФЕДЕРАТИВНОЙ СИСТЕМЫ

Ключевые шаги для создания успешной модели федеративного обучения для обмена конфиденциальными данными:

1. Построение доверительных взаимоотношений между заинтересованными сторонами, установка четких каналов связи и обеспечение прозрачности процессов принятия решений.
2. Определение конкретных данных для совместного использования, а также оценки масштаба проекта, целей и задач коллектива для совместного определения проблематики в рамках применения федеративного подхода.
3. Определение потенциальной пользы для каждой заинтересованной стороны, а также гарантия наличия необходимых ресурсов у каждой организации для участия. Это необходимо для соотнесения интересов и возможностей каждой стороны.
4. Определение ключевых ресурсов проекта: сотрудников, которые будут вести проект, его финансирование, бюджет для согласования состава руководства проекта, а также источников финансирования.
5. Выявление нормативных препятствий для обмена данными между учреждениями или странами, чтобы убедиться, что операции проводятся законным образом.
6. Разработка системы принятия решений, включающей в себя установление правил доступа к данным и их использования, а также определение ролей и обязанностей всех заинтересованных сторон для создания соответствующей модели управления.
7. Разработка стандартов сбора, хранения и обмена данными между учреждениями для построения структуры данных.
8. Внедрение API-протокола, который обеспечит безопасный доступ к модели или общим данным, обеспечивая при этом защиту конфиденциальности для внедрения модели федеративного обучения для обмена конфиденциальными данными.

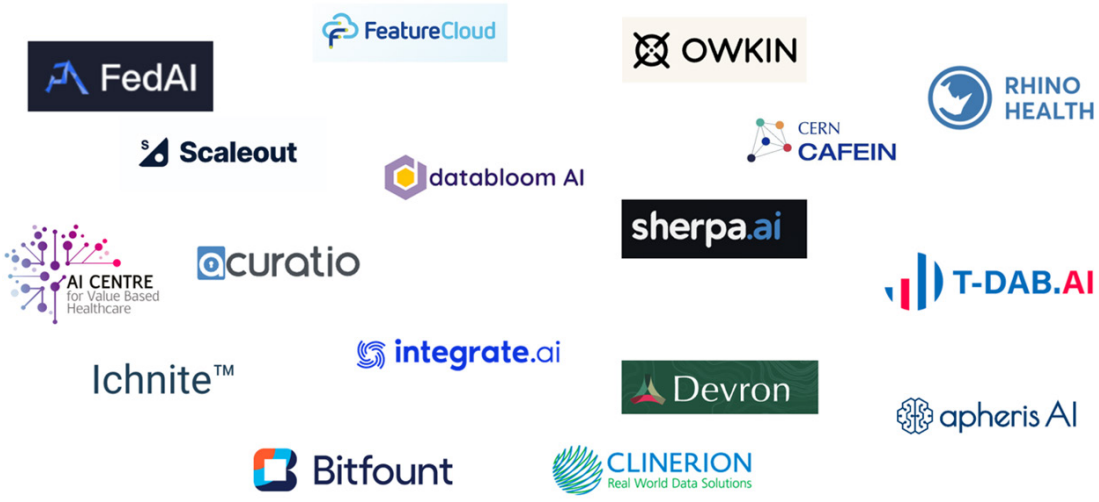
ПРОБЛЕМЫ ПРИ СОЗДАНИИ ФЕДЕРАТИВНОЙ СИСТЕМЫ

• Неравномерность данных: имеются участники сети, чьи объемы данных существенно отличаются от других.
• Неоднородность данных: организации собирают и обрабатывают данные по-разному, что может привести к необъективности результатов модели.
• Замедление процесса обучения: распределение данных между разными устройствами может затруднить и замедлить процесс обучения модели.
• Несовместимость систем: компании располагают различным аппаратным и программным обеспечением, что может снизить производительность системы федеративного обучения.
• Несовершенность технологического оснащения: недостаточно продуманное построение системы федеративного обучения может привести к задержкам и низкой пропускной способности, негативно сказывающимся на точности и производительности.
• Распределение вычислительных ресурсов: распределение обучения на несколько устройств или организаций требует оптимизации вычислительной мощности с учетом пропускной способности сети.
• Роли и обязанности участников: для успешной реализации федеративной системы необходимы четкие механизмы взаимодействия и определение зон ответственности. Больший объем данных у одного участника может существенно повлиять на результаты модели. Для того, чтобы присоединение новых участников не нарушило процесс обучения, необходимо гибкое и согласованное со всеми сторонами масштабирование технических и организационных процессов.
• Защищенность данных: конфиденциальность – основная причина, по которой специалисты обращаются к федеративному подходу. Передача локальных обновлений модели на протяжении всего процесса обучения может привести к разглашению данных центральному серверу или третьей стороне. Хотя в настоящее время предпринимаются попытки снизить вероятность утечки за счет использования таких механизмов, как дифференциальная приватность и протокол конфиденциальных вычислений, они часто приводят к снижению эффективности системы или уменьшению точности модели.

КАРТА РЕШЕНИЙ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

ИНСТРУМЕНТЫ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ И FL-ФРЕЙМВОРКИ

FL-ПЛАТФОРМЫ И РЕШЕНИЯ



БУДУЩЕЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

Федеративное обучение позволяет обучать модель на собственных данных множеству устройств или организаций сразу. Благодаря растущей емкости памяти и вычислительных мощностей смартфонов, планшетов, ноутбуков и даже автономных автомобилей, а также растущей скорости обмена данных благодаря 5G, FL произвел революцию в машинном обучении.

Однако есть отдельные области, в которых необходимо произвести улучшения для более массового использования этого подхода. Например, стоит изучить или разработать более совершенные методы сбора и компоновки данных. Желательно найти более эффективные методики распределения вычислительных ресурсов, так как проекты FL становятся все более масштабными. К тому же с ростом «амбиций» моделей, построенных на федеративном обучении, необходимо разработать более гибкие и понятные методики для управления затратами.

Большинство исследований с фокусом на федеративное обучение обычно охватывают область здравоохранения и IoT. Однако этот подход также может быть полезен и в других областях, таких как системы доставки еды, VR-приложения, финансы, общественная безопасность, выявление угроз, управление автомобильным движением и пр.

ПОЧИТАТЬ ДОПОЛНИТЕЛЬНО ПО ТЕМЕ:

Google AI

Федеративное обучение: Онлайн-комикс

PriceWaterhouseCoopers

Рекомендательные системы: Применение в сфере финансов

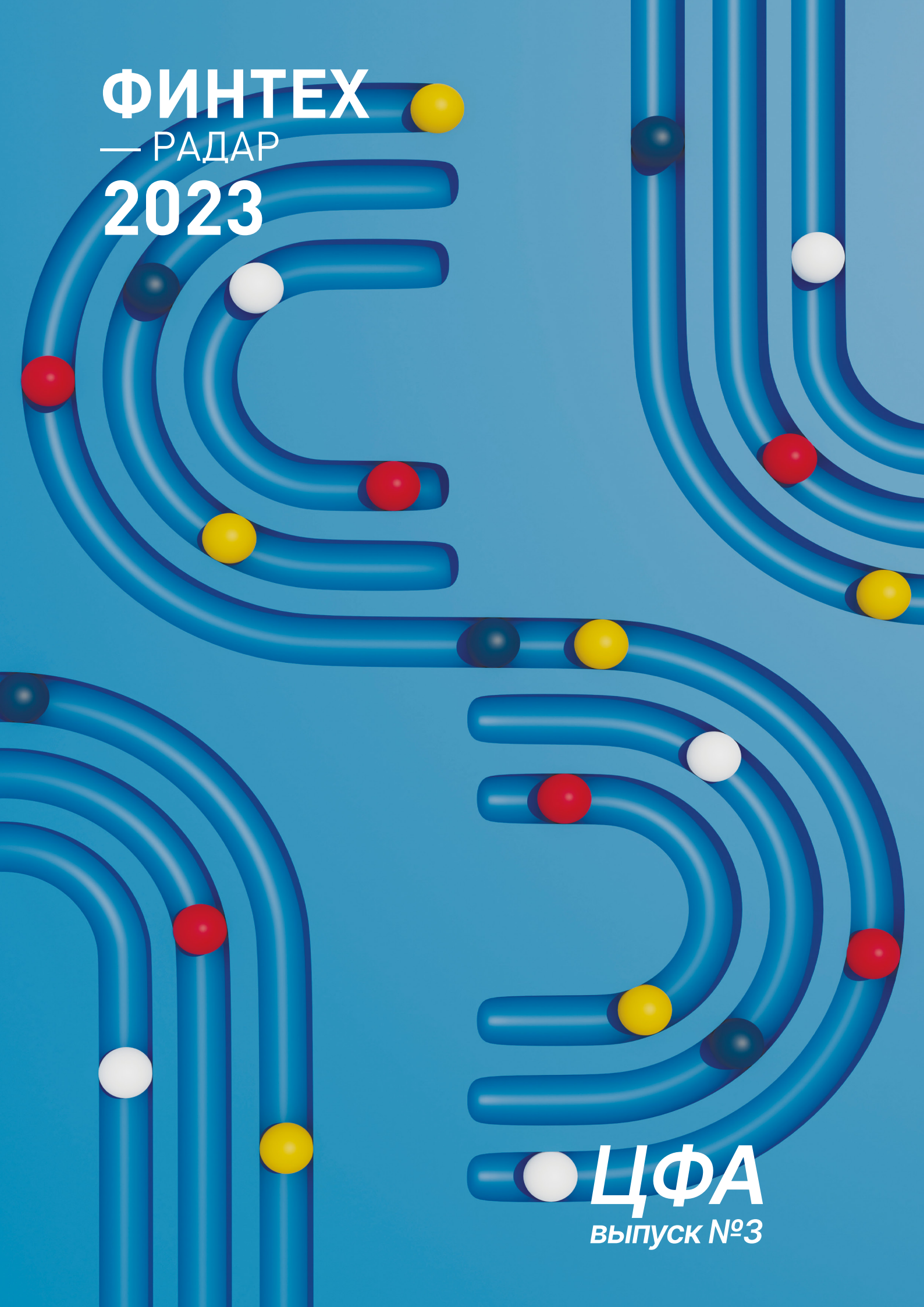
BCG

Борьба за периферийные вычисления

Яндекс

Трансферное обучение: почему deep learning стал доступнее

ФИНТЕХ — РАДАР 2023



ЦФА

выпуск №3

Цифровые финансовые активы

Данные в статье актуальны на июнь 2023 года

ЦИФРОВЫЕ ФИНАНСОВЫЕ АКТИВЫ

Российский финансовый сектор значительно преобразился за последние 5 лет. В первую очередь это касается цифровизации банковской сферы.

Цифровизация коснулась не только внутренних бизнес-процессов и улучшения клиентского опыта, но и создания нового рынка финансовых инструментов, использующего преимущества таких технологий, как блокчейн и смарт-контракты, который закреплен в законодательстве РФ как **Цифровые финансовые активы (ЦФА)**.

3 февраля 2022 года компания Атомайз первой получила статус оператора информационных систем. 28 июня 2022 года на платформе Лайтхаус произошел первый выпуск ЦФА объемом **5 млн рублей.**

С совершения первой сделки по ЦФА прошел один год. Приводим мнение ключевых участников финансового рынка о состоянии рынка ЦФА.

МНЕНИЯ УЧАСТНИКОВ РЫНКА

«Мы токенизировали 12 разных типов активов, от металлов и квадратных метров до долговых обязательств корпораций. Эмитент может выбрать уже готовый смарт-контракт или «индивидуальную комплектацию» цифрового финансового актива».

Екатерина Фроловичева
Генеральный директор Атомайз

*«Если (в долгосрочной перспективе) этот рынок (ЦФА) не достигнет хотя бы **одного трлн рублей,** то его можно будет закрывать».*

Денис Додон
директор центра инноваций Альфа-Банка

«Развивается важная для рынка ЦФА технология смарт-контрактов. Сбер запустил ComUnity – сообщество разработчиков и экспертов в области децентрализованных финансов (DeFi)».

Александр Нам
директор Лаборатории блокчейн Сбера

Появлению ЦФА предшествовали десятки инноваций в области финтеха. Со многими из них у ЦФА есть как общие свойства, так и значительные различия. Нужно отметить, что ключевой задачей развития ЦФА в России является преодоление как технических, так и регуляторных барьеров.

Технология распределенных реестров

«Технология распределенных реестров открыла возможности по использованию смарт-контрактов, появлению новых способов хранения, обработки и передачи информации.»

Применение технологии распределенных реестров сделало возможным появление цифровых инструментов, которые стали одним из наиболее значимых нововведений последних лет на финансовом рынке.

Технология распределенных реестров (ТРР) – тип технологии, в результате использования которой информация распределяется между всеми участниками сети. Для обеспечения согласованности данных используется технология консенсуса, которая помогает участникам достигнуть единства в отношении текущего состояния в реестре.

Криптографически связанная цепь блоков транзакций, называемая **блокчейн**, — это один из типов распределенного реестра. Блокчейн обеспечивает структурирование данных в цепочку блоков и гарантирует их неизменность.

Существуют **публичные, закрытые и гибридные сети** распределенных реестров. Публичные сети доступны для любого пользователя, что обеспечивает открытость и прозрачность операций. При этом пользователи не идентифицированы по умолчанию, что дает возможность обеспечить анонимность транзакций.

Технологии распределенных реестров позволяют использовать **смарт-контракты**, с помощью которых можно автоматизировать услуги, обеспечивать многостороннее взаимодействие между участниками одной сети, а также применять отдельные DeFi-инструменты.

Смарт-контракт – алгоритм (программный код), в рамках которого в распределенном реестре фиксируются права и обязанности сторон сделки, условия договорных отношений, а также механизм их будущего автоматического исполнения. Условиями для самостоятельного исполнения могут быть: наступление конкретной даты и времени, получение подписи определенного участника сети, события из внешних по отношению к распределенной сети систем и другое. Смарт-контракты позволяют снизить затраты за счет автоматизации, устранить необходимость в избыточных операциях, сократить число посредников.

Основные плюсы ТРР – неизменность информации и согласованность действий со всеми участниками сети – позволяют повысить эффективность бизнес-процессов за счет оптимизации хранения и передачи информации и реализации смарт-контрактов. Но, в то же время, из-за децентрализации изменение структуры сети становится сложно реализуемым процессом, поэтому к разработке и внедрению проектов на основе ТРР необходимо подходить с особой внимательностью.

Технологии распределенных реестров позволяют использовать смарт-контракты, с помощью которых можно автоматизировать взаимодействие между участниками одной сети, а также применять отдельные инструменты DeFi.

ЦИФРОВЫЕ АКТИВЫ В МИРЕ

Цифровой актив в мировой практике - это любой актив, существующий только в цифровой форме и имеющий право или разрешение на использование.

Одними из первых инструментов, которые были созданы на основе технологии распределенного реестра, являются **криптовалюты**, ставшие популярными в том числе благодаря возможности проведения анонимных транзакций,

а также непосредственного доступа пользователей к своим активам. Анонимность в данном контексте — это отсутствие связи адреса кошелька с инициатором операции. В то же время в подавляющем большинстве блокчейнов история транзакций по конкретному адресу открыта.

Также были созданы иные цифровые активы, представляющие собой новые финансовые инструменты. Традиционные финансовые инструменты также могут быть переведены в цифровую форму с применением ТРР.

ВИДЫ ЦИФРОВЫХ АКТИВОВ

Токенизированные финансовые инструменты – активы, которые существуют в виде токенов, предоставляющие их обладателям определенные права или являющиеся цифровой формой какого-либо актива, и права на которые записаны в виде программного кода в распределенном реестре. Примером таких активов в российском регулировании могут выступать цифровые финансовые активы и утилитарные цифровые права.

Стейблкоины – криптовалюты, у которых стоимость привязана к базовому активу, часто фиатной валюте или товарам, таким как золото. Так снижается волатильность цен. Обычно обеспечены проверенными резервами и могут взаимодействовать со смарт-контрактами.

Невзаимозаменяемые токены (NFT) – цифровые активы с уникальным идентификационным кодом, записанным в распределенном реестре, который может являться подтверждением наличия у обладателя NFT права в отношении уникального материального или нематериального объекта (актива) или может удостоверять его подлинность. Так, в виде NFT могут быть представлены такие уникальные объекты, как произведения искусства, интеллектуальная собственность, цифровые объекты (изображения, документы, аудио, видео).

Выпуск и обращение цифровых активов осуществляются непосредственно в блокчейне. При этом совершение сделок между владельцами может проводиться тремя способами:

1. **С привлечением посредников**, в качестве которых выступают специально созданные централизованные платформы – например, биржи, участники традиционного финансового рынка, операторы обмена цифровых активов. Перевод цифрового актива и денежных средств осуществляется с использованием платформенной биржевой инфраструктуры, в которой открываются соответствующие кошельки (счета) сторон сделок. Привлечение дополнительных посредников увеличивает расходы на совершение сделок.

2. **Без привлечения посредников, напрямую между участниками сделки.** Перевод цифрового актива осуществляется в блокчейне, а расчеты в основном происходят на базе защищенного номинального счета платформы в банке по модели DVP (delivery versus payment, поставка против платежа). Это безопасная схема, которая позволяет сократить комиссионные затраты участников.

3. **Без привлечения посредников с применением децентрализованных решений** (DeFi-инфраструктура). Заключение и исполнение сделок, включая расчеты, происходят в информационной системе без участия посредника. Это одна из возможных, но пока не реализованных моделей расчетов на рынке ЦФА.

ВИДЫ ЦИФРОВЫХ ПРАВ В РОССИИ

В России созданы правовые условия для выпуска и обращения цифровых инструментов – утилитарных цифровых прав и цифровых финансовых активов. И то, и другое является подвидом **цифровых прав**.

Цифровые права – обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу.

В 2019 году был принят Федеральный закон № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (Закон о краудфандинге). В этом законе были определены способы инвестирования, одним из которых было приобретение **утилитарных цифровых прав.**

Утилитарными цифровыми правами (УЦП) признаются цифровые права, включающие:
— право требовать передачи вещи/вещей;
— право требовать передачи исключительных прав на результаты интеллектуальной деятельности и/или прав использования результатов интеллектуальной деятельности;
— право требовать выполнения работ и/или оказания услуг.

Понятие ЦФА ввел Федеральный закон 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (Закон о ЦФА)[1]. Также он ввел регулирование отношений, возникающих при выпуске, учете и обращении цифровых финансовых активов (ЦФА), которые могут выпускаться и обращаться в системах, в том числе на основе распределенного реестра.

Цифровыми финансовыми активами (ЦФА) признаются цифровые права, включающие:
— денежные требования;
— возможность осуществления прав по эмиссионным ценным бумагам;
— права участия в капитале непубличного акционерного общества;
— право требовать передачи эмиссионных ценных бумаг, предусмотренных решением о выпуске цифровых финансовых активов в порядке, установленном Законом о ЦФА.

Выпуск, учет и обращение ЦФА возможны только путем внесения/изменения записей в информационную систему на основе распределенного реестра, а также в иные информационные системы.

Законодательством предусматривается выпуск актива, совмещающего свойства ЦФА и УЦП (утилитарных цифровых прав), именуемые **гибридными цифровыми правами (ГЦП)**. Они, например, одновременно удостоверяют денежное требование и право требовать передачи вещи. Из-за специфической природы данного актива существует ряд нерешенных вопросов налогообложения вышеуказанных активов, что в итоге негативно влияет на их привлекательность для инвесторов.

В 2020 году в России созданы правовые условия для выпуска и обращения цифровых финансовых активов и утилитарных цифровых прав.

[1]Законы, которые вводят понятия УЦП и ЦФА, имеют один номер, но их предмет регулирования отличается.

ВИДЫ ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ

В международной практике выделяют три основных типа цифровых финансовых активов: **utility-токены, security-токены и payment-токены.** Все они упомянуты в Законе о ЦФА[1], но в его рамках только security-токены можно отнести к цифровым финансовым активам согласно Закону.

Закон вводит определение «цифровой валюты», которое включает классические криптовалюты («payment-токены»), такие как Bitcoin и Ethereum. Однако цифровая валюта не признается в России законным платежным средством, и ее статус и обращение будут регулироваться отдельным федеральным законом.

Utility-токен

Utility-токен (утилитарный токен) — тип цифрового токена, выпущенного для финансирования проектов. Utility-токены предоставляют владельцам доступ к существующему или потенциальному продукту или услуге, но не предоставляют участникам продажи токенов права влиять на деятельность компании.

Security-токен

Security-токен (токен ценной бумаги) — цифровой актив, представляющий право собственности или другие права и передающий стоимость от актива или группы активов к токену. Фактически это традиционные ценные бумаги, которые созданы в цифровом виде, чтобы раскрыть потенциал блокчейна.

Payment-токен

Payment-токены (платежные токены) используются как альтернативный инструмент для совершения платежей и переводов. Некоторые из наиболее популярных криптовалют фактически являются платежными токенами.

Технология выпуска и обращения ЦФА должна обеспечивать идентификацию владельца ЦФА, возможность проверки подлинности ЦФА, предотвращение выпуска и обращения поддельных ЦФА.

Закон устанавливает общий порядок выпуска, учета и обращения ЦФА, при этом право на их выпуск имеют только юридические лица и ИП. ЦФА выдаются на основании решения о выпуске, в котором указываются вид и объем прав, представляемых выдаваемыми ЦФА, и содержатся некоторые другие сведения. Это решение должно быть опубликовано на сайте организации или лица, выпускающего ЦФА, а также на сайте оператора информационной системы, в которой они выпускаются.

В законе нет ограничений в отношении того, кто может приобретать ЦФА. Однако Банк России установил, что ЦФА, отвечающие определенным критериям, могут быть приобретены только квалифицированными инвесторами и/или могут быть приобретены покупателями, не являющимися квалифицированными инвесторами, в пределах суммы, установленной ЦБ РФ, или в пределах совокупной стоимости других ЦФА, передаваемых в качестве возмещения (на текущий момент – 600 000 рублей в год).

Данные в статье актуальны на июнь 2023 года

В настоящий момент цифровая валюта не признана законным платежным средством в России, ее статус и обращение будет регулироваться отдельным законом.

[1]Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 N 259-ФЗ

ОТЛИЧИЕ ЦФА ОТ ИНЫХ ЦИФРОВЫХ АКТИВОВ

Криптовалюты – децентрализованные цифровые активы, которые опираются на криптографию и технологию распределенных реестров для ведения безопасной и прозрачной записи транзакций. Они не имеют внутренней стоимости и не обеспечены ни эмитентом, ни базовым активом.

Пример: Bitcoin, Ethereum

CBDC – цифровая форма денежных средств центрального банка, доступная широкой общественности. Она является обязательством центрального банка и похожа на криптовалюты, за исключением того, что ее стоимость фиксируется центральным банком и эквивалентна фиатной валюте страны.

Пример: цифровой юань

Отличие ЦФА от криптовалют:

1 ЦФА и криптовалюты имеют разную инфраструктуру обращения. Цифровые финансовые активы, как и гибридные цифровые права, в России выпускаются официальными платформами, у которых есть статус «операторов информационных систем». За их деятельностью следит ЦБ РФ.
Легитимных российских криптобирж не существует, так как в стране нет детального спецрегулирования криптовалют. Таким образом, вкладываясь в криптовалюту, вы априори берете все риски на себя.

2 В отличие от большинства криптовалют, у цифровых финансовых активов и гибридных цифровых прав есть конкретный эмитент. Он несет обязательства перед инвесторами. Если что-то случится, вы имеете законное право защищать свои интересы в суде.
Выпуск ЦФА — прозрачная процедура. Эмитент обязан публиковать на платформе решение о выпуске. Это гарантирует правовую чистоту сделок с ЦФА.

Отличие ЦФА от CBDC:

От CBDC (цифровых валют центральных банков) ЦФА отличаются тем, что они не являются формой национальной валюты. Цифровой рубль выпускает Центральный банк РФ, он выполняет те же функции, что и наличные и безналичные деньги. В отличие от ЦФА, им можно будет расплачиваться за товары и услуги.

ИНФРАСТРУКТУРА РЫНКА ЦИФРОВЫХ ПРАВ

Основой для функционирования рынка цифровых активов является новая инфраструктура: операторы информационных систем и операторы обмена.

Операторы обмена цифровых финансовых активов (ООЦФА) обеспечивают заключение сделок с цифровыми финансовыми активами. На данный момент в России еще не зарегистрированы операторы обмена.

Оператор информационной системы (ОИС) организовывает выпуск и обращение ЦФА. Инфраструктура ОИС включает в себя и клиринг, и учет прав, и сбор и удовлетворение заявок, и расчеты по ним, и вторичную торговлю ЦФА, выпущенными в его информационной системе.

За год, прошедший с первой эмиссии на российском рынке, появились новые игроки и новые виды ЦФА. В настоящий момент[2] в России 8 операторов информационных систем, которые имеют право выпускать ЦФА.

[1]3-го августа 2023 года Банк России включил первую организацию в реестр операторов обмена цифровых финансовых активов - МосБиржу.
[2]Данные в статье актуальны на июнь 2023 года.

РАЗВИТИЕ РЫНКА ЦФА

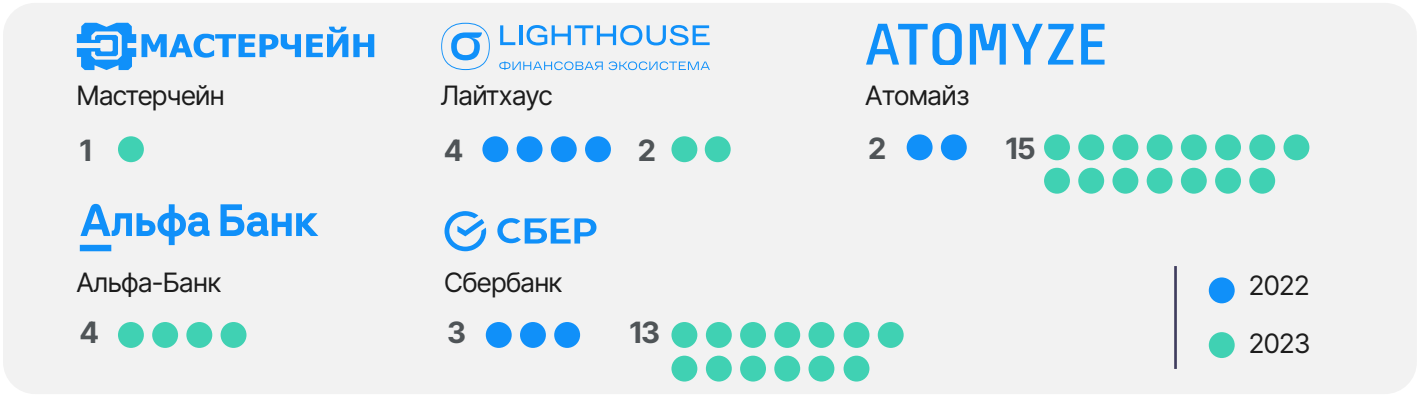
Данные в статье актуальны на июнь 2023 года

В России первое размещение ЦФА состоялось 28 июня 2022 года на платформе **Лайтхаус**. Сейчас, спустя год, суммарно на пяти платформах ОИС произошло **73 выпуска:** Сбер - 37, Атомайз - 25, Лайтхаус - 6, Альфа-Банк - 4 и Мастерчейн - 1.

Однако не все выпуски можно считать равноценными. Так, объем единственной эмиссии Мастерчейна составил 15 млрд руб., в то время как размер некоторых выпусков не превышал 1000 руб.

В рамках данного материала учитываются выпуски объемом не менее 1 млн рублей. В России за год произошло **44 выпуска ЦФА**, удовлетворяющих данному условию.

КОЛИЧЕСТВО ВЫПУСКОВ ЦФА ОБЪЕМОМ НЕ МЕНЕЕ 1 МЛН РУБ.



Больше всего эмиссий ЦФА объемом не менее 1 млн рублей, а именно 17 выпусков, было произведено на платформе **Атомайз**. Следующим, с 16 эмиссиям, идет **Сбер**. При этом Атомайз протестировал самый широкий состав инструментов ЦФА.

Как видно из примеров ниже, ЦФА – гибкий инновационный инструмент. Благодаря смарт-контрактам его можно «связывать» с разнообразными активами реального мира и описывать самые разные механики обращения инструмента.

Долговые ЦФА
Цифровые финансовые активы этого типа связаны с финансовыми обязательствами корпораций. На текущий момент они составляют более 60% проведенных выпусков на российском рынке. В частности, выпуски данного типа преобладают на платформах Сбера и Лайтхаус.

ЦФА на металлы
Пионером в токенизации драгоценных металлов является Атомайз. Первый в России выпуск этого типа состоялся в июле 2022 г. Новизна инструмента заключается в праве на денежное требование в размере рыночной стоимости палладия, который ранее не был общедоступным для инвесторов.

Далее в октябре 2022 г. Атомайз выпустил «Цифровую корзину драгметаллов», включая первые в России ЦФА на золото и серебро. В состав «корзины» также вошли 5 металлов платиновой группы — платина, палладий, родий, иридий и рутений «Красцветмета». Это первый диверсифицированный портфель ЦФА, который содержит готовую инвестидею: вложить средства в драгметаллы.

Первые сделки с участием физических лиц
Первые сделки с ЦФА с участием физлиц были проведены в ноябре 2022 г. на платформе Атомайз. За каждый 1 ЦФА инвесторы получили рыночную стоимость 1 г палладия согласно котировкам на Лондонском рынке драгоценных металлов. Таким образом, Атомайз реализовал полный жизненный цикл сделок с ЦФА, включая выпуск, продажу инвестору-юридическому лицу, перепродажу на вторичном рынке инвесторам-физлицам и погашение.

Цифровые квадратные метры недвижимости
ЦФА, привязанный к стоимости квадратного метра, был выпущен на платформе Атомайз в мае 2023 г. Один ЦФА равноценен 1 кв. метру в ЖК «Квартал Западный» от девелоперской группы «Самолет». Причем, купить или продать можно не только целый «квадрат», но и долю в нем на доступную для инвестора сумму от 50 тыс. рублей, что значительно снижает барьер входа для инвесторов.

Старт выпусков по открытой подписке
Еще один важный этап развития рынка ЦФА — появление выпусков по открытой подписке, т.е. для неограниченного числа лиц. Первый такой выпуск организовал Альфа-Банк в апреле 2023 года.

ЦФА как инструмент мотивации персонала
В мае 2023 г. была запущена корпоративная программа Норникеля «Цифровой инвестор». На платформе Атомайз выпущены первые ЦФА «minetoken». Через них экономический доход от деятельности компании передается сотрудникам.

Доходность по финансовому инструменту складывается из двух частей. Первая часть — периодические выплаты, равные дивидендам по акциям компании. Вторая часть — единовременная выплата при погашении инструмента (через 5 лет) в размере стоимости акций на дату погашения.

ЦФА – гибкий инновационный инструмент. Благодаря смарт-контрактам его можно «связывать» с разнообразными активами реального мира и описывать самые разные механики обращения инструмента.

ПЕРСПЕКТИВЫ РЫНКА ЦФА

Будущее ЦФА в России и за ее пределами зависит от различных факторов, таких как потенциал роста, изменения в регуляторной среде и технологические разработки.

Государственная дума 14 июня 2023 года приняла закон, согласно которому операторы финансовых платформ, такие как **Московская биржа** и **Сравни.ру**, смогут совмещать свою деятельность с деятельностью блокчейн-платформы, которая выпускает или обменивает ЦФА[1]. Это потенциально увеличит количество ОИС на российском рынке и его ликвидность, отчего инвесторы окажутся только в плюсе.

«На данный момент созданы не все условия для того, чтобы рынок ЦФА развивался. Нужно предпринять ряд усилий, чтобы ЦФА для инвестора и эмитента работали бы не хуже, чем традиционный финансовый инструмент, который по свойствам соответствует разным ЦФА. Мы должны думать о том, чтобы инвестор был защищен, как и при действиях на традиционном рынке. Как минимум он должен понимать, с каким эмитентом взаимодействует, каковы условия выпуска ЦФА и т. д.».

«ЦФА должны быть доступны и функционировать в цифровой среде «бесшовно». Для этого необходимо, в первую очередь, предоставить клиенту возможность прохождения процедуры идентификации на платформе оператора, используя аналогичные протоколы и системы, такие как Единая система идентификации и аутентификации (ЕСИА). Во-вторых, необходимо дать возможность платформам-операторам взаимодействовать с другими участниками рынка и реализовывать делегированную идентификацию клиента.»

Кирилл Пронин
директор Департамента инфраструктуры финансового рынка Банка России

«Анализ проведенных выпусков ЦФА и их динамика показывают осторожность как инвесторов, так и эмитентов в использовании данного инструмента. Преимущества ЦФА реализуются в полной мере при решении ряда задач. В первую очередь — это определение реальных потребностей участников рынка (потенциальных эмитентов и инвесторов) для формирования необходимого спектра продуктов и технологий с дальнейшим предложением операторам информационных систем реализовать и поддерживать данный спектр. Важной темой, по мнению участников АФТ, является выпуск методических рекомендаций по учету различных типов ЦФА на балансах как финансовых, так и нефинансовых организаций, эмитентов и инвесторов.»

Дмитрий Ищенко
заместитель генерального директора Ассоциации ФинТех

Несмотря на некоторые барьеры, объем выпуска цифровых финансовых активов в РФ растет, а нормативно-правовая база совершенствуется. В ближайшие годы стоит ожидать, что ЦФА составят значительную долю финансовой отрасли страны.

[1]3-го августа 2023 года Банк России включил МосБиржу в реестр операторов обмена цифровых финансовых активов.

ПОЧИТАТЬ ДОПОЛНИТЕЛЬНО ПО ТЕМЕ

Банк России

Развитие рынка цифровых активов в Российской Федерации

GFMA, BCG, Clifford Chance and Cravath, Swaine & Moore LLP

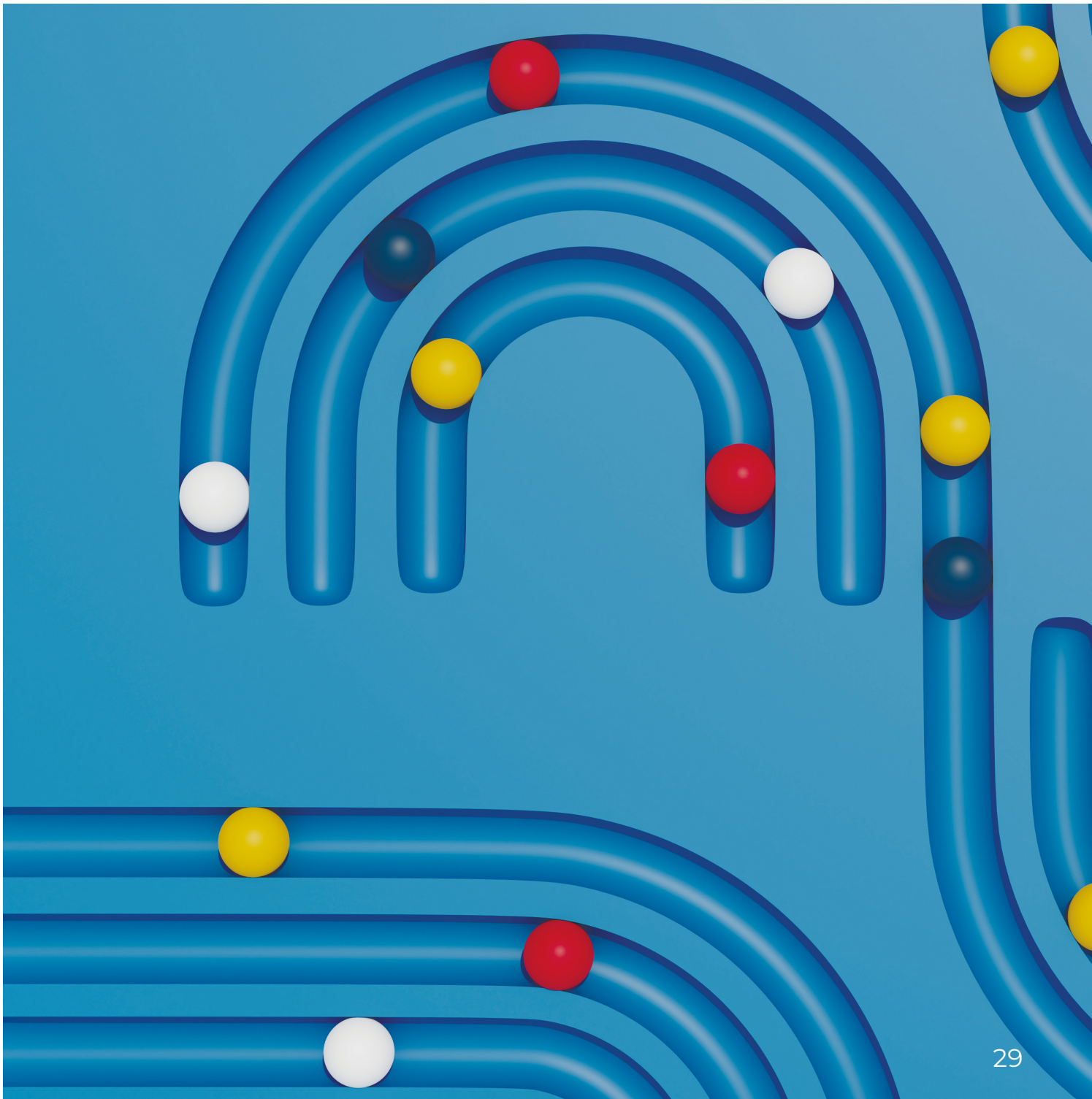
Влияние технологии распределенных реестров на глобальных рынок ценных бумаг

Atomyze

Цифровые финансовые активы: Инструкция по применению

KPMG

Инвестиции в цифровые активы



ФИНТЕХ — РАДАР 2023

DevSecOps

выпуск №4

DevSecOps

безопасная разработка

Данные в статье актуальны на июль 2023 года

БЕЗОПАСНАЯ РАЗРАБОТКА И РЕШЕНИЯ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Еще 10–15 лет назад разработки решений с открытым исходным кодом (Open Source) в России практически не существовало. Согласно новостному агентству Cnews, Министр цифрового развития, связи и массовых коммуникаций РФ Максут Шадаев называет открытые решения «главным трендом и магистралью», подчеркнув их важность тезисом «опенсорс – наше все». Перед страной стоит задача за короткий срок создать полноценные отечественные решения с открытой лицензией, которые смогут стать основой технологического развития страны.

*«Опенсорс – наше все»**

Максут Шадаев
Министр цифрового развития,связи и массовых коммуникаций РФ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ: СТАНОВЛЕНИЕ ПОДХОДА И ОСНОВНЫЕ ПРИНЦИПЫ

До середины 1970-х годов компьютерный код рассматривался как элемент работы вычислительной техники. Организации разрабатывали собственные программы, и обмен кодом был распространенной практикой.

Однако в 1974 году было установлено, что программный код подлежит защите авторским правом. Издание проприетарного ПО стало отраслью, в которой быстро возникла жесткая конкуренция.

«Бунт» против устоявшихся практик начался в 1983 году, когда программист Ричард Столлман основал Фонд свободного программного обеспечения (Free Software Foundation) и разработал первую лицензию на ПО с «авторским левом» (copyleft[1]) – **GNU General Public License (GPL)**.

Термин «Open source» был сформирован лидерами мнений в 1998 году. Многие считали, что понятие «свободное ПО» слишком сильно подчеркивает «безвозмездность» программного обеспечения в качестве его основной ценности. Для продвижения новой системы идей была создана организация **Open Source Initiative (OSI)**, которая установила основные принципы индустрии и разместила соответствующие лицензии на открытое ПО.

Понятие **«открытое свободное программное обеспечение»** (ОСПО) относится к тем лицензионным договорам, которые соответствуют условиям и GNU GPL, и OSI, и в таком случае корректным будет использование выражения «FLOSS» – «Free/Libre and Open Source Software». В нынешнем правовом поле РФ проблемы «действительности» ОСПО-лицензий нет, так как все лицензии, соответствующие этим условиям, соответствуют и принятым в стране понятиям «открытая лицензия[2]» и **«свободное программное обеспечение»** (СПО)[3].

*Глава Минцифры Максут Шадаев на CNews FORUM Кейсы — о системно значимых ИТ-компаниях, суверенном интернете и «Гостехе»

[1] Авторское лево – лицензия, которая требует от каждого, кто улучшает исходный код, аналогичным образом публиковать его отредактированную версию свободно для всех.

[2] Статья 1286.1 ГК РФ. Открытая лицензия на использование произведения науки, литературы или искусства (введена Федеральным законом от 12.03.2014 N 35-ФЗ).

[3] ГОСТ Р 54593–2011. Национальный стандарт Российской Федерации. Информационные технологии. Свободное программное обеспечение. Общие положения (утв. и введен в действие Приказом Росстандарта от 06.12.2011 N 718-ст).

Для того, чтобы лицензионный договор можно было называть «открытым», он должен соответствовать **10 критериям**, опубликованным OSI[4]:

1 Свободное распространение

Лицензия не ограничивает никакую сторону в продаже или передаче программного обеспечения в качестве компонента совокупного распространения. Лицензия не требует выплаты роялти или иного вознаграждения за такую продажу.

2 Доступность исходного кода

Программа должна включать исходный код и допускать распространение как в виде исходного кода, так и в скомпилированном виде.

3 Возможность модифицировать и редактировать ПО

Лицензия должна разрешать модификации и производные работы и позволять распространять их на тех же условиях, что и лицензия исходного программного обеспечения.

4 Целостность авторского исходного кода

Лицензия может ограничивать распространение исходного кода в измененном виде только в том случае, если лицензия допускает распространение «файлов исправлений» вместе с исходным кодом с целью модификации программы во время сборки.

5 Отсутствие дискриминации лиц или групп лиц

Лицензия не должна дискриминировать какое-либо лицо или группу лиц.

6 Отсутствие дискриминации по целям применения

Лицензия не должна ограничивать использование программы в какой-либо конкретной области деятельности.

7 Распространение лицензии

Права, прилагаемые к программе, должны распространяться на всех, кому она перераспространяется, без необходимости оформления дополнительной лицензии.

8 Независимость от другого ПО

Права, предоставляемые программе, не должны зависеть от принадлежности программы к тому или иному дистрибутиву программного обеспечения.

9 Отсутствие ограничений на иное ПО

Лицензия не должна накладывать ограничений на другие программы, распространяемые вместе с лицензионным программным обеспечением.

10 Технологическая нейтральность

Ни одно из положений лицензии не должно зависеть от какой-либо отдельной технологии или стиля интерфейса.

[4]Приводится короткая свободная интерпретация 10 принципов OSI. Для ознакомления с официальной трактовкой правительства РФ, указанной в постановлении к эксперименту по открытым лицензиям, рекомендуем ознакомиться с исходным текстом Постановления Правительства Российской Федерации от 10.10.2022 № 1804 на официальном интернет-портале правовой информации (www.pravo.gov.ru).

ОТЛИЧИЕ СВОБОДНОГО ПО И ОТКРЫТОГО ПО

Понятие **свободное ПО** (СПО), фигурирующее в законодательных проектах и нормативной базе Российской Федерации, **не эквивалентно** понятию **открытое ПО** (ОПО), используемого ИТ-специалистами.

Любое открытое ПО является свободным, однако не каждое свободное ПО является открытым

Сильно упрощая, свободное ПО – любое, которое не считается проприетарным[5] .

Лицензии СПО можно разделить на «разрешительные» и «вирусные». Разрешительные лицензии не налагают серьезных ограничений, в том числе и по дальнейшей судьбе производных продуктов. В этот список можно включить такие лицензии, как Apache и MIT.

Их важно различать, так как приложение, использующее ПО с «вирусной» лицензией, будет сложно зарегистрировать в Едином реестре российских программ (ЕРРП). Необходимо будет убедиться[6], что этот компонент правомерно используется и позволяет получить исключительные права на ПО, использующее его в составе.

ПОРЯДОК ИСПОЛЬЗОВАНИЯ СВОБОДНОГО ПО

В рамках методических рекомендаций Минцифры по переходу на использование российского программного обеспечения[7] любое ПО, которое не зарегистрировано в одном из реестров приложений, **приравнивается к иностранному ПО.**

Таким образом, любое свободное ПО может использоваться субъектами критической информационной инфраструктуры финансового рынка (КИИ ФР)[8] только при выполнении следующих условий:

1. в Едином реестре российских приложений (ЕРРП) отсутствует полнофункциональный аналог необходимого решения;
2. в Реестре евразийского программного обеспечения (РЕПО) отсутствует отсутствует соответствующий полнофункциональный аналог.

Также имеется дополнительное условие – между двумя аналогичными приложениями, одно из которых зарегистрировано в дружественной стране, а другое в недружественной[9], **рекомендуется выбирать первое.**

Свободное ПО позволяет разработчикам создавать комбинации различных программных компонентов, что может способствовать появлению новых инновационных продуктов и сервисов. Например, если есть две программы с открытым кодом, одна из которых предназначена для создания веб-сайтов, а другая – для управления базами данных, то разработчик может объединить их функциональность, чтобы создать новый продукт, который сочетает в себе возможности обеих программ.

[5] Корректное определение можно найти в ГОСТ Р 54593-2011 «Информационные технологии. Свободное программное обеспечение. Общие положения».

[6] Подробнее об условиях включения программного обучения в ЕРРП: «Правила формирования и ведения реестров Российского и Евразийского программного обеспечения»

[7] Приказ Минцифры России от 18.01.2023 N 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации»

[8] Критической информационной инфраструктуры финансового рынка

[9] Распоряжение от 5 марта 2022 года №430-р «Перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия».

ВОЗМОЖНОСТИ ОТКРЫТОГО ИСХОДНОГО КОДА (OPEN SOURCE)

Использование ПО с открытым кодом предоставляет значительные преимущества. Во-первых, **снижается время вывода продукта на рынок (T2M)**. Поскольку разработчики могут использовать существующие решения и модифицировать их под свои нужды, время и затраты на разработку значительно сокращаются. Кроме того, открытый код обеспечивает более быстрый доступ к новым технологиям, что также способствует ускорению процесса разработки и выходу конечного продукта.

Во-вторых, с точки зрения DevSecOps, открытый код **обеспечивает большую прозрачность и контроль над безопасностью приложений.** Разработчики могут легко проверить код на наличие уязвимостей и исправить их до того, как они станут проблемой для пользователей.

Практика DevSecOps ускоряет вывод продукта на рынок, что приводит к росту выручки на 15-20%

Открытый код также позволяет применять **лучшие практики безопасности**, которые были созданы сообществом разработчиков – использование **проверенных библиотек** и фреймворков, а также реализация **глубоко проработанных** процессов разработки и тестирования безопасности.

Безопасная разработка снижает долю уязвимого корпоративного ПО в 2,5 раза

Открытый исходный код может помочь в соблюдении требований по безопасности и соответствию регуляторным нормативам. Компании могут использовать безопасные и проверенные решения, которые уже были протестированы сообществом разработчиков, а также иметь доступ к открытым стандартам и документации.

В рамках исследования **«Применение технологий искусственного интеллекта на финансовом рынке»**, разработанного **Ассоциацией ФинТех**, выявлено, что всего **15%** компонентов технологического стека опрошенных компаний составляют **иностранные проприетарные решения.** Более **75%** составляют либо **открытое ПО**, либо **собственные разработки** компаний, которые, в свою очередь, в значительной мере основываются на открытом исходном коде.

ДОЛЯ ТИПОВ ПО В ТЕХНОЛОГИЧЕСКОМ СТЕКЕ ИИ-СИСТЕМ КЛЮЧЕВЫХ ИГРОКОВ ФИНАНСОВОГО РЫНКА

ТОП-3 ИСПОЛЬЗУЕМЫХ РЕШЕНИЙ ПО ОТКРЫТОЙ ЛИЦЕНЗИИ

Управление данными	Управление жизненным циклом ML-модели	Управление данными

Популярность применения открытого исходного кода организациями российского финансового рынка также подтверждается результатами проведенного **исследования уровня технологической готовности и цифровой зрелости – все** опрошенные организации (100%) подтвердили, что **применяют открытое ПО** в своих разработках.

ВЫЗОВЫ ОТКРЫТОГО ИСХОДНОГО КОДА

Использование решений с открытым кодом становится все более распространенным, предоставляя множество преимуществ, таких как экономия времени и ресурсов на разработку. Однако такой подход, как и любой другой, также обладает рядом рисков.

ОГРАНИЧЕНИЯ ПО ЗАКУПКАМ ЛИЦЕНЗИЙ

Компания может столкнуться с ограничениями на использование открытого исходного кода в коммерческих целях или на продажу продуктов, основанных на этом коде. Некоторые лицензии могут также требовать, чтобы компания открыла свой собственный код и поделилась им с сообществом разработчиков. Это может привести к тому, что компания не сможет полностью контролировать свое ПО и не сможет получать прибыль от продажи продуктов, основанных на нем. Кроме того, ограничения по лицензированию могут привести к проблемам совместимости и функциональности, если организация не может использовать необходимые компоненты или библиотеки, которые требуются для работы ее ПО.

ОГРАНИЧЕНИЯ НА ЗАРУБЕЖНЫЕ ИТ-ПРОСТРАНСТВА

Компания может столкнуться с ограничениями на доступ к открытому исходному коду, хранящемуся за рубежом. Это может быть вызвано политическими, экономическими или юридическими причинами. Например, некоторые страны могут запретить доступ к отдельным сайтам или сервисам, которые содержат открытый код. Кроме того, некоторые страны могут требовать, чтобы организации хранили код своих решений на серверах внутри страны или использовали только локальные инструменты для разработки ПО. Это может привести к тому, что компания не сможет получить доступ к необходимым компонентам или библиотекам, которые хранятся в другой стране, что может привести к проблемам интероперабельности и функциональности ее ПО.

НАЛИЧИЕ ЗАКЛАДОК И BACKDOOR

Закладки – это специальные участки кода, которые могут быть внедрены в исходный код программного обеспечения, а также использованы злоумышленниками для получения доступа к корпоративным системам, нарушения конфиденциальности данных и проведения кибератак. Backdoor представляет собой скрытый канал в ПО, который может быть использован для получения несанкционированного доступа к системам и данным компании. Он может быть создан злоумышленниками или даже разработчиками с целью облегчения технической поддержки или обновления технического решения.

ОБНОВЛЕНИЕ ЗАВИСИМОСТЕЙ

В данном случае риск возникает из-за того, что многие программы используют сторонние библиотеки и компоненты, которые могут содержать уязвимости и лозунги. Обновление зависимостей может привести к нарушению работы приложения или даже к появлению новых уязвимостей. Например, если приложение использует для обработки изображений стороннюю библиотеку, содержащую уязвимость, то при ее обновлении ПО может перестать работать или стать уязвимой для кибератак.

НЕОБХОДИМОСТЬ В ОРГАНИЗАЦИИ ФОРКОВ

Риск возникает в случае, когда разработчикам необходимо изменить исходный код сторонней зависимости с целью исправить ошибку или добавить новый функционал. Если изначальная зависимость перестает поддерживаться сообществом, то разработчики могут быть вынуждены создавать собственную версию зависимости – форк. Форки создают дополнительные риски для проекта, так как могут привести к разделению кодовой базы и увеличению сложности поддержки. Кроме того, форки могут содержать свои уязвимости и ошибки, которые не будут исправлены в изначальной зависимости.

ОГРАНИЧЕНИЯ РОССИЙСКИХ АНАЛОГОВ ПО

Риск возникает в случае использования ПО, которое не соответствует законодательству РФ. Например, в России действует закон «О персональных данных», который устанавливает требования к обработке данных граждан России. Использование иностранного ПО, которое не соответствует этим требованиям, может привести к нарушению закона и штрафам. Кроме того, Россия также имеет свои национальные стандарты и требования к информационной безопасности, которые могут отличаться от международных. Из-за использования иностранного ПО, не соответствующего этим требованиям, могут повыситься риски для информационной безопасности.

Ключевой вызов открытого исходного кода – ограничение доступа к иностранному ПО

Таким образом, решения с открытым кодом имеют свои преимущества, такие как более прозрачный и доступный код, возможность участия в разработке и улучшении продукта, а также экономия на лицензионных платежах. Однако, при использовании таких решений необходимо учитывать и вышеупомянутые риски.

Для обеспечения безопасности ПО необходимо внедрять методы **безопасной разработки.** Это означает, что **безопасность должна обеспечиваться на всех этапах – от планирования до сопровождения конечного продукта**. Такой подход позволяет выявлять и устранять уязвимости на ранних этапах разработки, что снижает риски для пользователя.

Безопасная разработка

В последние годы наблюдается резкий рост интереса к безопасной разработке ПО.
Это обусловлено рядом факторов:

увеличением числа кибератак и утечек данных;

усилением нормативных требований к организациям
по части информационной безопасности и защиты данных;

зависимостью бизнеса от технологий.

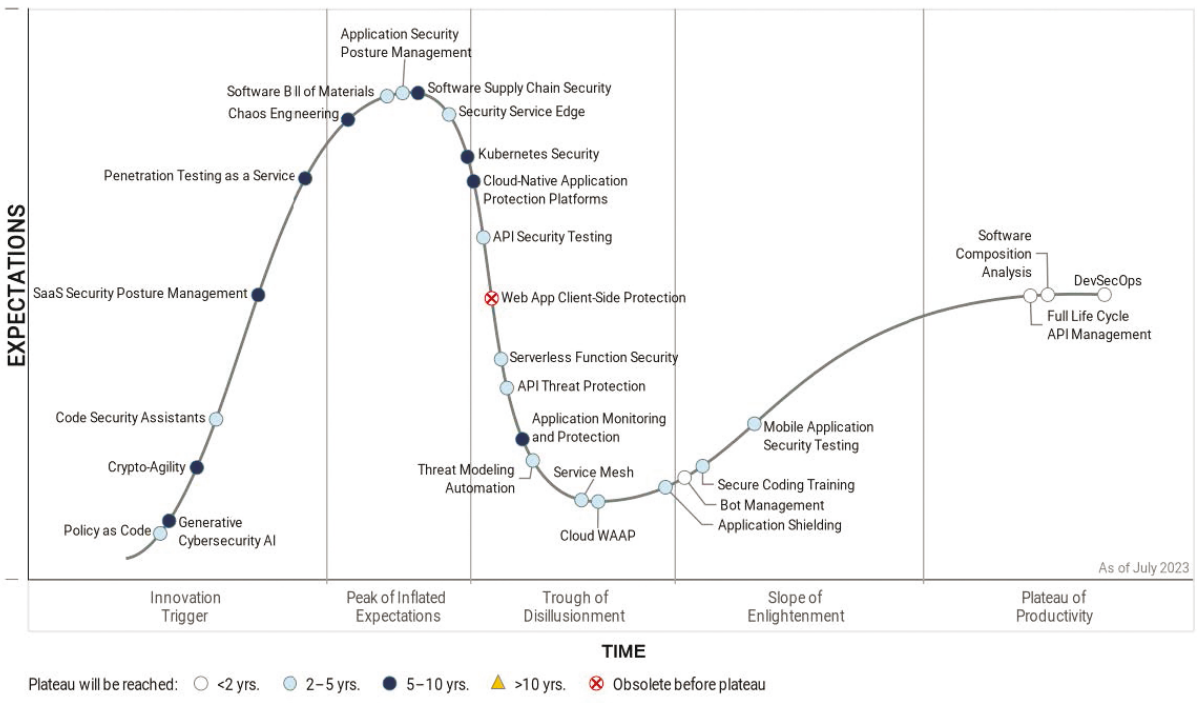
Безопасная разработка (DevSecOps) – подход к интеграции и автоматизации тестирования безопасности и соответствия нормативным требованиям в гибкие конвейеры разработки IT и DevOps, не снижающий гибкость и скорость работы разработчиков и не требующие от них выхода из системы разработки.

Безопасная разработка может быть внедрена как в последовательных моделях организации процесса (Waterfall), так и в гибких методологиях (Agile, DevOps). В данном материале фокус сделан на гибких подходах, так как именно они наиболее часто используются в проектах технологических лидеров.

ВАЖНОСТЬ БЕЗОПАСНОЙ РАЗРАБОТКИ

DevSecOps – это средство эффективной интеграции практик информационной безопасности в процесс разработки, позволяющее устранить или уменьшить трения между безопасностью и разработкой. Целью DevSecOps является достижение безопасного и работоспособного жизненного цикла разработки ПО (Software Development Life Cycle, SDLC). Безопасная разработка является развитым технологическим подходом по мнению аналитического агентства Gartner. В недавно опубликованном отчете[10] об актуальных трендах и этапах развития технологий в обеспечении безопасности предложений, эксперты оценили уровень развития DevSecOps как «зрелый мейнстрим».

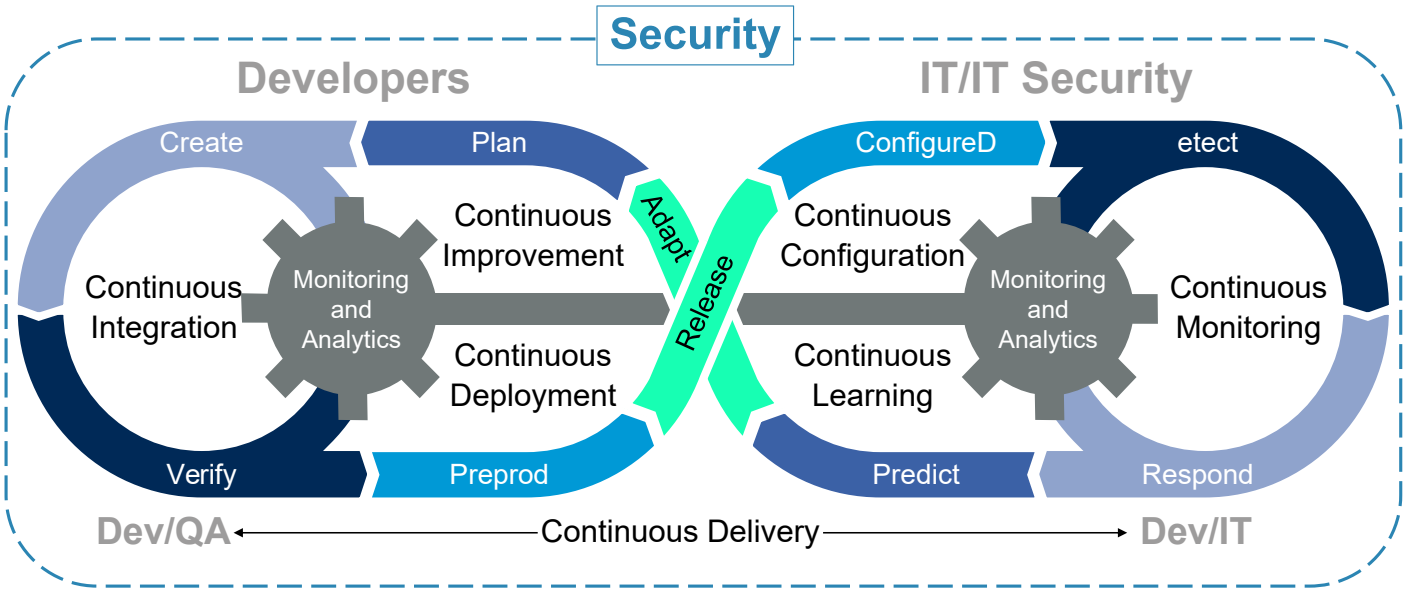
GARTNER HYPE CYCLE FOR APPLICATION SECURITY, 2023



[10] Gartner: Hype Cycle for Application Security, 2023

Стимулом для укрепления позиций концепции безопасной разработки является значительное повышение риска непреднамеренного использования разработчиками известных уязвимых компонентов и фреймворков при использовании открытого исходного кода. Подход DevSecOps стоит применять как можно раньше в процессе разработки, в то время как традиционные средства тестирования безопасности приложений (AST), связанные с более старыми моделями разработки, применяются на поздних этапах цикла и вызывают недовольство разработчиков и корпоративных стейкхолдеров.

ЦИКЛ БЕЗОПАСНОЙ РАЗРАБОТКИ GARTNER



ОСНОВНЫЕ ПРАКТИКИ DEVSECOPS

Подавляющая доля нарушений безопасности происходит по причине использования злоумышленниками известных программных ошибок. Поэтому крайне важно устранять уязвимости на этапе разработки ПО для снижения рисков информационной безопасности. Существует ряд технологий, которые помогают выявлять недостатки безопасности на ранних этапах и устранять их до релиза продукта:

Системы анализа состава ПО (SCA) – специализированные средства обеспечения безопасности приложений, позволяющие обнаруживать открытое ПО и компоненты сторонних производителей, имеющие уязвимости в системе безопасности, выявлять потенциально неблагоприятные риски лицензирования и цепочки поставок. SCA сегодня считается основополагающим элементом тестирования безопасности приложений (AST).

Тестирование безопасности приложений (AST) – процесс выявления и устранения уязвимостей в приложениях. Он может выполняться вручную или быть автоматизирован.

Кроме SCA существуют и другие типы AST, в том числе:

Статическое тестирование (SAST) – в рамках подхода происходит сканирование исходного кода приложения на наличие потенциальных уязвимостей;

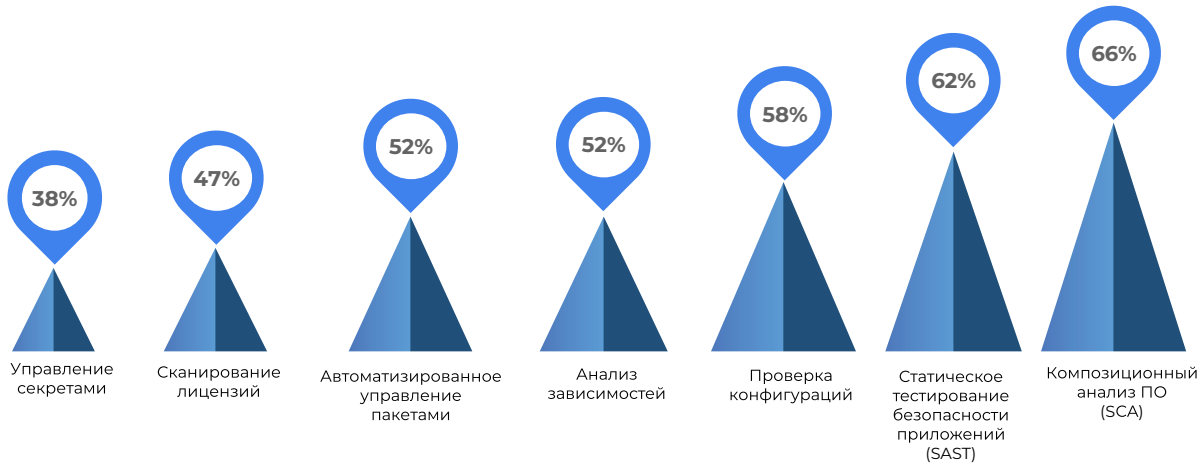
Динамическое тестирование (DAST) – в рамках подхода производится симулирование атак на приложение для проверки уязвимостей;

Интерактивное тестирование (IAST) – подход сочетает в себе практики SAST и DAST, динамически анализируя приложение во время его работы.

Глобально в рамках безопасной разработки компании **наиболее активно применяют композиционный анализ ПО (66%) и статическое тестирование безопасности приложений (SAST) (62%).** Также значительную популярность имеют проверка конфигураций (58%), автоматизированное управление пакетами и анализ зависимостей (52%). Эти инструменты позволяют обеспечить высокий уровень безопасности при разработке программного обеспечения, что является критически важным в современном мире информационных технологий.

ВНЕДРЕННЫЕ ПРОЦЕССЫ DEVSECOPS В ГЛОБАЛЬНОМ РАЗРЕЗЕ

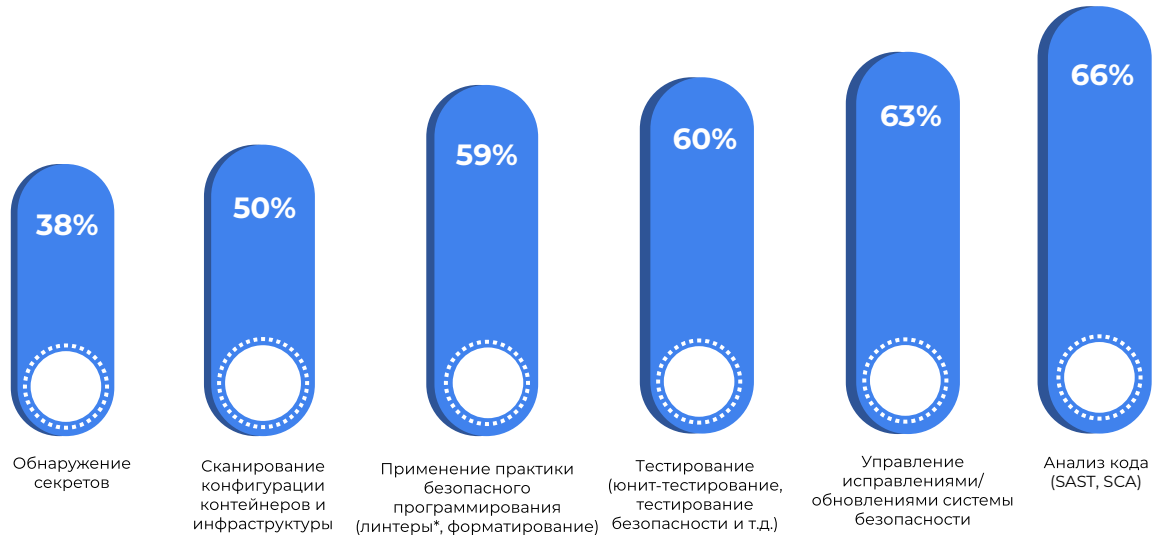
Источник: Snyk



Несмотря на то, что количество кибератак с каждым годом увеличивается, в частности, на открытый код, **40% мировых организаций по-прежнему не используют две наиболее фундаментальные технологии цепочки безопасности – SCA и SAST**. Еще меньшее число компаний применяют «облачные» меры безопасности, такие как проверка конфигурации инфраструктуры как инструмента кода и сканирование секретов[11].

АВТОМАТИЗИРОВАННЫЕ ПРОЦЕССЫ DEVSECOPS

Источник: Snyk



Автоматизация мер безопасности на различных этапах жизненного цикла разработки осуществляется **в большей степени** при **анализе кода** (66%), **управлении исправлениями системы безопасности** (63%), в **процессах тестирования** (60%), а также в применении **практики безопасного программирования** (59%).

Устранение последствий инцидента выходит гораздо дороже, чем применение мер по недопущению изъянов. Практики безопасной разработки позволяют создать продукты, которые содержат меньшее число уязвимостей. Так организации сокращают затраты на доработки продуктов после проведения финальных тестов безопасности.

[11] Управление секретами – это практика, позволяющая разработчикам надежно хранить конфиденциальные данные, такие как пароли, ключи и маркеры, в защищенной среде со строгим контролем доступа.

* Линтер – программа, проверяющая код на соответствие стандартам, согласно определенному набору правил. Правила описывают отступы, названия создаваемых сущностей, скобки, математические операции и другие аспекты.

РЫНОЧНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Развитие новых инструментов и технологий способствует увеличению интереса к безопасной разработке, и на российском рынке представлены эффективные продукты для статитического, динамического и интерактивного анализа кода, решения по обнаружению уязвимостей в автоматическом режиме, мониторинг сетевой активности и пр. С точки зрения конкурентоспособного технологического стека **Россия занимает сильную позицию** – на отечественном рынке **присутствуют ключевые системные инструменты сборки, анализа и тестирования**, обеспечивающие **полный цикл безопасной разработки**.

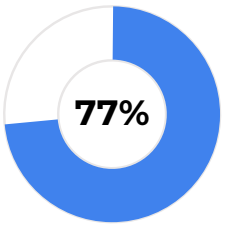
На сегодняшний день под угрозой кибератак находятся не только крупные финансовые организации, но практически любая российская компания с ИТ-инфраструктурой. Так, РТК-Солар, провайдер сервисов и технологий ИБ, отметила, что **количество инцидентов[12] в рамках информационной безопасности** во 2 квартале 2023 г. **выросло на 12%** в сравнении с 1 кварталом 2023 г., а также более, чем на **75%** в сравнении с 1 кварталом 2022 г. В другом отчете[13] РТК-Солар отмечает, что киберпреступники сменили ландшафт угроз. Это связано с тем, что значительно повысились объем идеологически мотивированных атак и количество автоматизированных инструментов, облегчающих типовые кибератаки.

Хакеры чаще стали прибегать к кибербразведке, а атаки становятся все более сложными. На сегодняшний момент невозможно полностью защититься, создавая только периметр безопасности. **Огромное количество уязвимостей возникает непосредственно в коде приложений, и устранять их достаточно затруднительно, особенно когда приложение уже разработано.** На рынке встал вопрос безопасности используемого открытого кода, так как с недавних пор в него стали добавляться закладки[14] и иной контент, нежелательный для российских организаций.

«Практики безопасной разработки помогают обеспечить надлежащую безопасность итогового продукта компании и ускорить процесс его вывода на рынок. Именно поэтому DevSecOps оказался актуален, как никогда».

Сергей Демидов
Директор Департамента операционных рисков,информационной безопасности и непрерывности бизнеса Московской Биржи

Согласно оценкам заместителя генерального директора, «Гарда Технологии» Владимира Пономарева, при внедрении практик безопасной разработки можно **«смело прибавлять 7–10% к текущим затратам на разработку»**. Кроме того, при использовании инструментов на базе ИИ, генерирующих код, отмечается повышение уровня безопасности разработки.



компаний отметили повышение качества безопасной разработки при использовании инструментов ИИ, генерирующих код

По мнению Gartner, внедрение DevSecOps-практик позволяет сократить общие затраты на проект на 25%.

[12] РТК-Солар: «Атаки на российские компании во II квартале 2023 года».

[13] РТК-Солар: «Отчет о ключевых внешних цифровых угрозах для российских компаний».

[14] Закладкой (или программной закладкой) в информационной безопасности называют скрытно внедренную в защищенную систему программу, либо намеренно измененный фрагмент программы, которая позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

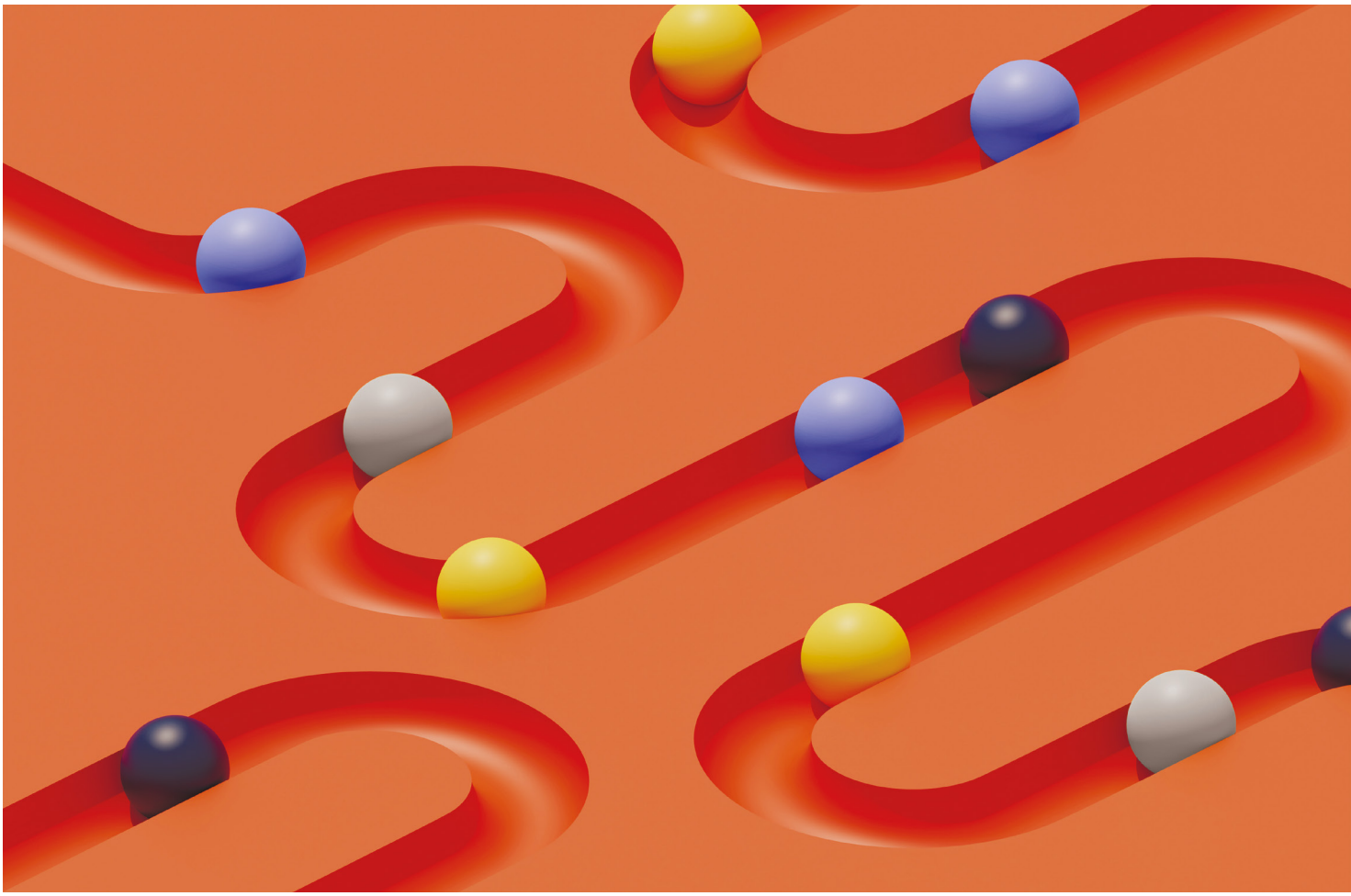
РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Требования к безопасности ПО в финансовом секторе прописаны в положениях Банка России 683-П[15] и 757-П[16]. Они обязывают финансовые организации использовать ПО, которое либо прошло оценку в системе сертификации Федеральной службы по техническому и экспортному контролю (ФСТЭК), либо прошли оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже, чем ОУД 4, в соответствии с требованиями национального стандарта ГОСТ 15408[17].

Система сертификации ФСТЭК сильно перегружена. Срок проверки одного экземпляра ПО составляет полгода, а иногда достигает 9–12 месяцев. При надлежащей частоте релизов банковского ПО в 2 недели данное условие выглядит мало приемлемым.

По этой причине финансовые организации присматриваются к ГОСТ Р 15408. Механика работы ГОСТ Р 15408 неочевидная: стандарт описывает только общие практики к обеспечению безопасности ПО. Поэтому Банк России разработал методический документ «Профиль защиты»[18] для финансового сектора, покрывающий как требования к безопасности ПО общего назначения, так и требования со стороны Банка России для кредитных и некредитных финансовых организаций.

Безопасная разработка – эффективный инструмент снижения общего страхового киберриска.



[15] Положение Банка России от 17.04.2019 N 683-П (ред. от 18.02.2022) «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

[16] Положение Банка России от 20.04.2021 N 757-П (ред. от 20.04.2021) «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

[17] ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

[18] Полное наименование: «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

БЕЗОПАСНАЯ РАЗРАБОТКА: КЕЙС МОСКОВСКОЙ БИРЖИ

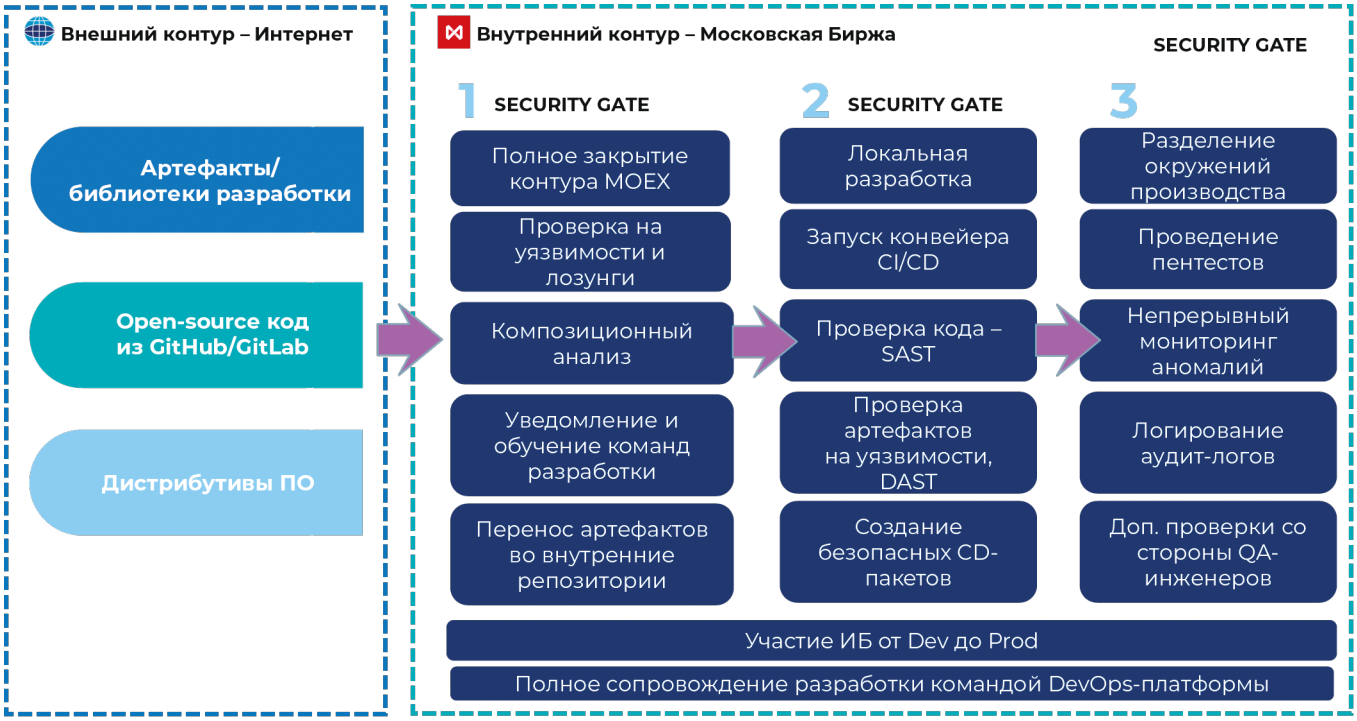
В качестве примера практического кейса применения безопасной разработки рассмотрим опыт члена Ассоциации ФинТех – Московской Биржи:

ФУНКЦИОНАЛ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ВНЕШНИХ БИБЛИОТЕК

В рамках безопасной разработки на платформе DevOps существует сервис DOPSecurity. Данный продукт используется для автоматической загрузки объектов проверки и зависимостей в карантин с последующей передачей на проверку специалистам Лаборатории информационной безопасности. После прохождения проверки, на платформе доступен отчет и резолюция по допустимости использования объектов. На настоящий момент доступны следующие типы загрузок:

Особенность решения в том, что сервис не только загружает объекты и зависимости в карантин, но еще и проводит сканирование данных артефактов[23] автоматизированными средствами, что сокращает трудоемкость и время проверки. Это стало особенно актуально, когда многие внешние артефакты стали содержать в себе закладки и лозунги.

ФУНКЦИОНАЛ SECURITY GATES В КОНВЕЙЕРАХ РАЗРАБОТКИ И В ПРАКТИКЕ НЕПРЕРЫВНОЙ ИНТЕГРАЦИИ И ДОСТАВКИ (CI/CD)



В каждом из конвейеров внедрены этапы проверки кода и артефактов на уязвимости по базам данных уязвимостей.

[19] Docker Images – шаблоны (образы) для создания контейнеров в Docker, содержащие все необходимые компоненты, такие как операционная система, приложения, библиотеки и другие зависимости

[20] Node Package Manager (NPM) – менеджер пакетов для языка программирования JavaScript. Он позволяет устанавливать и управлять зависимостями проекта, а также использовать готовые модули и библиотеки, созданные другими разработчиками. NPM входит в состав Node.js – среды выполнения JavaScript на сервере

[21] Python-пакеты – наборы модулей, которые позволяют расширять функциональность языка Python. Могут содержать как стандартные библиотеки, так и сторонние модули, разработанные сообществом Python.

[22] Maven – инструмент для управления проектами на языке программирования Java

[23] Артефакт — это любой созданный искусственно элемент программной системы. К элементам программной системы, а, следовательно, и к артефактам, могут относиться исполняемые файлы, исходный код, веб страницы, справочные файлы и многое другое, являющееся носителем информации.

ЦЕНТР КОМПЕТЕНЦИЙ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ АФТ

Ассоциация ФинТех совместно с **Московской Биржей** и другими ключевыми участниками финансового рынка создают отраслевой центр компетенций по безопасной разработке и проверке решений на основе свободного программного обеспечения (СПО).

Цель создания центра: обеспечение понятного и прозрачного процесса внедрения безопасной разработки и использования свободного программного обеспечения на финансовом рынке.

ОСНОВНЫЕ ЗАДАЧИ ЦЕНТРА:

- **Консолидация опыта, знаний и компетенций участников АФТ по безопасной разработке и применению СПО;**
- **Анализ и разъяснение требований, формирование предложений и рекомендаций по совершенствованию нормативного регулирования;**
- **Согласование типового технологического стека;**
- **Разработка и поддержка методологии процессов безопасной разработки;**
- **Организация обучения специалистов;**
- **Поддержка и консультация специалистов и участников АФТ;**
- **Идентификация, оценка и тестирование ИТ-решений на основе СПО;**
- **Организация совместных проектов по развитию ИТ-решений на основе СПО.**

*«Вместе с специалистами Московской Биржи планируем создать **сообщество экспертов**, совместная работа которых **упростит процесс внедрения DevSecOps**, что приведет к **повышению уровня защищенности разрабатываемых решений** и, как результат, выполнению задачи достижения требуемого уровня технологической независимости организаций»*

Олег Моргун
Руководитель управления развития технологий АФТ

Для решения задач по размещению, хранению и проверке решений на основе открытого кода будет использоваться созданный АФТ **Репозиторий ИТ-решений для финансовой отрасли**. Реализация проектов по развитию ИТ-решений на основе СПО будет происходить на платформе ранее запущенной **Технологической песочницы АФТ.**

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ

Безопасность приложений является одним из **важнейших аспектов** при разработке программного обеспечения. Необходимо учитывать потенциальные уязвимости и риски, связанные с конфиденциальной информацией, а также возможностью атак со стороны злоумышленников. Таким образом, при внедрении безопасной разработки необходимо руководствоваться **комплексом мер:**

1 ОЦЕНИВАТЬ РИСКИ

Применение инструментария безопасной разработки для каждой строчки кода на практике не реализуемо. Организация должна понимать, **насколько безопасной** должна быть разработка, и сосредоточить усилия на ПО, подверженном наибольшему риску.

2 ПЛАНИРОВАТЬ ПРОЦЕСС ВНЕДРЕНИЯ БЕЗОПАСНОЙ РАЗРАБОТКИ

Необходимо **спланировать внедрение** безопасной разработки и **выработать метрики** для каждого этапа. Так получится оценивать успешность внедрения, и метриками смогут быть результаты проверки безопасности итогового продукта. Эти же метрики помогут оценить **экономический эффект внедрения** безопасной разработки, поскольку будет видно, как каждый этап влияет на общий уровень безопасности конечного продукта. Может выясниться, что часть инструментария безопасной разработки в действительности не нужна, поскольку не добавляет ожидаемого уровня безопасности.

3 ВЫБИРАТЬ ИНСТРУМЕНТЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

Выбор инструментария для безопасной разработки обширен, даже после ухода зарубежных вендоров. Замглавы Минцифры Александр Шойтов заявил, что **доля российских средств защиты информации** на рынке составляет около **90%**. Многие инструменты распространяются по открытой лицензии. С них и стоит **начинать внедрение практик безопасной разработки**, поскольку они позволяют запустить процесс без серьезных инвестиций. Определив узкие места, инструментарий в них можно будет усилить, а где-то обойтись базовыми решениями.

4 УКРЕПЛЯТЬ ВЗАИМОДЕЙСТВИЕ МЕЖДУ РАЗВИТИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Между разработчиками и специалистами по информационной безопасности должен быть выстроен **здравый диалог**. У продуктовой команды должны быть выставлены сбалансированные КПЭ как по метрикам безопасности, так и по времени сдачи проекта.

ПЕРСПЕКТИВЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

Рынок кибербезопасности Российской Федерации **по результатам 2022 года** оценивается[24] в **193,3 млрд руб.**, а **к 2027** должен составить **559 млрд руб.** На рынке продуктов средств защиты информации (СЗВ) в 2022 году **положение российских вендоров усилилось:** они занимают **70%** рынка. Прирост доли рынка от года в год составил 15%.

На настоящий момент Правительством РФ проводится **эксперимент по созданию условий для использования программного обеспечения в условиях открытой лицензии[25].** Основными целями эксперимента заявляются обеспечение повторного использования программ для ЭВМ и внедрение передовых практик создания и развития ПО. В рамках данного эксперимента **планируется ввести русскоязычные открытые государственные лицензии**, которые будут **одновременно соответствовать и требованиям OSI к открытым лицензиям, и гражданскому кодексу РФ,** а также не предусматривать авторское лево (copyleft).

В то же время проводится **эксперимент по созданию национального репозитория** – отечественного аналога GitHub. Основными целями эксперимента в РФРИТ определили:

поддержку сообщества разработчиков ПО с открытым кодом;

создание **среды** для их совместной работы;

увеличение участия **российских компаний** в разработке.

Безопасный *доверенный репозиторий,* соответствующий требованиям Минцифры, будет *создаваться и на базе Ассоциации ФинТех*.

Решения с открытым кодом являются важным фактором для развития финансового сектора, так как они представляют собой наиболее современные технологические практики, позволяют гибко их настраивать под нужды конкретного продукта и обходятся дешевле, чем проприетарные аналоги. Благодаря доступности кода разработчики могут анализировать его на предмет уязвимостей и исправлять их, что способствует повышению уровня безопасности приложений. Разработчики и организации финансового сектора должны уделять особое внимание использованию открытого кода и обеспечению его безопасности для защиты пользователей и повышения доверия к сервисам.

Таким образом, **безопасная разработка – это не только обеспечение безопасности, но и безопасного развития.** Практики безопасной разработки позволяют обеспечить баланс между рисками и развитием, необходимый российскому финтеху.

*Особая благодарность **Сергею Демидову** за помощь в подготовке материала*

[24]Центр стратегических инициатив: «Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы».

[25]Подробнее в постановлении Правительства Российской Федерации от 10.10.2022 № 1804 «О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения».

ПОЧИТАТЬ ДОПОЛНИТЕЛЬНО ПО ТЕМЕ:

РТК-Солар

Отчет о ключевых внешних цифровых угрозах для российских компаний в январе-апреле 2023 года

Endor Labs

Топ-10 рисков, связанных с открытым исходным кодом

АНО «Открытый код»

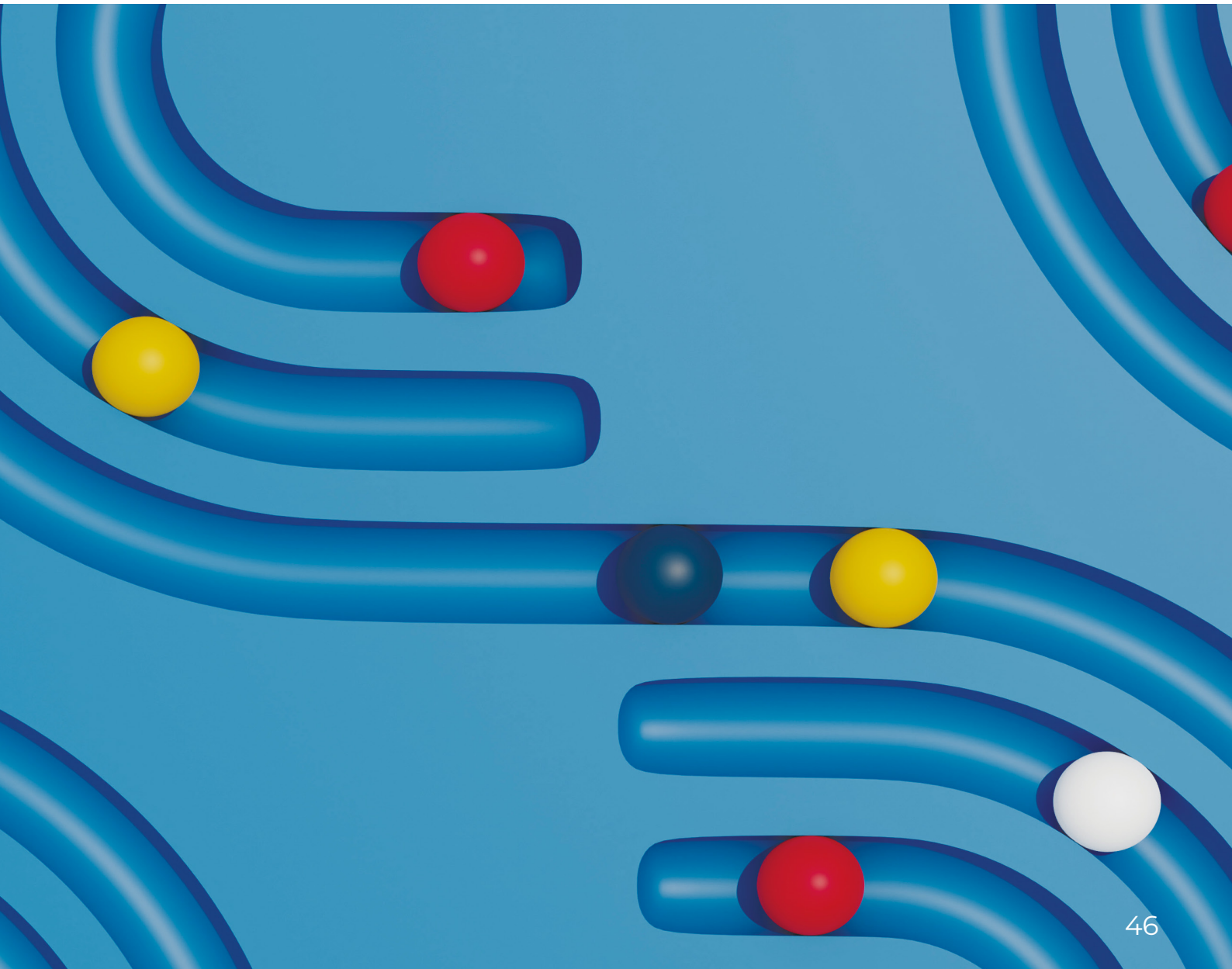
О корректном использовании ОСПО–компонент при создании и коммерциализации программных продуктов

Open Logic x OSI

Отчет о состоянии открытого ПО на 2023 год

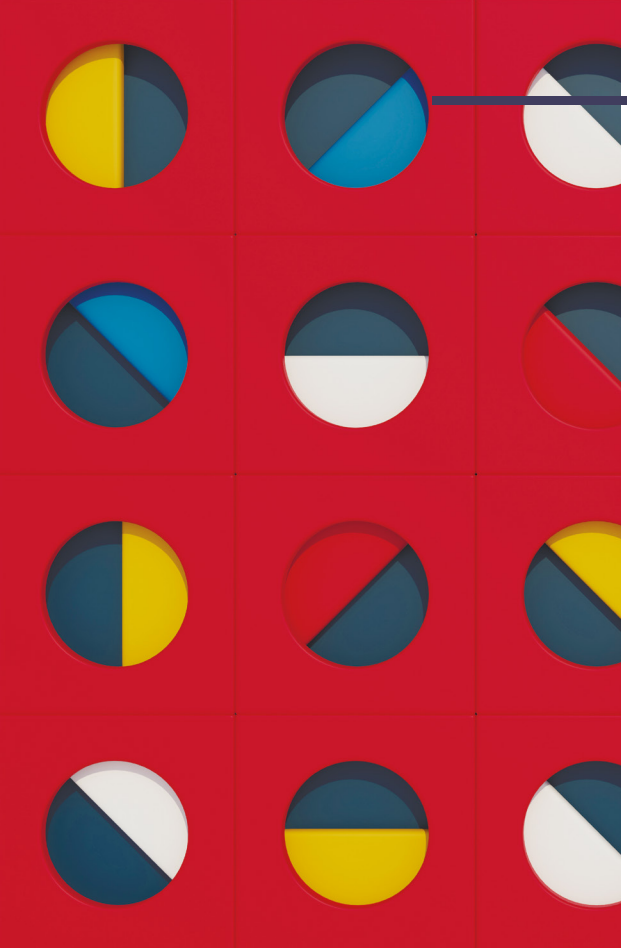
Red Hat

Отчет о состоянии открытого ПО на предприятиях: финансовый сектор



ДЛЯ ЗАМЕТОК

АНАЛИТИЧЕСКИЕ
МАТЕРИАЛЫ АФТ



АССОЦИАЦИЯ ФИНТЕХ ИССЛЕДОВАНИЯ И АНАЛИТИКА

МАРИАННА ДАНИЛИНА
Руководитель Управления исследований и аналитики
m.danilina@fintechru.org

ДАРЬЯ ПЕТРОВА
Ведущий бизнес-аналитик по исследовательской деятельности
d.petrova@fintechru.org

ГРИГОРИЙ КАРУНАС
Бизнес-аналитик по информационным сервисам
g.karunas@fintechru.org

TELEGRAM КАНАЛ

WWW.FINTECHRU.ORG

Информация, содержащаяся в настоящем материале, предназначена только для информационных целей и не является профессиональной консультацией или рекомендацией. Ассоциация ФинТех не дает обещаний или гарантий относительно точности, полноты, адекватности, своевременности или актуальности информации, содержащейся в материале.

Ассоциация ФинТех оставляет за собой право вносить изменения в информацию, содержащуюся в материале, однако не берет на себя обязательств по обновлению такой информации после даты, указанной в настоящем документе, несмотря на то что информация может стать устаревшей, неточной или неполной.

Ассоциация ФинТех не проводила независимую проверку данных и предположений, использованных в настоящем материале.

Ассоциация ФинТех не несет никакой ответственности за любой ущерб, который может быть причинен в любой форме любому лицу вследствие использования, неполноты, некорректности, неактуальности любой информации, содержащейся в материале.

Материалы полностью или частично нельзя распространять, копировать или передавать какому-либо лицу без предварительного письменного согласия Ассоциации ФинТех.