ФИНТЕХ
АССОЦИАЦИЯ

Безопасность Открытых API

Товстолип Александр,

Ассоциация ФинТех

конференция
РусКрипто

Содержание

Открытые API

программные интерфейсы, публикуемые организациями в соответствии с требованиями Банка России для обеспечения возможности цифрового обмена данными с поставщиками услуг (с согласия клиента) и клиентами в рамках организации и предоставления финансовых услуг.

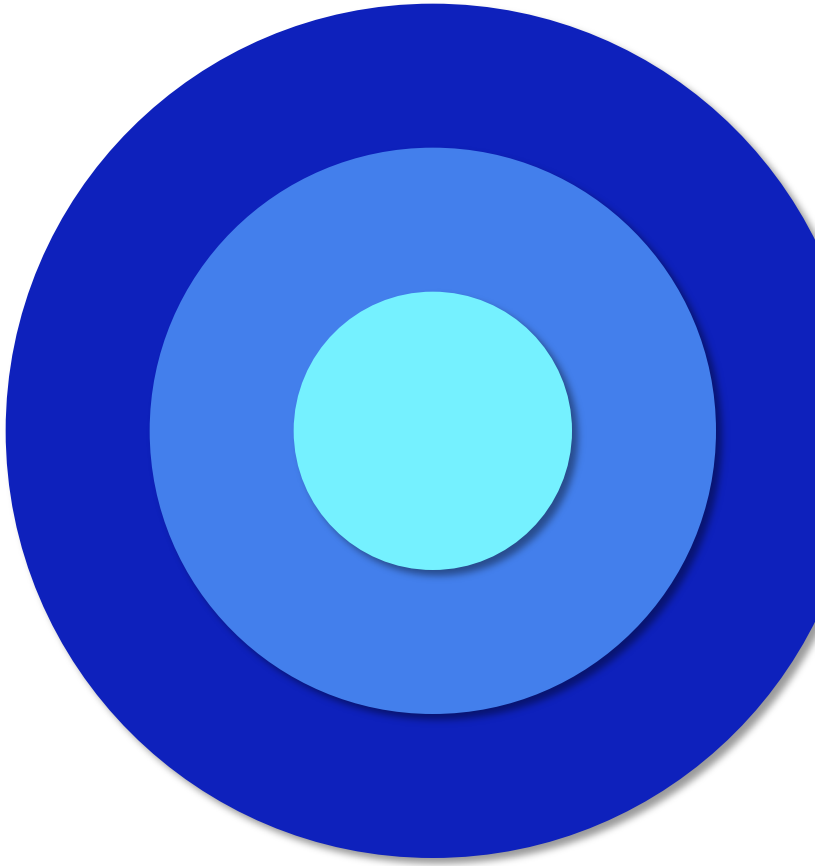
Открытые API – технология, которая лежит в основе моделей внедрения концепций отрытого банкинга, открытых финансов и открытых данных.

ОТКРЫТЫЙ БАНКИНГ

модель, предполагающая получение поставщиками услуг банковских и платежных данных о клиенте, а также осуществление банковских операций по его поручению.

ОТКРЫТЫЕ ФИНАНСЫ

модель, в рамках которой поставщики услуг получают не только банковские и платежные данные о клиенте, но и данные об иных финансовых услугах: страховые, инвестиционные, пенсионные и другие.



ОТКРЫТЫЕ ДАННЫЕ

модель, которая распространяет требование к установлению открытого обмена клиентскими данными как на финансовые, так и на нефинансовые организации (например, организации в сфере телекоммуникаций, электронной коммерции и так далее), а также на государственные информационные базы, в которых хранятся и обрабатываются клиентские данные.

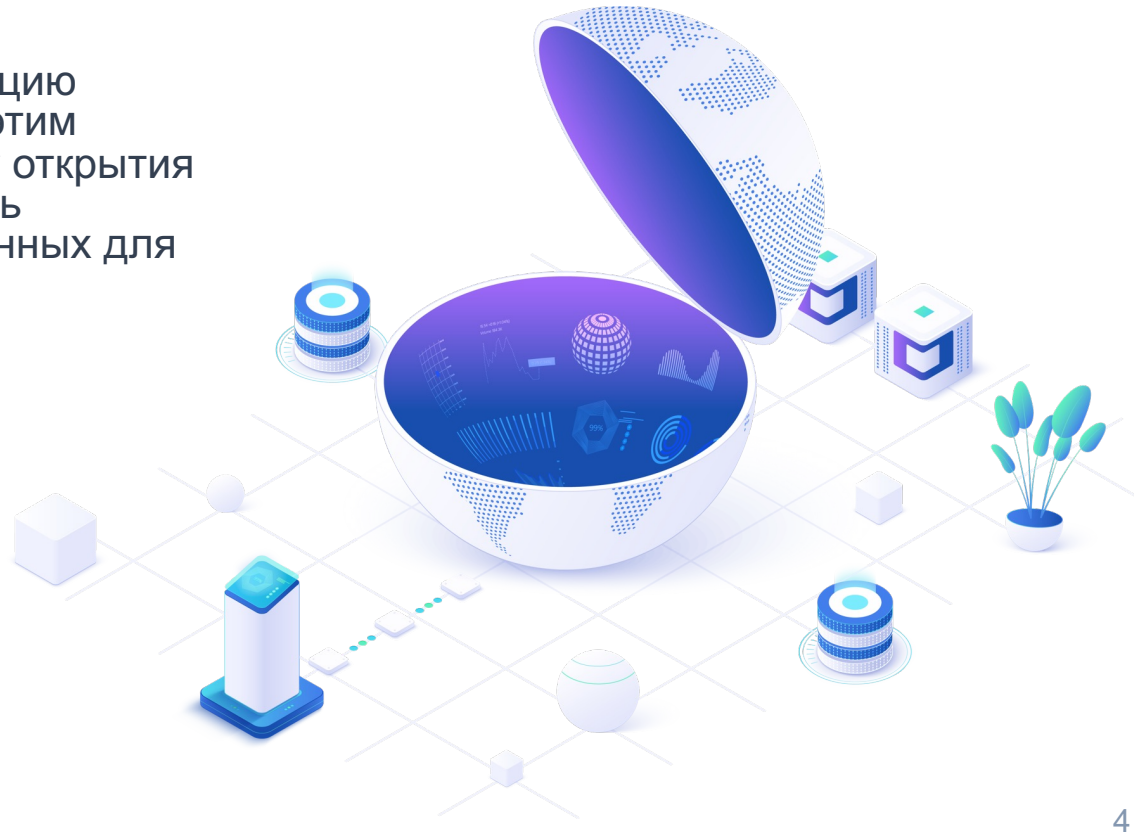
Открытые API

Сегодня различные страны уже внедряют технологии Открытых API не только на финансовый, но и на другие рынки для развития экономики и улучшения клиентского опыта.

Делается большой фокус на человекоцентричность финтех-сервисов.

Внедрение концепции Открытых API предполагает обмен именно клиентскими персональными данными между компаниями.

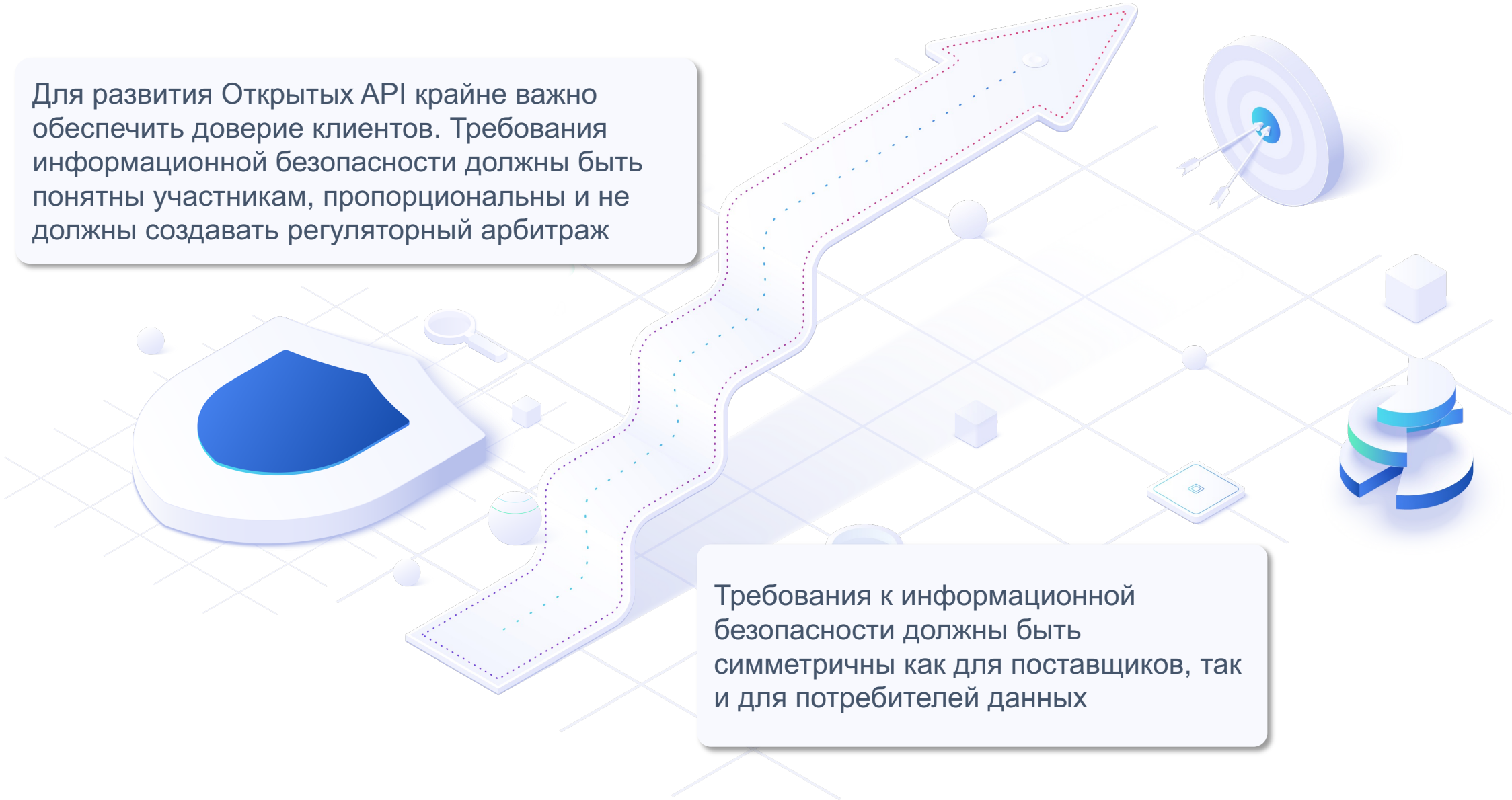
В 2022 году Банк России разработал и опубликовал Концепцию внедрения Открытых API на финансовом рынке. В связи с этим российскому рынку, который уже начал движение в сторону открытия данных, очень важно обеспечить их сохранность и повысить уверенность клиентов в безопасности предоставленных данных для успешного развития сервисов на базе Открытых API.



https://cbr.ru/Content/Document/File/142114/concept_09-11-2022.pdf

Безопасность Открытых API

Для развития Открытых API крайне важно обеспечить доверие клиентов. Требования информационной безопасности должны быть понятны участникам, пропорциональны и не должны создавать регуляторный арбитраж



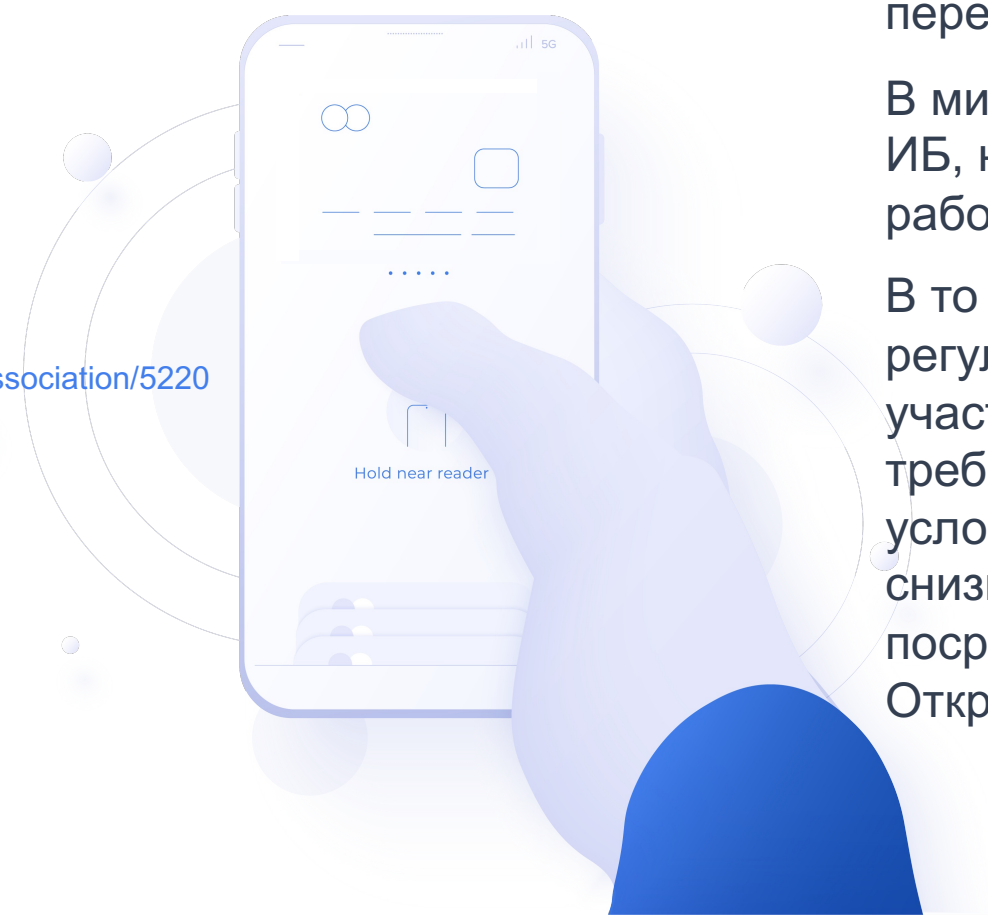
Требования к информационной безопасности должны быть симметричны как для поставщиков, так и для потребителей данных

Доверие к Открытым API

«ВЫСОКИЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОВЫШАЕТ ДОВЕРИЕ К API»

Из исследования АФТ

https://t.me/fintechassociation/5220



Анализ международного опыта показал, что ряд стран не принял специализированное регулирование по обеспечению информационной безопасности в рамках передачи данных с помощью стандартов API.

В мире придерживаются общих требований ИБ, не ниже существующих требований при работе с конфиденциальными данными.

В то же время в ЕС изучается возможность регулирования в области ИБ для новых участников Открытого Банкинга. Различия в требованиях к обеспечению ИБ могут создать условия для регулятивного арбитража и снизить интерес участников взаимодействия посредством Открытых API к развитию Открытых Финансов.

Безопасность Открытых API

Для обеспечения необходимого уровня безопасности при взаимодействии организаций с использованием Открытых API в процессе обмена данными о клиентах и их продуктах предполагается проработка следующих вопросов:

• регулирование деятельности и надзор за организациями, осуществляющими обмен данными с использованием Открытых API, в области обеспечения защиты информации;

• стандартизация и контроль реализации требований по информационной безопасности к протокольному решению, используемому при создании Открытых API.

В целях обеспечения защиты информации при взаимодействии организаций с использованием Открытых API необходимо разработать набор требований к проектируемым API и приложениям. Такой набор требований должен учитывать вопросы:

- безопасной разработки API и приложений;
- безопасности каналов связи;
- использования отечественных криптографических алгоритмов.

Что сделано на площадке АФТ

1 Стандартизация протокола

- Стандарт ФАПИ.СЕК
- Стандарт ФАПИ.ПАОК

2 Адаптация стандартов

- в 2023 добавили отечественную криптографию при согласовании ТК26, ТК122
- в 2024 планируется публикация методических рекомендаций

3 Стенд среды открытого банкинга

- реализована среда для проверки выполнения требований стандартов ФАПИ в программных решениях

Основа для долгосрочного использования стандартов в Открытом банкинге, Открытых финансах, Открытых данных

Планы

Развитие стандартов

- информационной безопасности
- прикладные стандарты

Контроль за соответствием уровня ИБ

повышение безопасности

повышение доверия

Создание (крипто)сервисов

развитие сервисов и решений для снижения порога входа в среду открытых API в части реализации требований по ИБ

СПАСИБО ЗА ВНИМАНИЕ!

Товстолип Александр

Управление информационной безопасности

Ассоциация ФинТех

telegram: @mydzen

a.tovstolip@fintechru.org

TELEGRAM-КАНАЛ АФТ

САЙТ: fintechru.org