Банк России
Центральный банк Российской Федерации

ДЕКАБРЬ 2018

ДОКЛАД
ДЛЯ ОБЩЕСТВЕННЫХ
КОНСУЛЬТАЦИЙ

ПРИМЕНЕНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ НА ФИНАНСОВОМ РЫНКЕ

МОСКВА

СОДЕРЖАНИЕ

Комментарии, включая ответы на поставленные в докладе вопросы, а также предложения и замечания просим направлять по адресу *fintech@cbr.ru*.

ВВЕДЕНИЕ

В данном докладе раскрываются основные подходы к применению облачных технологий и созданию облачной инфраструктуры на финансовом рынке, описываются сценарии применения и реализации облачных сервисов финансовыми организациями в разных странах, а также проводится анализ подходов финансовых регуляторов к управлению рисками и регулированию в соответствующей сфере.

Целью доклада является определение возможных областей применения облачных технологий в финансовом секторе, а также определение мероприятий, необходимых для развития облачных сервисов для финансового рынка и выработка рекомендаций и подходов к соответствующему регулированию.

1. ПОНЯТИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ И ПОДХОДЫ К ИХ ПРИМЕНЕНИЮ

Облачные технологии – это модель обеспечения удобного сетевого доступа по требованию к фонду конфигурируемых ресурсов (от систем хранения данных до бизнес-услуг), которые могут быть оперативно предоставлены, масштабированы и освобождены с минимальными эксплуатационными затратами и обращениями к поставщику.

Облачная инфраструктура формирует необходимые условия для реализации совместных инициатив между финансовыми организациями, финтех-компаниями и организациями иных секторов экономики, позволяет оперативно создавать новые бизнес-модели и ускоряет вывод новых продуктов на рынок.

Облачные сервисы разделяются на несколько моделей предоставления услуг – от базовых инфраструктурных сервисов до комплекса готовых бизнес-функций, например сервисов учетно-операционной деятельности.

Существуют следующие модели услуг в форме облачных сервисов:

IaaS (Infrastructure as a Service)

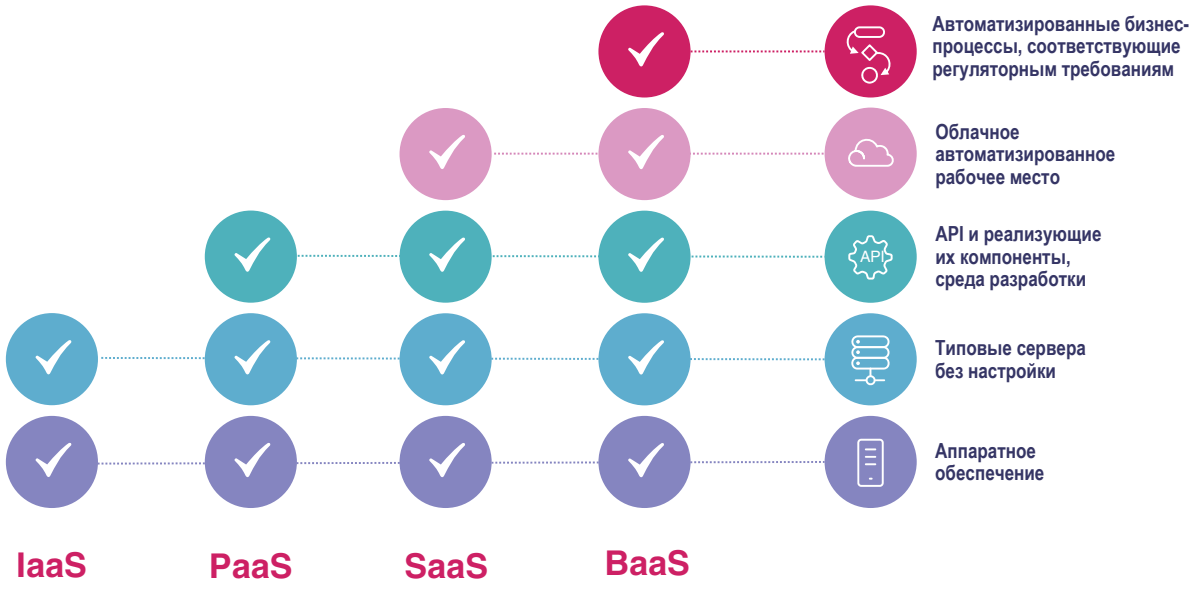
В данной модели потребитель услуг не работает с аппаратным обеспечением напрямую, а получает по подписке предварительно настроенные виртуальные серверы, обладающие заданной мощностью, пространством для хранения и доступом к сетям.

Потребитель услуг самостоятельно управляет арендованными вычислительными ресурсами, а также настраивает программное обеспечение для эксплуатации и развития своих приложений – например, в рамках управления базами данных, хранения электронных документов (ЭД) или систем для координации бизнес-процессов.

PaaS (Platform as a Service)

В данной модели потребитель услуг получает платформу с готовым набором компонентов для развития и эксплуатации

Рисунок 1
Форматы предоставления облачных услуг



собственных приложений, а также среду управления платформой, позволяющую быстро прототипировать и развертывать новые версии приложения, например мобильный банк-клиент, систему управления взаимоотношениями с клиентами (CRM) и автоматизированную банковскую систему (АБС).

SaaS (Software as a Service)

В данной модели клиент получает уже готовую функциональность в приложении, при этом развитие и сопровождение приложения остается в зоне ответственности поставщика услуги SaaS. Например, клиент может купить подписку на облачный CRM, систему автоматизации бухгалтерского учета или кадрового делопроизводства.

BaaS (Bank/Business as a Service)

Business as a service является принципиально новым уровнем применения облачных технологий, где клиенту предоставляются не технологические возможности, а готовый автоматизированный бизнес-процесс по модели подписки, которая позволяет гибко управлять объемом работ, переданных на аутсорсинг.

Например, если в модели SaaS потребитель заказывает облачную автоматизированную банковскую систему, в которой будет работать и выстраивать бизнес-процессы самостоятельно, то в BaaS он заказывает готовые учетно-операционные сервисы, не требующие затрат на их организацию.

2. ОБЛАЧНАЯ ИНФРАСТРУКТУРА ФИНАНСОВОГО РЫНКА

2.1. Сервисы облачной инфраструктуры

В данном разделе рассматриваются возможные сценарии предоставления услуг с использованием облачных технологий для финансового рынка.

Инфраструктурные услуги

На сегодняшний день в международной практике существует успешный опыт переноса в облачную инфраструктуру критических бизнес-функций, таких как учетно-операционная деятельность, управление рисками и информационная безопасность (ИБ). При этом, как правило, используется публичная облачная инфраструктура от одного из технологических гигантов, таких как Amazon, Microsoft или Google.

Примеры:

- Крупнейший цифровой банк **Capital One** (США) в 2015 г. полностью мигрировал свои среды разработки и тестирования ИТ-систем на Amazon Web Services (AWS, США), а в 2017 г. выстроил процессы миграции основных сервисов на AWS и сформировал команду в несколько тысяч сертифицированных облачных инженеров. К концу 2018 г. Capital One планирует отказаться от 5 из 8 собственных дата-центров в пользу облачной инфраструктуры в формате PaaS.
- Цифровой банк **Bunq** (Нидерланды) полностью мигрировал свои ИТ-системы на IaaS от Amazon Web Services за два года. Bunq удаленно предоставляет свои услуги клиентам в Нидерландах, Германии, Австрии, Италии и Испании из дата-центра Amazon во Франкфурте.

Помимо сценариев миграции сложившейся инфраструктуры на публичную облачную инфраструктуру, известно несколько случаев создания изначально облачных банковских ИТ-систем.

Примеры:

- **DBS Bank** (Сингапур) открыл в Индии банк DigiBank – мобильный банк-клиент в публичном облаке, который использует учетно-операционную систему материнского банка, размещенную на частной инфраструктуре.
- **Atom Bank** (Великобритания) – мобильный банк без отделений и вебсайта, развивается на облачной интеграционной платформе от поставщика MuleSoft (США). Использование облачной интеграционной платформы (integration Platform as a Service, iPaaS[1]) позволило Atom Bank реализовать полностью сквозную цифровую обработку (straight-through processing) заявок на ипотеку.
- **OakNorth Bank** (Великобритания) предоставляет кредитные и депозитные продукты малому и среднему бизнесу в режиме онлайн, используя облачную автоматизированную банковскую систему компании Mambu (Германия). Запуск АБС в облаке формата PaaS позволил ускорить вывод продуктов на рынок с нескольких раз в квартал до нескольких раз в неделю, что дает возможность быстро адаптироваться к изменению требований клиентов.
- Мобильный банк **Monzo** (Великобритания) разработал облачную АБС для того, чтобы размещать свои системы на инфраструктуре Amazon Web Services. Соответствие требованиям Управления по финансовому регулированию и надзору Великобритании

[1] *iPaaS – платформа для интеграции облачных сервисов между собой, а также облачных сервисов с локальными ИТ-системами компании-потребителя.*

(FCA) к аудиторскому следу[2] операций в ИТ-системах обеспечивается технологией CloudTrail от AWS[3].

Безопасность как услуга

Традиционно каждая организация внедряла решения по информационной безопасности на собственной инфраструктуре. Переход от частных решений к облачным позволяет внедрять высококачественные и современные системы информационной безопасности при совокупном снижении стоимости владения для организации за счет отказа от установки и сопровождения программного и аппаратного обеспечения, а также сокращения расходов на персонал, обслуживающий указанное оборудование.

Наиболее широко распространены облачные решения по безопасности, представляющие собой:

- антивирусные сервисы;
- сервисы защиты от спама;
- сервисы защиты хранения информации;
- сервисы защиты от мошенничества и DDoS-атак.

Также распространение получают принципиально новые сервисы по безопасности:

- Облачные решения, предоставляющие услуги по хранению и использованию закрытых ключей электронной подписи.

Пример: облачная подпись CryptoPro (Россия).

- Облачные решения, обеспечивающие дистанционное подписание/заверение предоставляемой информации (документов) с последующей передачей подписанной информации третьим лицам.

Пример: разрабатываемое ПАО «Ростелеком» облачное решение, обеспечивающее подписание собранных банками биометрических персональных данных и их передачу в Единую биометрическую систему.

Облачная среда для обмена данными

Связующим элементом облачной инфраструктуры для финансового сектора является среда для обмена данными на основе открытых API, обеспечивающая интеграцию между облачными компонентами поставщика инфраструктуры и частными компонентами одного из клиентов-участников. Например, облачная АБС и облачный шлюз к платежной системе могут быть интегрированы с частной реализацией мобильного банка-клиента. В другом случае кредитная организация может интегрировать свой процесс рассмотрения кредитных заявок с сервисами, которые предоставляет облачный поставщик KYC-аналитики или альтернативного кредитного скоринга.

При этом у потребителя услуги должна быть возможность параллельно использовать сервисы нескольких поставщиков с целью определения наиболее подходящего для решения конкретных задач. Таким образом, «облако» является форматом предоставления услуги обмена данными, а открытые API – способом публикации и использования этой услуги.

Примеры:

- Компания **SaltEdge** (Канада) предоставляет поставщикам платежных услуг доступ к информации о счете и каналам инициирования платежей через единый API-шлюз.
- Технологическая компания **SnapLogic** (США) предоставляет универсальную платформу для интеграции источников данных и ИТ-систем в облаке с локальными ИТ-системами в формате услуги.

Учетно-операционные сервисы

Подобные виды сервисов являются актуальными для быстрого выхода новых участников на финансовый рынок. Сервис облачного бэк-офиса не потребует значительных капиталовложений, так как ИТ-

---

[2] *Аудиторский след – хронологическая последовательность записей аудита, которые содержат доказательства изменения данных в результате выполнения бизнес-процесса или системной функции.*

[3] *AWS CloudTrail – сервис в облачной инфраструктуре Amazon, позволяющий вести журналы всех действий в учетной системе потребителя и проводить аудит операционных рисков.*

инфраструктура, обслуживающий персонал и операционные процессы включены в формат услуги, которую можно масштабировать пропорционально изменениям количества выполненных операций.

Поставщиком такой услуги может быть:

- Финансовая организация, предоставляющая сегмент своего бэк-офиса в формате Bank as a service.

Пример: необанк для юридических лиц «**Дело Банк**» (Россия) работает по лицензии «**СКБ-банка**».

- Технологическая компания, которая дополнительно к автоматизации бэк-офиса предлагает прочие функции, реализованные самостоятельно или через партнеров.

Пример: компания «Центр финансовых технологий» **(ЦФТ)** (Россия) предоставляет облачную автоматизированную банковскую систему.

Доступ к платежным системам

Поставщик облачной платформы может предоставлять шлюзы к платежным системам по модели подписки аналогично аренде учетно-операционных услуг. В такой схеме он создает безопасную и масштабируемую интеграцию с платежными системами, например с системами платежных карт или системами быстрых платежей. В свою очередь, организация-клиент, разместив свое приложение внутри контура облака, сможет получить упрощенную схему интеграции с платежными системами, существенно сократив затраты на инфраструктуру, необходимую для подключения к ним.

Пример:

- Компания **Ant Financial** (Китай) создала торговую площадку облачных услуг с облачной автоматизированной банковской системой и шлюзом к процессингу AliPay.

Шаблонные приложения на основе технологии распределенных реестров

В настоящее время обязательным условием для подключения к системам, основанным на технологии распределенных реестров (distributed ledger technology, DLT), является необходимость развертывания инфраструктуры для запуска соответствующего решения на стороне организации.

Возможность создать бизнес-приложение на основе технологии распределенных реестров из типовых шаблонов и впоследствии развернуть его на облачной инфраструктуре с минимальными временными издержками позволит ускорить время вывода продукта на рынок, снизить стоимость его запуска и в результате предложить более выгодные и конкурентные условия для партнеров и потенциальных клиентов.

Примеры:

- Microsoft (США) предоставляет шаблоны в рамках облачного решения Azure Blockhain Workbench, Amazon (США) – в рамках **Amazon Web Services** Blockchain.

RegTech-сервисы

Закономерным продолжением размещения операционной деятельности на облачной инфраструктуре является реализация облачных RegTech-сервисов, включая услуги формирования обязательной финансовой отчетности и ее передачи финансовому регулятору и государственным органам.

Одним из ключевых преимуществ осуществления деятельности финансового рынка на облачной инфраструктуре может стать создание среды, обеспечивающей своим клиентам автоматическое исполнение базовых регуляторных требований.

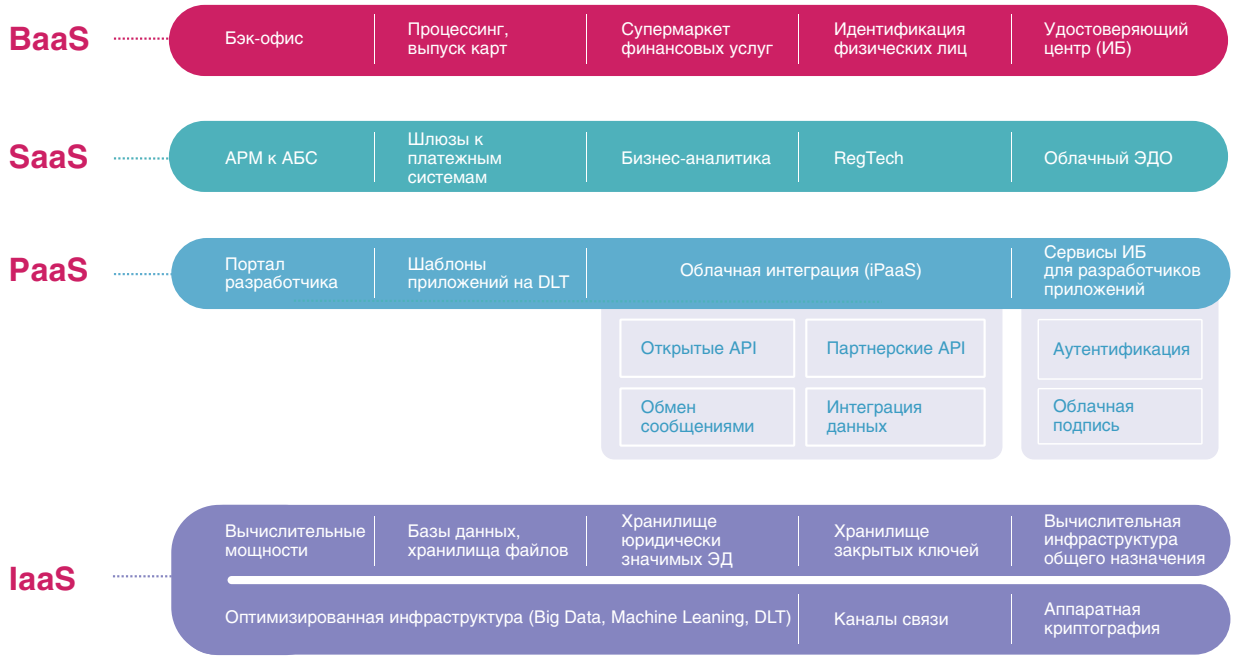
Примеры:

- Компания **nCino**[4] (США) обеспечивает предоставление обязательной отчетности.
- Компания **Tradle**[5] (США) обеспечивает анализ кредитных рисков и проведение процедур, направленных на

[4] *nCino – технологическая компания, которая предоставляет облачные решения для банковского сектора. Обладает собственной разработкой банковской операционной системы, которая позволяет оптимизировать внутренние процессы банков при цифровизации своих процессов.*

[5] *Tradle – технологическая компания, которая занимается разработкой решений на основе технологии распределенных реестров, связанных с KYC и соблюдением международных норм.*

Рисунок 2
Основные компоненты перспективной облачной инфраструктуры финансового рынка



соответствие требованиям по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ).

Супермаркет финансовых услуг

Помимо сервисов, автоматизирующих исполнение регуляторных требований, облачная инфраструктура может предлагать торговую площадку для публикации инновационных решений от нишевых компаний, например услуг по применению машинного обучения в кредитном скоринге, андеррайтинге или автоматизации маркетинговых кампаний.

В этом формате инновационные компании одновременно получат среду для размещения своих услуг и коллективный доступ к дорогостоящей инфраструктуре и информационным платформам. Таким образом, у финансово-технологических компаний появляется возможность сократить издержки на поддержку инфраструктуры и каналов продвижения своих услуг.

Пример:

- Международная финансовая группа ING предоставляет возможность приобретать через свою платформу как собственные финансовые продукты, так и продукты своих конкурентов.

Торговая площадка облачных услуг

Торговая площадка представляет собой комплексный набор облачных услуг, при этом способ реализации некоторых из них можно выбирать из нескольких вариантов от компаний-конкурентов. Такая среда может включать в себя единый подход к построению программных интерфейсов (API), возможность размещения своих приложений на инфраструктуре площадки, типовые договоры, а также унифицированные подходы к измерению показателей доступности сервисов, выставления счетов и оплаты облачных услуг.

Примеры:

- Компания **Ant Financial**[6] (Китай) создала торговую площадку облачных услуг, выстроенную по принципу Bank as a Service. В облачную инфраструктуру Ant Financial могут встраиваться как

[6] *Ant Financial (Китай) была выделена из холдинга Alibaba в 2011 году. Основным направлением Ant Financial является Alipay – крупнейший китайский сервис онлайн-платежей. Помимо платежной системы, Ant Financial ведет бизнес в области кредитования и управления частными капиталами, а также развивает фонд краткосрочных инвестиций, систему оценки кредитоспособности клиентов Sesame Credit и другие технологические решения в области платежей.*

традиционные банки, так и финтех-стартапы. В число сервисов, предоставляемых самой Ant Financial, входят шлюз к процессингу AliPay и облачная АБС.

- Банк **Fidor Solutions** (Германия) создал в ЕС аналогичную платформу Bank as a Service, в которую входят облачная АБС, шлюз к процессингу и супермаркет финансовых услуг. **Fidor Solutions** предоставляет банкам возможность использовать собственную лицензию на банковскую деятельность и облегченную интеграцию с сервисами из супермаркета услуг. У стартапов, развивающихся без привязки к одному банку-партнеру, есть возможность запускать свою деятельность с использованием банковской лицензии Fidor.
- Аналогично (за счет реализованных механизмов интеграции с партнерами) **N26** (Германия) является универсальным цифровым банком. Первоначально банк работал в формате BaaS с аутсорсингом учетно-операционного функционала Wirecard[7], затем получил собственную банковскую лицензию и перевел счета клиентов на свою инфраструктуру. После этого N26 стал развивать функционал финансового маркетплейса, предоставляя продукты партнеров через свой интерфейс. В частности, страховые продукты в N26 предоставляет Allianz, являющийся одновременно их инвестором, а трансграничные переводы организованы через TransferWise[8].
- Компания-разработчик программных продуктов для цифрового банкинга **Backbase** (Нидерланды) интегрирует данные и функциональность традиционных банковских систем с финтех-компаниями в единый цифровой клиентский интерфейс.

Торговая площадка Open Banking Marketplace от Backbase предоставляет услуги широкого спектра провайдеров. Среди услуг есть такие категории, как идентификация, аутентификация, подпись транзакций, финансовые сообщения, платежи, борьба с мошенничеством и соблюдение процедур KYC.

2.2. Бизнес-модели участников облачной экосистемы

У финансовых организаций должна быть возможность сократить свои издержки благодаря «коллективной» реализации тех функций, которые не являются их конкурентным преимуществом. В первую очередь это касается автоматизированных банковских систем, подготовки регуляторной отчетности и сертифицированной криптографии.

Применение облачных решений позволяет снизить барьеры выхода на рынок для инновационных компаний. Упрощение интеграции между участниками финансового и технологического секторов будет способствовать снижению транзакционных издержек и повышению прозрачности схем аутсорсинга, что повысит скорость адаптации финансовых организаций к меняющимся условиям на рынке.

Стоит отметить, что комплексные решения в облачной инфраструктуре могут быть качественнее решений, реализуемых на собственной инфраструктуре. Например, доступ к максимально широкому набору данных дает преимущество в таких областях, как кредитный скоринг, противодействие мошенничеству, отмыванию денег и финансированию терроризма.

---

[7] *Wirecard (Германия) – интернет-компания с банковской лицензией, которая имеет партнерские соглашения с Visa, MasterCard и большинством популярных платежных систем.*

[8] *TransferWise (Великобритания) – сервис недорогих трансграничных денежных переводов, основанный на минимизации фактической конверсии валюты. При переводе за границу система зачисляет исходящую валюту на свой технический счет в той же стране, передает в страну назначения сообщение о переводе, и платежная система в стране назначения перечисляет локальную валюту со своего технического счета на счет получателя, в результате чего операции конверсии минимизируются.*

Развитие облачной финансовой инфраструктуры создаст конкурентную среду, которая ускорит рост финансового сектора. С целью повышения лояльности клиентов и максимального увеличения своих конкурентных преимуществ финансовые и технологические компании будут наращивать ключевые компетенции, на основе которых могут выстраиваться различные бизнес-модели (см. рисунок 3).

Описание бизнес-моделей:

Нишевая финтех-компания – организация, обладающая экспертизой в узкой области, такой как дистанционное банковское обслуживание или кредитный скоринг на основе анализа пользовательского поведения розничного клиента в сети Интернет.

Пример: Рокетбанк (Россия) специализируется на предоставлении удобного мобильного банка-клиента, работая на базе инфраструктуры другого банка в формате BaaS по лицензии Киви Банка.

Дистрибьютор – организация, которая является супермаркетом финансовых продуктов, где потребители могут сравнить предложения и заключить сделку с тем, кто предложил более выгодные условия, не покидая платформу. Ключевой компетенцией дистрибьютора является постепенное наращивание клиентской базы за счет большого числа поставщиков и привлечение новых поставщиков путем увеличения числа клиентов (так называемый «эффект платформы»).

Пример: финансовая группа ING (Нидерланды) предоставляет возможность приобретать через свою платформу как собственные продукты, так и продукты других банков.

Продуктовая фабрика – финансовая организация, которая специализируется на разработке бизнес-процессов и выводе на финансовый рынок таких услуг, как предоставление кредитов, размещение депозитов, страховых продуктов, услуг по управлению финансами, проведение операций с гарантиями и аккредитивами, прочих сопутствующих услуг.

Основной целью такой организации является соблюдение баланса между финансовой устойчивостью и наличием возможности предлагать клиентам финансовые продукты на выгодных, конкурентных условиях.

Пример: крупные финансовые группы – Credit Agricole (Франция), Allianz (Германия), Сбербанк (Россия).

Технологическая компания – организация, которая обладает экспертизой в области создания высоконагруженных, масштабируемых и гибких ИТ-систем. Ключевая компетенция интегратора заключается в возможности реализовать «под ключ» готовое ИТ-решение для потребителя, состоящее из множества различных ИТ-систем.

Для развития и поддержки облачной инфраструктуры технологическая компания может предлагать следующие услуги:

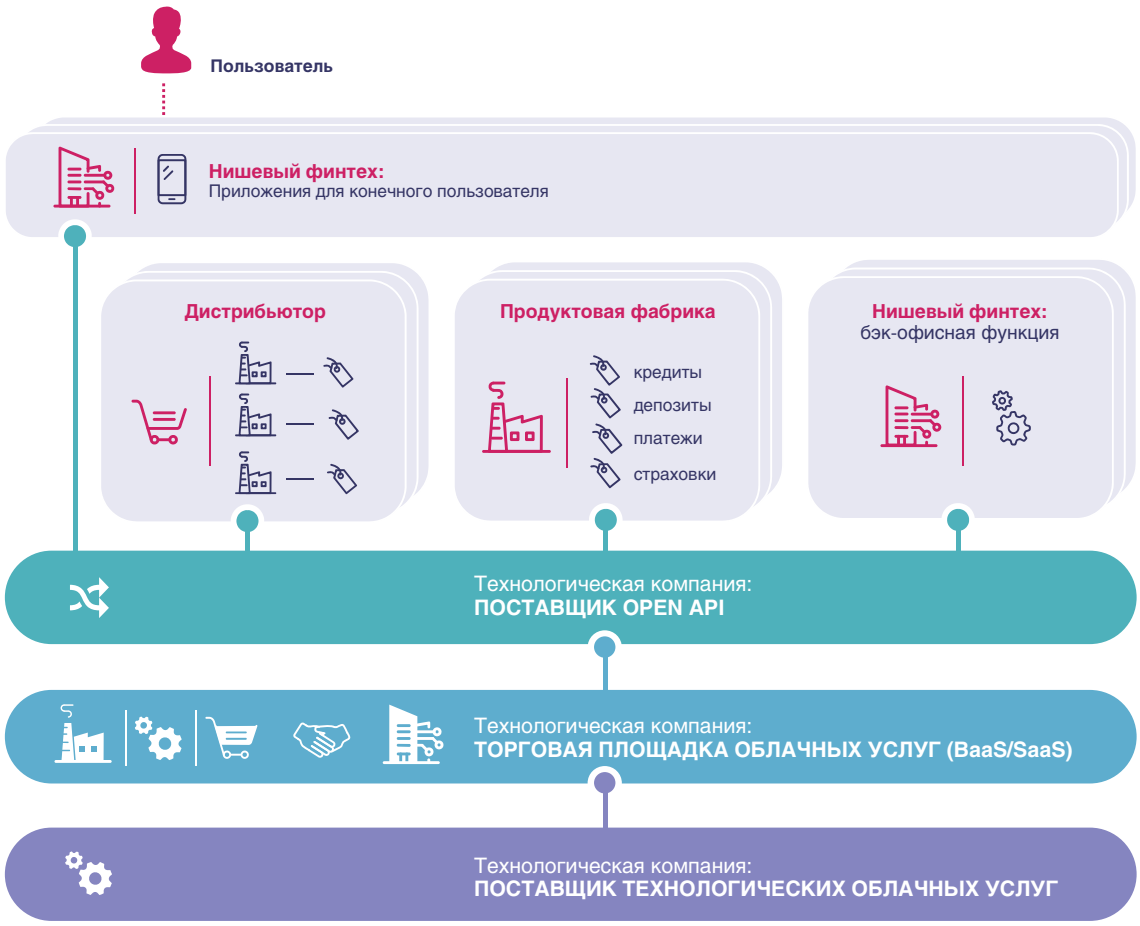
- Реализация открытых API, что включает в себя разработку стандартных программных интерфейсов к ИТ-системам финансовых организаций, а также предоставление технологической среды для обмена сообщениями.

*Пример: компания **SaltEdge** (Канада) предоставляет услуги по интеграции внутренних ИТ-систем участников финансового рынка с использованием открытых API в соответствии с требованиями Второй платежной директивы (PSD2)[9].*

- Размещение нескольких конкурирующих сервисов на торговой площадке облачных услуг, где клиенты могут пилотировать бизнес-услуги (BaaS) нескольких поставщиков параллельно и развивать сотрудничество с компаниями, предоставляющими наиболее подходящие решения. Торговая площадка облачных услуг может упрощать заключение контрактов между участниками, подписавшими рамочный договор с площадкой, предоставлять услуги хостинга, мониторинга качества предоставления услуг, биллинга (выставления счетов)

[9] https://eur-lex.europa.eu/eli/dir/2015/2366/oj.

Рисунок 3
Бизнес-модели участников облачной экосистемы



и расчетов по предоставляемым услугам.

Примеры: финансово-технологическая компания Ant Financial (Китай), банк Fidor Solutions (Германия).

➢ Предоставление подписки на облачные версии популярных ИТ-решений, которые обладают высокой стоимостью и требуют больших затрат на самостоятельное сопровождение.

Примеры: Amazon (США), Microsoft (США), Oracle (США), Ростелеком (Россия).

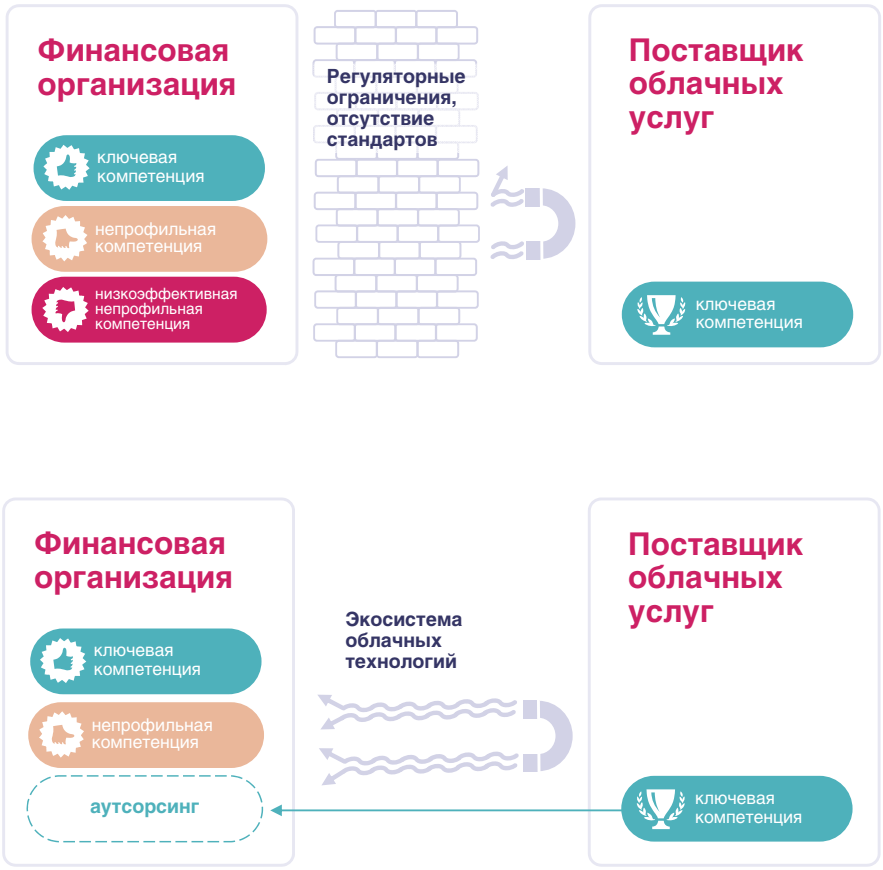
На рисунке 3 изображены бизнес-модели, или типовые направления деятельности, участников облачной экосистемы финансового сектора.

Для создания наиболее конкурентного предложения нишевые финтех-компании, дистрибьюторы финансовых продуктов и продуктовые фабрики могут интегрироваться друг с другом в любых сочетаниях через открытые API и торговые площадки облачных услуг. Open API является техническим средством интеграции участников экосистемы. Стоит отметить, что торговые площадки облачных услуг могут снижать транзакционные издержки на интеграцию за счет сопутствующих услуг (например, биллинг и мониторинг качества предоставления услуг).

Примеры:

- Фабрика финансовых продуктов может интегрироваться с поставщиком банка-клиента.
- Дистрибьютор объединяет предложения нескольких продуктовых фабрик.
- Поставщик Open API обеспечивает обмен данными между несколькими другими участниками и на этой основе создает дополнительные услуги: управление согласиями на обработку персональных данных или альтерна-

Рисунок 4
Адаптация бизнес-стратегии с акцентом на ключевые компетенции



тивный кредитный скоринг для продуктовой фабрики.

- Продуктовая фабрика может проводить интеграцию с несколькими поставщиками альтернативного скоринга.

Таким образом, в условиях развития облачной инфраструктуры у финансовых и технологических компаний появится возможность адаптировать стратегию с учетом своих конкурентных преимуществ, оптимизируя существующие издержки за счет перевода части своих процессов на облачную инфраструктуру.

2.3. Условия развития облачной инфраструктуры на финансовом рынке

В то время как проникновение облачных услуг находится на высоком уровне и все больше информационных систем компаний из реального сектора первоначально создаются для работы на облачной инфраструктуре, применение данных технологий в финансовом секторе ограничено. Это связано прежде всего с отсутствием готовых правил и механизмов, обеспечивающих должный уровень управления операционными и регуляторными рисками, возникающими при аутсорсинге критически важных функций финансовых организаций.

Практическая возможность и целесообразность размещения бизнес-критичных операций в облачной инфраструктуре зависит от прозрачности и исполнимости регуляторных требований по управлению рисками аутсорсинга, а также от отсутствия в них демотивирующих факторов.

Значительная часть инновационных решений в финансовой сфере основана на формировании продвинутой аналитики, качество которой зависит от возможности объединить максимально широкий набор данных. Одной из ключевых предпосылок развития экосистемы облачных финансо-

вых сервисов является наличие регуляторных требований, устанавливающих обязанность предоставлять персональные данные по запросу третьего лица, получившего согласие клиента на эту операцию. В зарубежной практике такой механизм получил название переносимости персональных данных (data portability).

Так, наиболее активное развитие облачных финансовых услуг происходит в Европе, где в рамках Второй платежной директивы и инициативы Open Banking внедряются открытые API, а также введен режим переносимости персональных данных в рамках General Data Protection Regulation (GDPR).

3. УПРАВЛЕНИЕ РИСКАМИ И РЕГУЛИРОВАНИЕ В СФЕРЕ ОБЛАЧНЫХ СЕРВИСОВ

При использовании облачных сервисов на финансовом рынке возникают следующие риски:

- влияние неблагоприятных инцидентов (аварий) на стороне поставщика на основную деятельность и деловую репутацию организации;
- регуляторные риски, которые возникают в связи с потерей контроля за мерами по защите персональных данных;
- концентрация критических функций на инфраструктуре небольшого количества поставщиков (с точки зрения количества точек отказа это аналогично ситуации, при которой большую долю розничного рынка контролирует один или несколько банков, как в России и Великобритании).

Управление рисками облачных сервисов входит в дисциплину управления операционными рисками, в частности рисками аутсорсинга. Управление операционными рисками регулируется на общих основаниях рекомендаций Базельского комитета по банковскому надзору, применяющихся во всех странах, которые их имплементируют в рамках локальных нормативных актов[1] (Principles for the Sound Management of Operational Risk, BCBS 195)[2].

Хотя общие рекомендации по управлению операционными рисками не теряют своей актуальности при активном развитии и внедрении облачных технологий, процессы и методология управления операционными рисками требуют изменений. В связи с этим регуляторы опубликовали рекомендации, которые отличаются по уровню детализации и обязательности их исполнения (см. таблицу 1).

В число регуляторов, разработавших рекомендации по управлению риском облачного аутсорсинга, входят:

- Европейская служба банковского надзора (European Banking Authority, EBA)[3];
- Управление по финансовому регулированию и надзору Великобритании (Financial Conduct Authority, FCA)[4];
- Денежно-кредитное управление Сингапура (Monetary Authority of Singapore, MAS)[5];
- Комиссия по регулированию банковской деятельности Китая (China Banking Regulatory Commission, CBRC)[6];
- Управление денежного обращения Гонконга (Hong Kong Monetary Authority, HKMA)[7];
- Федеральный совет по рассмотрению финансовых институтов США (Federal Financial Institutions Examination Council, FFIEC)[8].

Рекомендации относительно регулирования применения облачных технологий следуют единому подходу, в котором облачные технологии позиционируются в качестве формы аутсорсинга.

В то время как рекомендации FCA в большей степени являются инструментом для старта дискуссии с технологическими компаниями и аудиторами, рекомендации

[1] *https://www.bis.org/publ/bcbs/b3prog_dom_impl.htm.*

[2] *https://www.bis.org/publ/bcbs195.htm.*

[3] *https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.*

[4] *https://www.fca.org.uk/publication/finalised-guidance/fg16–5.pdf.*

[5] *http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Operational-Risk.aspx.*

[6] *http://www.cbrc.gov.cn/chinese/home/docView/200 90 6 304 236EC33D19A1CCDFF1B0985B7F10 000.html.*

[7] *http://https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.*

[8] *https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.*

Таблица 1

Сравнение подходов к регулированию аутсорсинга (в том числе облачных услуг) в финансовом секторе

	FCA (Великобритания)	EBA (ЕС)	MAS (Сингапур)	HKMA (Гонконг)	CBRC (Китай)	FFIEC (США)
Задачи	Информирование, мониторинг	Регулирование и надзор	Регулирование и надзор	Регулирование и надзор	Регулирование и надзор	Регулирование и надзор
Степень вовлечения регулятора	Детальные рекомендации	CBRC	Методические рекомендации	Верхнеуровневые требования	Верхнеуровневые требования, публикация ежегодного отчета по рискам аутсорсинга в финансовом секторе, мониторинг концентрации рисков среди поставщиков, организация оперативного обмена информации о рисках между банками	Методические рекомендации (очень подробные)
Обязательность исполнения рекомендаций	Нет	Да	Да	Да	Да	Да
Роль регулятора в заключении сделки	Информирование	Информирование	Информирование	Согласование	Согласование	Уведомление, согласование (страховые организации)
Требования к управлению рисками	Пропорциональны рискам	Пропорциональны рискам	Пропорциональны рискам	Пропорциональны рискам	Без градации по уровню риска, верхнеуровневые определения для максимальной свободы действий	Без градации по уровню риска
Обеспечение аудита и надзора	Возможность очной инспекции (на основании действующих нормативных и правовых актов)	Возможность очной инспекции, доступ к помещениям поставщика	Дистанционный надзор	Возможность очной инспекции, доступ к помещениям поставщика	Возможность очной инспекции	Возможность очной инспекции, доступ к помещениям поставщика
Аутсорсинг критических функций	Разрешен	Разрешен	Разрешен	Разрешен	Запрещен	Разрешен
Субподряд	Верхнеуровневые требования к анализу рисков субподряда	Требования к разграничению ответственности, требования к согласованию значимых действий и уведомлению о значимых событиях	Требования к обеспечению возможности аудита по всей цепочке	Не регулируется	Не регулируется	Требования к разграничению ответственности, требования к согласованию значимых действий и уведомлению о значимых событиях
Аутсорсинг в третьих странах	Верхнеуровневые требования к анализу рисков аутсорсинга за пределами Великобритании	Разрешен при отсутствии блокирующих страновых рисков	Разрешен при имплементации всех регуляторных требований на уровне контракта и отсутствии блокирующих страновых рисков	Разрешен при имплементации всех регуляторных требований на уровне контракта. HKMA может запрашивать данные о поставщике у регуляторов третьих стран	Только с юрисдикциями, подписавшими межправительственные соглашения	Разрешен при имплементации всех регуляторных требований на уровне контракта и отсутствии блокирующих страновых рисков
Обеспечение непрерывности деятельности	Наличие альтернативного поставщика и стратегии выхода, регулярное обновление планов обеспечения непрерывности деятельности	Наличие альтернативного поставщика и стратегии выхода, регулярное обновление планов обеспечения непрерывности деятельности	Наличие альтернативного поставщика, регулярные учения по противодействию неблагоприятным инцидентам	Наличие альтернативного поставщика или возможности запустить функцию внутри компании, регулярные учения по противодействию неблагоприятным инцидентам	Регулярные учения по противодействию неблагоприятным инцидентам и соответствующая отчетность регулятору, запуск учений по требованию регулятора	Регулярные учения по противодействию неблагоприятным инцидентам

Защита данных	Требования к анализу киберрисков	Юридически обязывающие требования к защите данных в контракте	Юридически обязывающие требования к защите конфиденциальности в контракте, отделение данных от прочих клиентов поставщика аутсорсинговых услуг, миграция и удаление данных после расторжения контракта	Юридически обязывающие требования к защите конфиденциальности в контракте, отделение данных от прочих клиентов поставщика аутсорсинговых услуг, миграция и удаление данных после расторжения контракта	Упоминание в формате кратких тезисов о конфиденциальности	Юридически обязывающие требования к защите данных в контракте, включая уведомления об авариях

прочих регуляторов обязательны к исполнению.

В Китае и Гонконге требования являются относительно верхнеуровневыми, в ЕС – детальными. В Сингапуре и США регуляторы создали методические рекомендации (наиболее подробные из них – в США).

Регулятор в Китае имеет наибольшую степень вовлеченности в процесс исполнения требований. CBRC собирает максимум данных, согласовывает все значимые шаги своих поднадзорных организаций и готовит для них аналитику.

Примечательно, что CBRC запрещает аутсорсинг ключевых банковских систем. С другой стороны, MAS, европейские и американские регуляторы не видят необходимости в запрете аутсорсинга ключевых банковских ИТ-систем, если соблюдены все правила управления операционными рисками. Такой же принцип действует в отношении аутсорсинга в третьих странах – в то время как для большинства рассмотренных регуляторов достаточно соответствующих мер предосторожности, в Китае аутсорсинг разрешен только в юрисдикциях, где подписаны межправительственные соглашения.

В ряде юрисдикций необходимо только уведомление о заключении сделки на аутсорсинг с риском материального ущерба (например, в Сингапуре). В других юрисдикциях установлена процедура согласования заключения сделки с регулятором – например, в Гонконге (все финансовые организации), США (субъекты страхового дела) и Китае (субъекты страхового дела и биржи).

Важной чертой рассмотренных рекомендаций является прозрачность аутсорсинга для финансового регулятора – с учетом надлежащего управления рисками участники рынка могут выстраивать цепочки субподряда без права переложить ответственность на третью сторону. При этом финансовая организация обязана обеспечить условия для эффективного проведения аудита и надзорных мероприятий.

4. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ НА ФИНАНСОВОМ РЫНКЕ В РОССИИ И ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ УСЛОВИЙ ДЛЯ ИХ РАЗВИТИЯ

На финансовом рынке в России существует большое количество поставщиков облачных услуг, покрывающих потребности организаций в гибкой инфраструктуре, на которой развернуты собственные ИТ-системы (IaaS, PaaS), а также предоставляющих коробочные корпоративные ИТ-системы (SaaS). Из специфических решений для сферы банковских услуг, массово поставляемых как сервис, на рынке существуют предложения в сфере АБС, дистанционного банковского обслуживания, процессинга и эквайринга платежных карт.

В частности, ЦФТ в течение нескольких лет предоставляет услуги по аренде АБС, развернутой на облачной инфраструктуре компании. Рокетбанк, предлагающий физическим лицам услуги мобильного банкинга, приобретает у банков-партнеров услугу формата BaaS.

Применение облачных технологий на финансовом рынке Российской Федерации связано с рядом рисков:

- отсутствие структурированной информации у участников рынка о перечне доступных облачных сервисов и условиях их использования;
- высокая стоимость перехода на облачные решения по причине использования участниками рынка большого количества программ собственной разработки, а также глубокой кастомизации унаследованных решений;
- отсутствие четко описанных регуляторных ограничений к применению облачных сервисов;
- отсутствие механизмов валидации качества сервисов, предоставляемых провайдерами облачных сервисов;
- отсутствие практики применения облачных сервисов у поднадзорных организаций;
- системный риск, возникающий в результате распространения облачных решений ненадлежащего качества.

В результате проведенного анализа практик применения и регулирования облачных технологий на финансовом рынке представляется целесообразным рассмотреть следующие предложения по развитию облачных сервисов на российском финансовом рынке:

- согласование проектов и направлений работы Банка России в сфере развития открытых API, создания платформенных решений, таких как маркетплейс для финансовых услуг и продуктов, системы быстрых платежей, системы передачи финансовых сообщений, и развития облачных сервисов;
- проведение анализа и определение состава облачных сервисов на финансовом рынке и регуляторных барьеров для их развития;
- публикация лучших практик управления рисками аутсорсинга с применением облачных технологий;
- создание типовых положений договоров на аутсорсинг с учетом требований финансового регулятора к поставщику ИТ-услуг, в том числе в области управления рисками, аудита и надзора;
- стимулирование развития практики квалифицированного аудита и сертификации поставщиков услуг в сфере облачных технологий путем установления требований к договорам и знакам качества согласно уровню зрелости внутреннего контроля;

- определение целесообразности введения специального режима надзора за системно значимыми поставщиками ИТ-услуг совместно с Минкомсвязью России.

Успешная реализация данных инициатив создаст благоприятные условия для инноваций в области облачных финансовых услуг, основанных на стабильной, безопасной и экономически эффективной инфраструктуре.

ЗАКЛЮЧЕНИЕ

Ключевым фактором эффективности облачной инфраструктуры является возможность размещать в облаке капиталоемкие функции, такие как учетно-операционная деятельность, подготовка обязательной отчетности и обеспечение безопасности.

Для развития облачной инфраструктуры финансового рынка необходимо создать благоприятные условия с прозрачными и выполнимыми требованиями к управлению операционными рисками. В 2019 г. Банк России совместно с участниками финансового рынка планирует рассмотреть вопросы, связанные с разработкой рекомендаций для финансовых организаций в целях использования ими облачных технологий.

Международный опыт показывает, что активное развитие облачных финансовых услуг происходит в странах, где финансовый регулятор принимает меры, направленные на развитие конкуренции. Важно отметить, что создание облачной инфраструктуры финансового рынка делает необходимой гармонизацию отдельных направлений развития финансовых технологий, что в первую очередь относится к развитию открытых API и технологий RegTech, а также построению и развитию платформенных решений в финансовом секторе.

Стимулирование рынка облачных услуг ускорит развитие финансового рынка Российской Федерации, в ходе которого традиционные участники рынка и технологические компании будут искать оптимальное сочетание собственных компетенций и партнерских соглашений, позволяющее конкурировать за клиентов в условиях цифровой экономики.

ВОПРОСЫ ДЛЯ УЧАСТНИКОВ РЫНКА

1. В каких моделях предоставления облачных услуг (IaaS, PaaS, SaaS, BaaS) вы видите наибольший потенциал для участников финансового рынка?

2. Какие из моделей предоставления облачных услуг вы используете? Приведите краткое обоснование, опишите пилотные проекты и примеры внедрения.

3. В каких сферах применения облачных технологий целесообразно использование единого оператора, а в каких – нескольких поставщиков:

- инфраструктурные услуги;
- безопасность как услуга;
- облачная среда для обмена данными;
- учетно-операционные сервисы;
- доступ к платежным сервисам;
- шаблоны приложений на распределенных реестрах;
- RegTech-сервисы;
- супермаркет финансовых услуг;
- торговая площадка облачных услуг.

Обоснуйте выбранные вами варианты реализации облачных решений в указанных сферах. На ваш взгляд, такой оператор или поставщики должны быть государственными и (или) частными?

4. Перечислите барьеры развития облачных технологий на финансовом рынке (с аргументацией).

5. Какие предложения по развитию облачных сервисов, содержащиеся в докладе, наиболее перспективны для реализации и почему?

6. Какие еще мероприятия по развитию облачных сервисов с участием регулятора/участников финансового рынка вы считаете целесообразными?

7. Какие аспекты применения облачных технологий должны быть отражены в рекомендациях Банка России по предоставлению соответствующих услуг участникам финансового рынка?

ПРИЛОЖЕНИЯ

Приложение 1. Рекомендации Европейской службы банковского надзора (EBA)

В июне 2018 г. EBA провела общественные консультации по руководящим принципам в отношении аутсорсинга функций поставщиков облачных услуг. С 1 июля 2018 г. данные рекомендации применяются к кредитным организациям, инвестиционным фондам и платежным организациям.

Анализ и планирование аутсорсинга

Организациям необходимо проводить всестороннюю оценку рисков передачи функций на аутсорсинг, возможности оперативного реагирования на сбои, возможные правовые и репутационные риски от наступления таких последствий. Компания также должна оценить риск материального ущерба и риск нарушения конфиденциальности данных.

Организация должна вести реестр информации о всех своих процессах, которые были переданы сторонним поставщикам облачных услуг. В данном реестре должна содержаться как минимум следующая информация:

- тип аутсорсинга (модель облачного сервиса и наличие публичной инфраструктуры);
- стороны, получающие облачные услуги в рамках соглашения об аутсорсинге;
- доказательства одобрения аутсорсинга органом управления или его ответственным уполномоченным;
- наименование любых субподрядчиков, если такие есть;
- страна, в которой зарегистрированы поставщик облачных услуг и его субподрядчики;
- факт аутсорсинга критически важных бизнес-операций;
- оценка взаимозаменяемости поставщика облачного сервиса (легко, трудно или невозможно);
- альтернативный поставщик услуг.

Взаимодействие с надзорным органом при заключении сделки

Компании должны информировать компетентные органы о том, каким сторонним поставщикам облачных услуг передаются процессы компании. Информировать необходимо о следующем:

- наименование поставщика облачных услуг и наименование материнской компании (при наличии);
- описание деятельности и данных, подлежащих передаче внешнему поставщику;
- страна или страны, где будет предоставляться облачная услуга (включая местоположение данных);
- дата начала передачи процессов на аутсорсинг и самая поздняя дата продления договора аутсорсинга.

Условия для осуществления аудита и надзора

Поднадзорная организация должна иметь письменное разрешение со стороны поставщика облачных услуг на полный доступ к служебным помещениям аутсорсинговой компании, включая полный доступ к устройствам, системам, сетям и данным, которые используются для предоставления услуг, переданных на аутсорсинг, в том числе и для аудиторов клиента.

В рекомендациях отмечается важность проведения аудиторской проверки поставщика облачных услуг. Учитывая то, что облачные решения имеют сложную технологическую структуру, клиент должен проверить, что сотрудники, проводящие аудит, обладают необходимыми навыками и знаниями для проведения эффективного аудита.

Защита данных

Договор на аутсорсинг должен обязывать поставщика услуг аутсорсинга защищать конфиденциальность информации, передаваемой финансовой организацией. В соответствии с руководящими принципами Комитета европейских банковских надзирателей (CEBS) организациям следует внедрять механизмы обеспечения непрерывности услуг, предоставляемых поставщиком.

Как указано в руководящем положении CEBS, организация должна проявлять особую осторожность при работе с аутсорсинговыми компаниями за пределами Европейской экономической зоны из-за возможных рисков защиты данных и возникающих рисков в области эффективного надзора со стороны контролирующего органа. Организация должна оценивать риски, связанные с местоположением данных и их обработкой, при работе со сторонними поставщиками облачных услуг.

Организация также должна обращать внимание на субподрядчиков аутсорсинговой компании и согласовывать цепочку оказания аутсорсинговых услуг только в том случае, если субподрядчик соответствует тем же требованиям, что и основной подрядчик.

План выхода

Согласно рекомендациям EBA, необходимо предусмотреть план действий на случай непредвиденных обстоятельств и стратегию выхода из соглашения на аутсорсинг. Организация должна планировать и осуществлять меры по поддержанию непрерывности своей деятельности в том случае, если предоставление услуги не может быть исполнено должным образом. Данные меры должны включать планирование на случай непредвиденных обстоятельств и четко определенную стратегию выхода. Также следует предусмотреть, чтобы при прекращении работы с аутсорсинговой компанией не было ущерба для непрерывности и качества предоставляемых услуг своим клиентам. Для этого необходимо разработать соответствующий «план выхода» и определить возможные альтернативные решения.

Приложение 2. Рекомендации Управления по финансовому регулированию и надзору Великобритании (FCA)

В 2015 г. FCA начало проводить консультации по применению облачных решений, после чего в 2016 г. была опубликована первая версия рекомендаций. В 2018 г. была опубликована обновленная редакция, в которой были отражены рекомендации EBA.

Анализ и планирование аутсорсинга

Финансовая организация должна управлять рисками, возникающими в результате перевода процессов на аутсорсинг:

- проводить оценку рисков, определять меры по их устранению;
- задокументировать проведенную оценку;
- определять лучшие практики в отрасли, включая требования к системе управления данными, управления киберрисками, а также все регуляторные требования, применимые к его деятельности;
- проверять, имеются ли юридические и нормативные риски, если аутсорсинговая компания и сотрудники находятся в разных юрисдикциях;
- обеспечивать в рамках договора устранение контрагентом возникших нарушений и последствий прочих неблагоприятных событий.

Потенциальный потребитель должен оценивать способность провайдера облачных услуг придерживаться международных стандартов и учитывать аттестацию или сертификацию соответствия стандартам, в том числе ISO 27000.

Организация-потребитель должна иметь четкое представление о предоставляемой услуге и о сфере ответственности со своей стороны и со стороны поставщика услуг. Также организация должна обеспечить наличие сотрудников, обладающих необходимыми навыками, компетенциями и ресурсами для надзора и проверки деятельности сторонних провайдеров для мониторинга и управления рисками, возникающими в ходе работы с данным подрядчиком. Кроме того, необходимо убедиться, что существуют приемлемые механизмы разрешения споров.

Аутсорсинговые услуги могут оказываться с привлечением нескольких субподрядчиков, и, если организация напрямую не заключает договор с одной аутсорсинговой компанией, она должна рассмотреть механизмы субподряда и определить, не запрещен ли этот вид деятельности для данной организации.

Помимо прочего, организация должна иметь комплекс мер по управлению изменениями оказываемых ей услуг, а также понимать, как будет проводиться тестирование изменений с целью снижения возможных рисков.

В части непрерывности бизнеса потребитель облачных услуг должен предусмотреть механизмы по обеспечению работы своих процессов в случае возникновения сбоев на стороне аутсорсинговой компании. В том числе необходимо на регулярной основе проводить тестирование и обновление механизмов функционирования своих процессов, которые переданы аутсорсинговой компании с целью повышения их эффективности.

Взаимодействие с надзорным органом при заключении сделки

Руководство FCA не является обязательным и носит рекомендательный характер, который должен являться сигналом для рынка о положительном отношении регулятора к инновациям. Аналогично Денежно-кредитному управлению Сингапура FCA определяет облачные услуги как форму аутсорсинга. Использование организацией облачных решений сохраняет ее

ответственность за выполнение всех обязательств поднадзорных регулятору организаций без делегирования ответственности третьей стороне.

Условия для осуществления аудита и надзора

Деятельность некоторых видов организаций регулируется соответствующими законодательными актами (к примеру, инвестиционные фонды UCITS), которые требуют доступ к данным, связанным с деятельностью сторонних организаций для аудиторов, регулирующих органов и других компетентных органов. Поэтому организация должна иметь возможность оперативно запросить у своего поставщика услуг доступ к требуемым данным. Поставщик услуг, в свою очередь, не должен устанавливать ограничения на то, как организация может получать доступ к своим данным, а также устанавливать лимит на количество запросов на эти данные и налагать ограничения при попытке извлечь данные из инфраструктуры поставщика облачных услуг.

В регуляторных требованиях к некоторым видам финансовых организаций (например, страховым организациям) установлен доступ к данным, связанным с аутсорсинговой деятельностью, а также при необходимости – физический доступ к служебным помещениям поставщика услуг. Организация также может направить аудитора, которому должен быть предоставлен беспрепятственный доступ к служебным помещениям аутсорсинговой компании. Исключением могут являться дата-центры из соображений безопасности.

Защита данных

Также организация-потребитель должна проводить оценку риска компрометации данных, передаваемых в облачную инфраструктуру. Необходимо учитывать категорию чувствительности данных, способ их хранения, передачи и шифрования, а также определить юрисдикции, где данные могут обрабатываться.

Организация должна соблюдать регламент General Data Protection Regulation (GDPR) и Закон о защите данных (Data Protection Bill, 2018). Исполнение требований GDPR контролируется и регулируется Управлением Информационного Комиссара (ICO). В связи с этим организация должна следовать Руководству ICO по облачным вычислениям и другим соответствующим указаниям.

План выхода

Потребитель облачных услуг должен предусмотреть меры по расторжению договора с аутсорсинговой компанией таким образом, чтобы данное действие не стало фактором нарушения целевых показателей деятельности и не приводило к нарушениям регуляторных требований. Необходимо предусмотреть возможность перехода к другому поставщику услуг и использовать процедуры, в результате которых чувствительные данные будут удалены с инфраструктуры поставщика облачных услуг.

Приложение 3. Рекомендации Денежно-кредитного управления Сингапура (MAS)

В 2011 г. финансовый регулятор Сингапура Monetary Authority of Singapore (MAS) опубликовал рекомендации по аутсорсингу, в которых облачные услуги рассматриваются как частный случай аутсорсинга (Циркуляр SRD TR 01/2011[1]).

Позднее, в 2016 г., MAS опубликовало официальные рекомендации по аутсорсингу (MAS Outsourcing Guidelines). Также MAS установило регуляторные требования к доступности критических ИТ-систем и разработало опросник с реестром контрольных вопросов, необходимых для проработки в рамках заключения сделки на аутсорсинг.

Анализ и планирование аутсорсинга

На этапе оценки должной добросовестности клиент обязан удостовериться в достаточности средств обеспечения непрерывной деятельности на стороне поставщика и оценить влияние нового соглашения на данные процессы. Клиент и поставщик должны совместно проводить регулярные и исчерпывающие испытания сквозных процессов обеспечения непрерывности деятельности.

Также клиент должен осуществлять мониторинг и контроль работы вынесенной на аутсорсинг функции, при этом степень детализации и формальности процесса должна быть пропорциональна материальным рискам, связанным с соглашением.

Рекомендации MAS фиксируют требования к анализу рисков аутсорсинга, подразумевающего определение роли аутсорсинга в бизнес-стратегии компании, проведение процедур установления должной добросовестности поставщика услуг (due diligence), оценку влияния аутсорсинга на риск-профиль компании и соотнесение выгод с рисками компрометации безопасности, сбоев и разрыва соглашения.

MAS выделяет категорию материальных соглашений[2] на аутсорсинг. Причисление соглашения на аутсорсинг к категории материальных требует экспертного суждения на основании ряда критериев, в том числе масштаба влияния функции, вынесенной за пределы компании, на финансовый результат, риск-профиль, стратегию и деловую репутацию. Аутсорсинг процедур соответствия регуляторным требованиям является материальным соглашением.

Оценка должной добросовестности поставщика услуг подразумевает подтверждение ряда качеств поставщика, в том числе достаточности его компетенций для обеспечения необходимого уровня сервиса, работоспособности процедур внутреннего контроля, должного уровня деловой и профессиональной этики, а также финансовой устойчивости. Рекомендации MAS устанавливают обязанность документировать процедуру оценки должной добросовестности и периодически ее обновлять.

Взаимодействие с надзорным органом при заключении сделки

Подход к исполнению данных рекомендаций в конкретной организации должен быть пропорционален природе и степени существенности рисков аутсорсинга, при этом MAS в первую очередь интересует управление рисками по материальным соглашениям на аутсорсинг.

Вне зависимости от сочетания собственных функций и функций на аутсорсинге потребитель облачной услуги несет ответственность за обеспечение мониторинга

[1] *http://www.mas.gov.sg/~/media/resource/legislation_guidelines/banks/circulars/IT%20Outsourcing%20Circular%20Jul%202011.pdf.*

[2] *Material agreement, или соглашение на аутсорсинг, влекущее материальные риски.*

рисков, внутреннего контроля, аудита и инспекции, как если бы все функции были реализованы самостоятельно. Следует отметить, что рекомендации распространяются на дочерние структуры компаний, учрежденных на территории Сингапура, путем их имплементации на уровне внутрикорпоративных правил.

Ежегодно или по требованию регулятора участник финансового рынка должен подтвердить, что договорные отношения с поставщиком услуг соответствуют рекомендациям по аутсорсингу. В случае обнаружения несоответствия регулятор предписывает организации корректирующие меры.

Несмотря на то, что руководство компании может поручить операционную работу по управлению рисками третьему лицу, ответственность за обеспечение сквозного управления рисками остается за руководством компании – потребителя услуг аутсорсинга.

Регулятор устанавливает минимальные требования к полноте соглашения на аутсорсинг, согласно которым оно должно содержать положения о предмете аутсорсинга, стандартах производительности и управления рисками, конфиденциальности и информационной безопасности, управлении непрерывностью деятельности, мониторинга и контроля, аудита и инспекции, механизмов разрешения споров и досрочного расторжения соглашения. Также соглашение об аутсорсинге должно устанавливать обязательство своевременного информирования клиента об авариях. В случае наличия субподряда контракт должен фиксировать соответствующие ограничения и меры предосторожности, а также обязательство поставщика услуг согласовывать условия субподряда с потребителем.

Условия для осуществления аудита и надзора

Соглашение на аутсорсинг не должно препятствовать эффективному осуществлению аудита со стороны клиента и инспекции финансовым регулятором. В частности, MAS или иной уполномоченный надзорный орган имеют доступ к аудиторскому следу всех операций в рамках соглашения на аутсорсинг. Материальное соглашение на аутсорсинг обязывает поставщика услуг выполнять надзорные запросы MAS или иного уполномоченного надзорного органа, касающиеся данного соглашения.

Защита данных

Согласно рекомендациям MAS, потенциальный клиент должен удостовериться в способности поставщика обеспечить необходимый уровень конфиденциальности и безопасности данных. Поставщик услуг, в свою очередь, должен регулярно проходить независимый аудит, устанавливающий факт достаточности мер безопасности для обеспечения конфиденциальности коммерческих и персональных данных, и предоставлять его результаты клиенту.

План выхода

Потребитель облачных услуг должен предусмотреть меры по изменению или расторжению договора с аутсорсинговой компанией таким образом, чтобы обеспечить непрерывность деятельности. Необходимо предусмотреть возможность временного или постоянного перехода к другому поставщику услуг. Примечательно, что даже при заключении соглашения на аутсорсинг внутри группы компании данные требования должны иметь статус юридических обязательств.