СТАНДАРТЫ ОТКРЫТЫХ БАНКОВСКИХ API. Регламент взаимодействия банка со сторонними потребителями API

Минск, 2019

Содержание

1 Общие положения

Настоящий Регламент определяет модели взаимодействия Банка и Стороннего потребителя API с использованием Информационных API, содержащих только открытые данные.

Состав открытых данных для передачи с использованием Информационных API:

1) Данные о курсах валют (наличных, безналичных, онлайн, АТМ/ПСТ, для ЮЛ и ФЛ, в зависимости от суммы и т.п.);

2) Данные о точках обслуживания банка (отделения, филиалы, обменные пункты, банкоматы, инфокиоски) с адресами и временем работы, контактными телефонами, e-mail, списком оказываемых услуг и т.п.;

3) Данные об АТМ и ПСТ с информацией о валютах, времени доступа, адресе и т.п.;

4) Данные о банковских продуктах:

– текущих счетах;
– кредитах и их вариациях;
– депозитах и их вариациях;
– банковские платежные карточки;
– драгметаллы, монеты и т.п.;
– условия денежных переводов, включая переводы без открытия счета.

Требования настоящего Регламента распространяются на участников экосистемы открытого банкинга.

Настоящий Регламент предназначен для использования участниками экосистемы открытого банкинга при реализации процессов в ходе разработки приложений, предоставляющих или потребляющих открытые API.

Настоящий Регламент может быть дополнен или расширен при последующей работе над платежными и статистическими API.

2 Термины и определения

В настоящем документе используются следующие термины и их определения:

2.1 ATM/ПСТ

Банковский терминал самообслуживания, в том числе банкомат, платежно-справочный терминал.

2.2 Банк

Юридическое лицо, имеющее исключительное право осуществлять банковские операции в соответствии с Банковским Кодексом Республики Беларусь.

2.3 Информационный API

API с публичным доступом для передачи Открытых данных.

2.4 Клиент

Юридическое или физическое лицо, являющееся действительным или потенциальным пользователем банковских услуг, использующее данные и/или услуги, предоставляемые Сторонним потребителем API посредством банковского API.

2.5 Национальный банк Республики Беларусь

Используется в значении, определенном Банковским Кодексом Республики Беларусь.

2.6 Небанковская кредитно-финансовая организация

Используется в значении, определенном Банковским Кодексом Республики Беларусь.

2.7 Открытый банкинг

Концепция банковских услуг, основанная на современном и безопасном способе для потребителей (пользователей банковских услуг), в том числе малых предприятий, обмениваться информацией, позволяя новым и существующим компаниям предлагать сверхбыстрые методы оплаты и инновационные банковские продукты.

2.8 Открытый API; API

Способ доступа к данным на основе открытого и безопасного стандарта API.

2.9 Платежный API

API с партнерским доступом для передачи Справочных данных Клиента и Транзакционных данных Клиента при условии получения согласия от Клиента. Доступ предоставляется зарегистрированному партнеру в целях оказания Клиентам услуг.

2.10 Поставщик API

Банк, участник экосистемы открытого банкинга, предоставляющий Открытый API.

2.11 Потребитель API

Любое физическое или юридическое лицо, которое разрабатывает или использует программные средства, использующие открытые API.

2.12 Программный интерфейс приложения; API

Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах.

2.13 Реестр Сторонних потребителей API

Реестр Сторонних потребителей API, прошедших в установленном порядке процедуру идентификации и соответствующих предъявляемым требованиям к разработчикам программных средств – Сторонним потребителям API и/или программным средствам.

2.14 Согласие

Разрешение Клиента на получение Справочных данных Клиента и Транзакционных данных Клиента Третьей стороной от Поставщика API и/или на передачу данных Третьей стороной Поставщику API от имени Клиента, выраженное в письменной форме лично представленного поставщику API, либо согласия, представленного поставщику API в электронном виде с применением программно-аппаратных средств и технологий, позволяющих достоверно установить, что оно исходит от соответствующих лиц.

2.15 Стандарт открытых API; стандарт API

Комплекс требований к API, включающий спецификацию данных, подход к реализации API и требования по обеспечению безопасности, которые принимаются Национальным банком Республики Беларусь в установленном порядке в виде стандартов проведения расчетов.

2.16 Сторонний потребитель API

Юридическое лицо, являющееся резидентом или нерезидентом Республики Беларусь, участник экосистемы открытого банкинга, предоставляющий Клиентам банков услуги на базе программных средств, использующих Открытый API.

2.17 Тестовая среда API

Отдельное программное решение или специальный режим функционирования API, которое имитирует работу API с использованием тестовых данных.

2.18 Участник экосистемы открытого банкинга

Поставщик или Потребитель API.

2.19 Фаззинг

Техника тестирования программного обеспечения, часто автоматическая или полуавтоматическая, заключающаяся в передаче приложению на вход неправильных, неожиданных или случайных данных (от англ. fuzzing).

2.20 Экосистема открытого банкинга

Составляющие, обеспечивающие функционирование Открытого банкинга. Включает политики, стандарты API, процедуры, участников, программные средства, регулирование и безопасность.

3 Базовые понятия открытого банкинга

3.1 Участники экосистемы открытого банкинга и их роли

Под открытыми API в данном документе подразумеваются открытые API, позволяющие реализовать концепцию открытого банкинга.

При взаимодействии с использованием открытых API участники исполняют роли экосистемы открытого банкинга, приведенные в таблице:

Таблица 1 - Роли и участники экосистемы открытого банкинга

Роль	Участник
Поставщик открытых API	Банки
Сторонний потребитель открытых API	Юридические лица, предоставляющие услуги другим юридическим и физическим лицам - клиентам банков с использованием открытых API
Надзорный орган	(будет определено позже)
Центр компетенции по стандартам открытого банкинга	(будет определено позже)

Данный Регламент не описывает взаимодействие банков и Потребителей API, одновременно являющихся клиентами этих банков и использующих API для интеграции исключительно в рамках своей компании.

3.1.1 Надзорный орган открытого банкинга

Основная роль Надзорного органа заключается в обеспечении соблюдения стандартов API и обязательств между участниками экосистемы открытого банкинга с использованием подхода, основанного на оценке рисков. Эти обязательства охватывают такие вопросы, как обработка жалоб Клиентов, обеспечение защиты данных, а также безопасность, надежность и масштабируемость предоставляемых API.

Надзорный орган должен:

1) Работать в соответствии со следующими принципами:
   a) действовать прозрачно;
   b) обеспечить инновации и полноценное участие всех участников;
   c) способствовать эволюции экосистемы открытого банкинга в соответствии с новыми технологиями и потребностями Клиентов;
   d) принять подход, основанный на оценке рисков.
2) Контролировать соблюдение требований, которые применяются к экосистеме открытого банкинга;
3) Контролировать стандарты API в банковском секторе;

4) Создать четкий процесс разрешения проблем между участниками, а также процесс эскалации и апелляции;

5) Установить процесс, посредством которого заинтересованные стороны могут участвовать в качестве консультанта для обеспечения эффективного развития экосистемы;

6) Вести реестр Сторонних потребителей открытых API.

3.1.2 Центр компетенции по стандартам открытого банкинга

Для своевременного обновления стандартов API и учета интересов всех Участников необходим орган, основная роль которого заключается в установлении и развитии Регламента и стандартов API, которые будут применяться к экосистеме (далее – центр компетенции по стандартам).

В рамках процесса развития API центру компетенции по стандартам необходимо обеспечить:

1) Прием и обработку замечаний по Регламенту и Стандартам API (опечатки, ошибки, несоответствия);

2) Прием и обработку запросов на изменение Регламента и Стандартов API (расширение или изменение состава передаваемых данных);

3) Формирование предложений Национальному банку Республики Беларусь для внесения изменений в Стандарты API.

Процедура принятия замечаний и запросов на изменение стандартов API должна быть принята и размещена в публичном доступе для всех Участников. Процедура должна позволять Поставщику API и Стороннему потребителю API подавать замечания и запросы на изменение Регламента и стандартов API. Процедура должна позволять Поставщику API и Стороннему потребителю API подавать апелляцию, в случае несогласия с действиями центра компетенции по стандартам.

3.2 Виды API

В соответствии с типом доступа и типом данных открытые API делятся на следующие виды:

1) Информационные;
2) Платежные;
3) Статистические.

В настоящем документе описаны только Информационные API.

3.2.1 Типы доступа к данным

1) Публичный доступ – доступ, при котором любой потребитель API может получить информацию для использования и дальнейшего распространения.

2) Партнерский доступ – доступ, предоставляемый Стороннему потребителю API после регистрации идентификации Стороннего потребителя API:

a) доступ на чтение – Сторонний потребитель API может получать данные без возможности изменять их каким-либо образом;

b) доступ на запись – Сторонний потребитель API может изменять данные по определенным правилам, включая инициацию платежа.

3.2.2 Типы данных

3.2.2.1 Открытые данные

Справочная информация о Банке, например, расположение и режим работы отделений и банкоматов, каталог продуктов, курсы валют и т.д.

3.2.2.2 Статистические данные

Обезличенные агрегированные данные основанные на транзакциях, Клиентах или прочих источниках информации (например, данные об общем числе и сумме транзакций по SIC кодам и т.д.).

3.2.2.3 Справочные данные Клиента

Данные о Клиентах, не относящиеся к транзакционным, полученные банком в ходе корпоративных процедур (проверка платежеспособности, противодействие отмыванию денег и т.д.).

3.2.2.4 Транзакционные данные Клиента

Данные о счетах, а также история транзакций Клиента. Также включает информацию о счете, необходимую для инициации платежа (баланс счета, выписка, реквизиты счета и т.д.).

3.2.2.5 Конфиденциальные данные

Информация, составляющая коммерческую тайну банка (ценовая политика, уровень маржинальности и т.д).

3.2.3 Классификация API

В таблице ниже приведена классификация видов API по видам данных и видам доступа к данным:

Таблица 2 - Классификация видов открытых API

Тип данных	**Тип доступа/Вид API**	
	публичный	***партнерский***

Открытые данные	Информацион-ные	x
Транзакционные данные Клиента	x	Платежные
Справочные данные Клиента	x	Платежные
Статистические данные	x	Статистичес-кие
Конфиденциальные данные	x	x

4 Взаимодействие Поставщика API и Стороннего потребителя API для Информационных API

С целью систематизации работ, возникающих при взаимодействии Поставщика API и Стороннего потребителя API, в рамках Регламента сгруппированы в следующие процедуры:

1) Публикация API;
2) Подписка на API;
3) Тестирование API;
4) Использование API;
5) Мониторинг и контроль использования API;
6) Прекращение доступа к API;
7) Развитие API.

4.1 Публикация API

4.1.1 Первоначальная публикация

Поставщик API должен вести и публиковать реестр своих открытых API согласно стандартам.

Поставщик API должен публиковать в открытом доступе Регламент подключения и использования Открытого API, а также параметры подключения к тестовой среде.

Поставщик API должен классифицировать среды API следующим образом:

1) тестовая;
2) производственная.

Поставщик API должен предоставить следующие сведения:

1) описание API, включая описание форматов, ограничения, известные ошибки, примеры, в том случае, если есть расширения по отношению к стандарту API.

2) соглашение об уровне оказываемой ИТ-услуги, в том числе:

2.1. параметры гарантии (уровень доступности и производительности);

2.2. описание стандартных процедур и шаблоны документов, включая временные параметры (например, получение доступа);

2.3. формализованные каналы коммуникации (например, телефонный номер, адрес электронной почты, форма обратной связи на сайте);

3) параметры подключения к тестовой среде, если она существует.

4.1.2 Публикация новых версий API

Поставщик API может информировать Стороннего потребителя API о новой версии API, размещая сведения на своем сайте или с использованием других средств коммуникации.

В случае публикации новой версии API, Поставщику API рекомендуется обеспечить доступность предыдущей версии API на протяжении, по крайней мере, 90 календарных дней.

Поставщику API следует включать в сведения о новой версии API перечень изменений по сравнению с предыдущей версией.

Поставщику API следует в URL API отражать версию и среду, например: https://api.v2143.sandbox.bank.by.

Поставщику API следует информировать Сторонних потребителей API о статусах опубликованных версий API. Рекомендуемый перечень статусов:

- находящиеся в эксплуатации (Release) – полностью описанные и поддерживаемые, доступные всем текущим и новым Потребителям API;
- ограниченно эксплуатируемые (Limited release) – полностью описанные и поддерживаемые, но доступные не всем Потребителям API (доступ может быть ограничен по принципу участия в бета-тестировании, присутствия в определенном сегменте рынка и т.д.);
- устаревшие (Deprecated) – полностью описанные и поддерживаемые, включая обратно-совместимые исправления ошибок, но недоступные для новых подписчиков;
- выведенные из эксплуатации (Retired) – полностью описанные, но не поддерживаемые и недоступные никому.

4.2 Подписка на API

Сторонний потребитель API для предоставления своим Клиентам информации и/или услуг может подключиться к любому количеству Поставщиков API.

Поставщик API может организовать регистрацию Стороннего потребителя API с целью установления канала коммуникации с Сторонним потребителем API. Процесс регистрации Стороннего потребителя API включает следующие шаги:

1) Сторонний потребитель API отправляет заявку Поставщику API. Примерный перечень реквизитов заявки:

1.1. наименование организации;
1.2. УНП;
1.3. юридический адрес;
1.4. почтовый адрес;
1.5. адрес сайта;
1.6. ФИО представителя;
1.7. телефон представителя;

1.8. адрес электронной почты представителя;

1.9. вид API согласно п. 4.2 Виды API.

2) В ответ Поставщик API может прислать мотивированный отказ или одобрить заявку и предоставить параметры подключения к тестовой среде.

4.3 Тестирование API

Сторонний потребитель API должен провести тестирование API в Тестовой среде.

Поставщик API может организовать тестирование взаимодействия с API на базе собственной Тестовой среды API.

После того, как Потребителем API подтверждено завершение процесса тестирования API, Поставщик API предоставляет параметры подключения к промышленной среде, и Сторонний потребитель API может подключиться к промышленной среде.

4.4 Использование API

Поставщик API должен обеспечить работоспособность Открытого API в соответствии со стандартом.

Поставщик API должен предоставлять Стороннему потребителю API Справочные данные Клиента и Транзакционные данные Клиента только при наличии выраженного согласия Клиента.

Поставщик API должен предоставить Клиенту возможность выразить свое согласие на передачу своих Справочных данных Клиентов и Транзакционных данных Клиентов конкретному Стороннему потребителю API.

Поставщик API должен предоставить Клиенту возможность отозвать свое согласие на передачу своих Справочных данных Клиентов и Транзакционных данных Клиентов конкретному Стороннему потребителю API.

Поставщику API рекомендуется организовать единую точку контакта для Стороннего потребителя API и Клиента по всем вопросам, касающимся использования Открытого API.

Сторонний потребитель API должен обеспечить сохранность информации, не относящейся к открытым данным, полученной при использовании API.

Стороннему потребителю API рекомендуется организовать единый канал коммуникации для Поставщика API и Клиента по всем вопросам, касающимся использования Открытого API.

4.4.1 Мониторинг и контроль использования API

Поставщику API рекомендуется накапливать статистическую информацию по использованию Открытого API, например:

- периоды простоя;
- количество запросов, всего;
- среднее количество запросов в час/день/месяц;
- топ-5 запросов.

Стороннему потребителю API рекомендуется накапливать статистическую информацию по использованию API, например:

- количество запросов к конкретному Поставщику API;
- среднее количество запросов по всем Поставщикам API.

4.5 Прекращение доступа к API

4.5.1 Добровольное прекращение доступа к API

Сторонний потребитель API может в добровольном порядке отказаться от доступа к API. Процедура добровольного отзыва должна быть определена Поставщиком API.

4.5.2 Принудительное прекращение доступа к API

Поставщик API может отключить Стороннего потребителя API от использования API в следующих случаях:

- умышленное или неумышленное искажение данных Поставщика API;
- по договорным основаниям (договор между Поставщиком API и Сторонним потребителем API).

В случае Инцидента (например, информационной безопасности) полное или частичное прекращение доступа Стороннего потребителя API к API может быть осуществлено без предварительного уведомления.

Уведомление о прекращении доступа может публиковаться Поставщиком API на официальном сайте или передаваться по другим каналам коммуникации со Сторонним потребителем API.

4.6 Развитие API

Поставщик API и Сторонний потребитель API не ограничены в праве разрабатывать расширения к стандарту API в рамках двусторонних отношений.

5 Взаимодействие участников экосистемы открытого банкинга

5.1 Проверка и включение в реестр Сторонних потребителей открытых API

Надзорный орган должен проверять Сторонних потребителей API и их программные решения. Обязательства будут распространяться на Сторонних потребителей API как на уровне организации, так и на уровне предоставляемого ими программного решения. Уровень проверки будет различаться для разных видов API и должен быть пропорционален рискам.

Предоставление Сторонним потребителем API Программы и методики испытаний, а также собственного отчета о тестировании, считается достаточным уровнем проверки для Сторонних потребителей API по Информационным API.

5.2 Правовые аспекты

Правоотношения между Поставщиком API и Сторонним потребителем API в части использования Информационных API, выполняющих информационные функции и содержащих только открытые сведения, рекомендуется оформлять в виде договора присоединения. В таком случае Поставщик API предоставляет Информационные API по принципу «как есть» и не гарантирует бесперебойную и безошибочную работу API.

При необходимости Поставщик API и Сторонний потребитель API могут заключить договор другого вида с необходимыми коммерческими условиями, ответственностью и уровнем оказания услуг.

Правовые отношения между Сторонним потребителем API и Клиентом определяются соглашением, заключенным между ними.

6 Стандартизация в области открытых API

Для каждого вида API разрабатывается стандарт API. Стандарт API должен включать следующие части:

1) Спецификация (описание) данных;
2) Описание подхода к реализации API;
3) Требования по обеспечению безопасности.

Спецификация данных необходима всем участникам Регламента для понимания состава и качества передаваемых данных. Структура данных включает в себя описание передаваемых сложных объектов данных, структур запросов и ответов. В качестве языка описания API должен использоваться один из наиболее распространенных языков описания (RAML или OpenAPI).

Описание подхода к реализации API включает в себя архитектурный подход, требования к формату запросов и ответов, документированию. Данный раздел обеспечит единообразие реализации и упрощение разработки для Сторонних потребителей API.

Требования по обеспечению безопасности должны обеспечить защиту Клиентов банков от злоумышленников.

Должен быть создан общедоступный ресурс для потенциальных разработчиков, на котором будут доступны актуальные версии стандарта API.

Рекомендуется создать общедоступную Тестовую среду API для тестирования API, с помощью которой разработчики смогут протестировать свои приложения без необходимости подключаться к локальным Тестовым средам API банков. При этом общедоступная Тестовая среда API может быть реализована в виде скачиваемого контейнера (виртуальной машины), которую каждый разработчик может скачать и запустить локально, чтобы не было необходимости создавать и поддерживать постоянно работающую инфраструктуру.

6.1 Ключевые требования к реализации API

Подход к реализации API должен соответствовать следующим критериям:

- Использование REST в качестве архитектурного стиля и HTTPS в качестве транспорта;
- Использование JSON и XML в качестве формата ресурса;
- Достижение уровня 2 из модели зрелости Ричардсона;
- Принятие независимого от технологии и поставщика определения интерфейса, то есть URI, запросы, ответы, методы HTTPS и коды состояния.

Стандарт реализации API должен соответствовать следующим требованиям к версиям:

- Поддержка основных и второстепенных выпусков версий;
- Обратная совместимость для всех второстепенных и, насколько это возможно, основных выпусков версий;

● Назначение минимальных периодов поддержки для основных выпусков версий;

● Встроенная гибкость и скорость реагирования для устранения проблем безопасности или функциональных ошибок.

Стандарт реализации API должен включать следующие возможности:

● Поставщику API должны быть разрешены локальные расширения API, что позволит ему предлагать нововведения с последующим возможным включением в стандарт;

● Специфические характеристики, позволяющие Поставщикам API решать проблемы масштабируемости.

6.2 Рекомендации по лицензированию стандарта

Стандарт API может публиковаться на условиях, эквивалентных лицензии CC-BY (https://creativecommons.org/licenses/?lang=ru).

7 Обеспечение безопасности в области открытых API

7.1 Существующие стандарты безопасности

Открытые API должны использовать, насколько это возможно, существующие, зрелые, открытые протоколы и стандарты безопасности. Существует ряд очевидных кандидатов для включения в стандарты API (например, TLS, OAuth и OpenID Connect).

Предлагается принять подход к стандартам безопасности, основанный на серии стандартов ISO 27000, с многоуровневым подходом, т.е. стандарт, которому должен соответствовать Сторонний потребитель API, и степень проверки, которой он подлежит, должна быть соразмерна с уровнем доступа, который Сторонний потребитель API намеревается получить. Для более низких уровней доступа (например, доступа к открытым данным) самопроверка может быть признана достаточной, в то время как для высоких уровней может потребоваться независимая проверка соответствия Стороннего потребителя API соответствующим стандартам.

Серверы и инфраструктура, которыми управляют Сторонние потребители API и Поставщики API, должны быть защищены от кибератак. Стандарты безопасности должны предусматривать меры безопасности, соразмерные характеру предоставляемых данных и функциональности. На данном этапе в этом Регламенте не рассматриваются подробности, относящиеся к соответствующим элементам управления безопасностью, но ожидается, что они будут включать в себя использование тестирования на проникновение, брандмауэры, системы обнаружения вторжений, модули аппаратной безопасности, политики обновления операционных систем и т.д. Рекомендуется для определения стандартов безопасности в этой области и последующего их анализа через определенные промежутки времени проводить встречи рабочей группы, чтобы обеспечить их соответствие новейшим угрозам и технологиям.

Необходимость и степень своевременного включения тестирования безопасности приложений и услуг – это тема, которая должна быть более подробно рассмотрена на будущих этапах работы.

7.2 Шифрование

Соединения API должны выполняться только с использованием HTTPS с использованием протокола TLS v1.2+.

Шифрование сообщений на получателя следует рассмотреть в будущем, если среда угроз безопасности существенно изменится и/или ее использование станет более распространенным.

7.3 Обеспечение безопасности при разработке приложений

Как Сторонние потребители API, так и Поставщики API должны быть обязаны принимать меры для минимизации рисков недостатка безопасности в любом программном обеспечении, которое они развертывают для предоставления или использования API. Меры могут включать принятие методологии безопасного жизненного цикла разработки программного обеспечения (например, OpenSAMM, Security Development Lifecycle), тестирование на проникновение, фаззинг или анализ исходного кода. Строгость необходимых мер должна соответствовать характеру передаваемых или потребляемых данных.

7.4 Обмен информацией и обработка инцидентов

Все участники экосистемы открытых API должны нести ответственность за передачу любой информации о мошеннических угрозах безопасности. Сторонний потребитель API должен сообщать о любых инцидентах и проблемах, имеющих значение для безопасности, принимать формальные процедуры для подтверждения и расследования таких случаев, устранения любых обнаруженных уязвимостей безопасности. В дополнение к существующим законодательным требованиям рекомендуется, чтобы Сторонние потребители API и Поставщики API сообщали о любых нарушениях безопасности, которые влияют на данные или функциональные возможности API, как в Надзорный орган, так и всем затронутым нарушениями Клиентам. В случае, если Сторонний потребитель API страдает от нарушения безопасности, которое затрагивает данные API, полученные от Поставщика API, Поставщик API также должен быть уведомлен. Должны быть разработаны протоколы для ускорения обмена информацией между Поставщиками и Потребителями API в поддержку расследования потенциальных случаев мошенничества или нарушений безопасности.

7.5 Аудит использования API

Ожидается, что подробные журналы вызовов открытых API должны будут вестись Поставщиками API и Сторонними потребителями API для облегчения расследований. Данные журналы должны автоматически формироваться программным обеспечением Поставщика API и Стороннего потребителя API и включать следующие параметры:

1) Дата и время вызова;
2) IP адрес вызывающей стороны;
3) URL вызова;
4) Заголовки HTTP;
5) Содержимое запроса;
6) Дата и время ответа;
7) Содержимое ответа.

7.6 Подход к обеспечению безопасности Информационных API

По определению, нет причин ограничивать доступ к открытым данным. Поэтому нет необходимости предотвращать несанкционированный доступ к открытым данным (хотя может возникнуть необходимость ограничить доступ по другим причинам, таким как предотвращение DoS-атак).

Может возникнуть необходимость защитить целостность открытых данных и предотвратить изменение открытых данных недобросовестными Участниками. Поэтому инфраструктура, используемая для обеспечения доступа к открытым данным, должна быть защищена от несанкционированных изменений. Также может потребоваться аутентификация источника данных.

В случае, если личные данные анонимизируются для публикации в качестве открытых данных, необходимо позаботиться о том, чтобы шаги, предпринятые для анонимизации, исключали деанонимизацию (в том числе посредством комбинации нескольких открытых наборов данных).

8 Список используемой литературы

При разработке Регламента использовались следующие источники:

- Open Banking Standard (https://www.openbanking.org.uk/providers/standards/);
- Directive (EU) 2015/2366 on payment services (PSD2) European Commission и European Banking Authority (EBA);
- Отчет о научно-исследовательской работе по теме «Пути внедрения в банковскую практику открытых протоколов интерфейса прикладного программирования».

При разработке Регламента учтен опыт иностранных и отечественных банков, а также положения международных нормативно-правовых актов, таких как:

- Директива о защите персональных данных (General Data Protection Regulation – GDPR);
- Технический стандарт по строгой аутентификации Клиентов в рамках PSD2 (Technical Standards on Strong Customer Authentication – TS-SCA);
- Требования к платежным услугам (Payment Services Regulations – PSR).