УТВЕРЖДЕНО

Постановление Правления
Национального банка
Республики Беларусь
31.12.2019 № 552

СТАНДАРТ ПРОВЕДЕНИЯ РАСЧЕТОВ

СПР 6.01-2020 ”Банковская деятельность. Информационные технологии. Открытые банковские API. Регламент взаимодействия поставщиков API и пользователей API“

РАЗДЕЛ I
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий стандарт проведения расчетов (далее – стандарт) определяет регламент взаимодействия банков, небанковских кредитно-финансовых организаций, открытого акционерного общества ”Банк развития Республики Беларусь“, открытого акционерного общества ”Белорусская валютно-фондовая биржа“ (далее – банки), являющихся поставщиками программного интерфейса приложения (далее – API), и пользователей API.

2. Настоящий стандарт предназначен для поставщиков API и пользователей API и применяется при разработке приложений, использующих открытые API, и в процессах предоставления API их поставщиками.

3. В настоящем стандарте используются следующие термины и их определения:

API – набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних по отношению к данному приложению (библиотеке, сервису) программных продуктах;

информационный API – API к общедоступной информации по операциям и услугам банков;

клиент – юридическое лицо, в том числе банк, нотариус, адвокат, осуществляющий адвокатскую деятельность индивидуально, физическое лицо, в том числе индивидуальный предприниматель, обслуживаемые банком;

открытый API – API, открытый доступ к которому предоставляется его поставщиком при выполнении пользователем API требований, установленных Национальным банком и (или) поставщиком API;

платежный API – API, предоставляемый банком пользователю API с целью получения последним информации о состоянии счета клиента, открытого в банке, информации о наличии на указанном счете необходимой суммы денежных средств и их движении, и другая информация по счету клиента;

пользователь API – клиент, который использует API в собственных целях не для коммерческого использования (пользователь API первого типа) либо в коммерческих интересах (пользователь API второго типа);

поставщик API – банк, предоставляющий открытый API;

статистический API – API, предоставляющий доступ к информации первичных учетных документов по операциям в банках, о первичных операциях в банках;

тестовая среда API – совокупность программных и (или) программно-технических средств и (или) специальный режим функционирования API с использованием тестовых данных.

4. Открытые API делятся на следующие типы:

информационные;

платежные;

статистические.

5. Персональные данные клиента, информация по его счету, информация первичных учетных документов по операциям в банках, о первичных операциях в банках являются информацией ограниченного распространения. Предоставление и хранение указанных сведений осуществляются в соответствии с законодательством.

6. При каждом запросе (сеансе связи) на предоставление информации по счету клиента, информации первичных учетных документов по операциям в банках, о первичных операциях в банках пользователь API должен быть однозначно авторизован поставщиком API.

7. Запрос информации о наличии на счете необходимой суммы денежных средств не является авторизацией на блокировку указанной суммы денежных средств на счете.

8. В состав общедоступной информации, предоставляемой посредством информационных API, входит:

информация о курсах валют (при проведении операций с наличными и (или) безналичными денежными средствами, в том числе с использованием банковских платежных карточек, систем дистанционного банковского обслуживания, программно-технической инфраструктуры с использованием банковских платежных карточек);

информация о пунктах обслуживания клиентов банка (отделения, филиалы, обменные пункты, пункты самообслуживания с использованием программно-технической инфраструктуры с использованием банковских платежных карточек) с указанием адреса и времени работы, контактных телефонов, адресов электронной почты, списком оказываемых услуг и иная информация о каждом пункте обслуживания;

информация о банковских операциях и услугах (об открытии и ведении банковских счетов, предоставлении кредитов, привлечении денежных средств во вклады (депозиты), выпуске в обращение (эмиссии) банковских платежных карточек, привлечении драгоценных металлов во вклады (депозиты), условиях осуществления денежных переводов, включая переводы без открытия счета, и иная информация).

9. Для тестирования API может быть создана общедоступная тестовая среда API, с помощью которой потенциальные пользователи API второго типа, и, при необходимости, пользователи первого типа, смогут протестировать свои приложения на соответствие предъявляемым требования API без необходимости подключаться к локальным тестовым средам поставщиков API.

Общедоступная тестовая среда API может быть реализована в виде скачиваемого контейнера (виртуальной машины), которую потенциальный пользователь API может скачать и запустить локально, чтобы не было необходимости создавать и поддерживать постоянно работающую инфраструктуру.

РАЗДЕЛ II
РЕГЛАМЕНТ ВЗАИМОДЕЙСТВИЯ ПОСТАВЩИКОВ API И ПОЛЬЗОВАТЕЛЕЙ API

ГЛАВА 1
ОБЩИЕ ТРЕБОВАНИЯ

10. Предоставление поставщиками API доступа к API осуществляется на основании публичного договора, в который рекомендуется включать следующие положения:

10.1. пользователь API второго типа получает доступ к общедоступной информации после идентификации и авторизации его поставщиком API;

10.2. пользователь API второго типа имеет право на обработку информации, получаемой посредством платежных или статистических API для предоставления клиенту, и отвечает за корректность такой обработки;

10.3. предоставление пользователю услуг пользователя API второго типа общедоступной информации, полученной посредством информационных API, предоставляется клиенту в неизменном виде;

10.4. при нарушении пользователем API второго типа требований, согласованных поставщиком API и пользователем API в публичном договоре, поставщик API имеет право прекратить доступ к API такому пользователю API в случае:

искажения пользователем API второго типа данных поставщика API;

деструктивного действия со стороны пользователя API второго типа;

невыполнения пользователем API второго типа условий договора с поставщиком API;

10.5. информация по счету клиента может быть предоставлена поставщиком платежных API:

поставщику платежных API первого типа в целях получения указанной информации по счетам, владельцем которых он является;

поставщику платежных API второго типа в целях предоставления (обеспечения предоставления) данным поставщиком указанной информации пользователю своих услуг по счетам, владельцем которых такой пользователь является;

10.6. согласие клиента на предоставление пользователю API своих персональных данных и информации по его счету может быть отозвано клиентом;

10.7. ответственность пользователя API за ненадлежащую обработку, передачу, хранение, защиту и обеспечение безопасности полученных посредством API персональных данных пользователя его услуг и информации по его счету.

11. Правоотношения между поставщиком API и пользователем API в части использования информационных и платежных API, как правило, оформляются в виде договора присоединения.

В случае предоставления информационных API его поставщиком на основании публичного договора с офертой поставщик API предоставляет информационные API по принципу ”как есть“ и не гарантирует бесперебойную и безошибочную работу API.

При необходимости поставщик API и пользователь API могут заключить договор другого вида с необходимыми коммерческими условиями, степенью ответственности и уровнем оказания услуг.

12. Правоотношения между пользователем API второго типа и пользователем его услуг определяются договором либо соглашением, заключенным между ними.

13. С целью систематизации работ, возникающих при взаимодействии поставщика API и пользователя API второго типа, могут использоваться следующие формы взаимодействия, которые согласовываются поставщиком API и пользователем API второго типа в публичном договоре:

публикация API;

подписка на API;

тестирование API;

использование API и прекращение доступа к API;

мониторинг использования API и развитие API.

ГЛАВА 2
ПУБЛИКАЦИЯ API

14. Поставщик API ведет и публикует перечень своих открытых API согласно стандартам API.

Поставщик API публикует в открытом доступе регламент подключения и использования открытого API, а также параметры подключения к тестовой среде.

15. Поставщик API классифицирует среды API следующим образом:

тестовая;

производственная.

16. Поставщик API предоставляет следующие сведения:

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

16.2. соглашение об уровне оказываемой ИТ-услуги, в том числе:

параметры гарантии (уровень доступности и производительности);

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

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

16.3. параметры подключения к тестовой среде поставщика API (в случае ее наличия).

17. Поставщик API информирует пользователей API второго типа о новой версии API и планируемых датах ее выхода, размещая сведения на своем сайте в глобальной компьютерной сети Интернет или с использованием других средств коммуникации.

В случае публикации новой версии API поставщик API обеспечивает доступность предыдущей версии API на протяжении не менее 90 календарных дней.

Поставщик API включает в сведения о новой версии API перечень изменений по сравнению с предыдущей версией.

Поставщик API отражает версию и среду API в URL (например: https://api.v2143.sandbox.bank.by).

18. Поставщик API информирует пользователей API второго типа о статусах опубликованных версий API.

Рекомендуемый перечень статусов:

находящиеся в эксплуатации (Release) – полностью описанные и поддерживаемые, доступные всем текущим и новым пользователям API второго типа;

ограниченно эксплуатируемые (Limited release) – полностью описанные и поддерживаемые, но доступные не всем пользователям API второго типа (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 пользователей API второго типа;

выведенные из эксплуатации (Retired) – полностью описанные, но не поддерживаемые и недоступные всем пользователям API второго типа.

ГЛАВА 3
ПОДПИСКА НА API

19. Пользователь API второго типа для предоставления своим клиентам информации и (или) услуг может подключиться к любому количеству поставщиков API.

20. Поставщик API осуществляет регистрацию в своей автоматизированной системе пользователя API второго типа. Процесс регистрации пользователя API второго типа включает следующие этапы:

20.1. направление пользователем API второго типа поставщику API заявки на регистрацию.

Примерный перечень реквизитов заявки на регистрацию:

наименование организации;

учетный номер плательщика (УНП);

адрес места нахождения;

почтовый адрес;

адрес сайта в глобальной компьютерной сети Интернет;

фамилия, собственное имя и отчество (если таковое имеется) представителя;

телефон представителя;

адрес электронной почты представителя;

тип API (согласно пункту 4);

20.2. согласование поставщиком API заявки на регистрацию с предоставлением параметров для подключения к тестовой среде или направление пользователю API второго типа мотивированного отказа по заявке на подписку на API.

ГЛАВА 4
ТЕСТИРОВАНИЕ API

21. Пользователь API второго типа тестирует свое программное решение в тестовой среде поставщика API в соответствии с требованиями поставщика API.

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

23. После того, как пользователем API второго типа подтверждено завершение процесса тестирования API, поставщик API предоставляет параметры подключения к производственной среде и пользователь API второго типа может к ней подключиться.

ГЛАВА 5
ИСПОЛЬЗОВАНИЕ API И ПРЕКРАЩЕНИЕ ДОСТУПА К API

24. Поставщик API обеспечивает работоспособность открытого API в соответствии со стандартом API.

25. Пользователь API второго типа может в добровольном порядке отказаться от доступа к API. Процедура добровольного отказа определяется поставщиком API.

26. В случае инцидента (например, нарушение информационной безопасности) полное или частичное прекращение доступа пользователя API второго типа к API может быть осуществлено без предварительного уведомления.

27. Уведомление о прекращении доступа может публиковаться поставщиком API на его официальном сайте в глобальной компьютерной сети Интернет или передаваться по другим каналам коммуникации с пользователем API второго типа.

ГЛАВА 6
МОНИТОРИНГ ИСПОЛЬЗОВАНИЯ API И РАЗВИТИЕ API

28. С целью отслеживания использования API, а также последующего анализа и развития API поставщик API накапливает показатели и

аналитическую информацию по использованию открытого API, в том числе:

периоды простоя;

общее количество запросов;

среднее количество запросов в час, день, месяц;

топ-5 запросов.

Поставщик API обеспечивает хранение указанной в части первой настоящего пункта информации в течение не менее одного года.

29. С целью отслеживания использования API, а также последующего анализа и развития API пользователь API второго типа накапливает показатели и аналитическую информацию по использованию API, в том числе:

количество запросов к конкретному поставщику API;

среднее количество запросов по всем поставщикам API.

Пользователь API второго типа обеспечивает хранение данной информации в течение не менее 1 года.

30. Поставщик API и пользователь API второго типа могут разрабатывать расширения к стандарту API в рамках двусторонних отношений.

ГЛАВА 7
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

31. Открытые API используют стандарты информационной безопасности и защищенные открытые протоколы (например, TLS, OAuth и OpenID Connect и иные).

32. Система защиты информации информационной системы пользователя платежного API второго типа должна соответствовать требованиям законодательства в области безопасности и защиты информации.

33. Для информационных API в качестве стандартов информационной безопасности используются стандарты, основанные на серии стандартов ISO 27000, с многоуровневым подходом, который основывается на принципе рискориентированного подхода.

34. Система управления риском безопасности, в том числе киберриском, пользователя API предусматривает:

тестирование на проникновение, брандмауэры, системы обнаружения вторжений, модули аппаратной безопасности, политики обновления операционных систем и т.д.;

реализацию жизненного цикла разработки программного обеспечения (например, OpenSAMM, Security Development Lifecycle и иные);

тестирование программного обеспечения пользователя API второго типа на проникновение, в том числе автоматическое или полуавтоматическое, заключающееся в передаче программному приложению, использующему открытые API, на вход неправильных, неожиданных или случайных данных, или анализ исходного кода.

35. Соединения между клиентом и пользователем API, а также между пользователем API и поставщиком API выполняются только с использованием HTTPS и протокола TLS v1.2+.

36. В случае, если персональные данные анонимизируются для публикации в качестве общедоступной информации, необходимо обеспечить невозможность их деанонимизации (в том числе посредством комбинации нескольких открытых наборов данных).

ГЛАВА 8
ОБМЕН ИНФОРМАЦИЕЙ И ОБРАБОТКА ИНЦИДЕНТОВ

37. Пользователь API сообщает поставщику API о любых инцидентах и проблемах, имеющих значение для информационной безопасности, принимает формальные процедуры для подтверждения и расследования таких случаев, устранения любых обнаруженных уязвимостей информационной безопасности.

38. Пользователи API и поставщики API сообщают о любых нарушениях информационной безопасности, которые влияют на данные или функциональные возможности API, всем затронутым нарушениями клиентам. В случае нарушения информационной безопасности, которые влияют на данные, полученные от поставщика API, пользователь API также уведомляет поставщика API.

39. С целью поддержки расследования потенциальных случаев мошенничества или нарушений безопасности между поставщиками и пользователями API обеспечивается обмен информацией в режиме реального времени.

ГЛАВА 9
ПРОТОКОЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ API

40. С целью облегчения выявления подозрительных случаев реализации риска безопасности, в том числе киберриска, поставщиками

API и пользователями API второго типа ведутся журналы запросов открытых API.

41. Журналы запросов открытых API автоматически формируются поставщиком API и пользователем API второго типа и включают следующие параметры:

дата и время вызова;

IP адрес вызывающей стороны;

URL вызова;

заголовки HTTP;

содержимое запроса;

дата и время ответа;

содержимое ответа.

42. Поставщик API и пользователи API второго типа обеспечивают хранение журналов запросов открытых API в течение не менее 3 лет.