# Токенизация в контексте совершенствования системы безопасности мобильных платежей

# Tokenization in the context of development of the mobile payments safety system

**Левашов А.И.**
Специалист отдела цифрового права Центра технологии распределенных реестров Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет»
e-mail: artem.i.levashov@gmail.com

**Levashov A.I.**
Specialist of digital law department of Distributed ledger technology center of the federal state-owned higher education institution «Saint-Petersburg State University»
e-mail: artem.i.levashov@gmail.com

**Аннотация**
В настоящей статье рассматривается механизм токенизации мобильных платежей при помощи таких приложений, как Apple Pay и Samsung Pay. Анализируется положение поставщиков подобных приложений с точки зрения законодательства о национальной платежной системе. Особое внимание уделяется повышению уровня информационной безопасности расчетов с использованием электронных средств платежа за счет интеграции токенизирующих мобильных приложений.
**Ключевые слова:** мобильные платежи, токенизация, электронные средства платежа, информационная безопасность.

**Abstract**
The article deals with the tokenization mechanism of mobile payments by such applications as Apple Pay and Samsung Pay. This paper is devoted to the analysis of site of mentioned applications providers with regard to the legislation of national payment system. The author focuses on the improvement of information security of payments by electronic means by integration of tokenizing mobile applications.
**Keywords:** mobile payments, tokenization, electronic means of payment, information security.

В настоящее время понятие «токенизация» приобрело в публичном медиапространстве довольно устойчивую коннотацию с тематикой технологий распределенного хранения данных и криптовалют. Следует, однако, учитывать, что данный термин для сферы информационных технологий отнюдь не является новым. Так, под «токеном» обычно понимается некий объем информации или объект материального мира, не обладающий самостоятельной ценностью, однако символизирующий для целей взаимодействия сторон некий более ценный объект правообладания, юридический факт, состояние или иное явление, имеющее юридическое значение. Ввиду широты данного определения, в зависимости от конкретной области под токенизацией могут пониматься отличные друг от друга процессы, что обуславливает многозначность понятия в прикладном смысле. Однако концептуальное значение токена как некого субститута в большинстве случаев сохраняется, и именно от него следует отталкиваться при анализе правовых моделей, включающих в себя взаимодействие с токенами.

Применительно к кредитно-расчетным отношениям, токенизация, наряду с шифрованием, является одним из основных механизмов обеспечения конфиденциальности платежной информации. С ее помощью конфиденциальные элементы платежного инструмента (например,

«критичные аутентификационные данные» банковской карты [1, с. 6]) при переводе денежных средств от держателя инструмента мерчанту подменяются идентификатором, присваиваемым администратором системы токенизации. За счет этой операции дальнейшее информационное взаимодействие между мерчантом и его клиентом осуществляется без вовлечения конфиденциальных данных, что позволяет существенно снизить риск компрометации платежного инструмента. При этом, в сравнении со сквозным шифрованием, токенизация является более адаптивным и менее затратным механизмом повышения уровня безопасности расчетов [2]. В частности, токенизацию легче интегрировать в процесс оказания банковских электронных услуг, растущая популярность которых среди основного населения неизбежно коррелирует с увеличением числа несанкционированных переводов денежных переводов [3, с. 4–7].

Яркими примерами подобной интеграции являются системы мобильных платежей, в частности, Apple Pay и Samsung Pay. Данные сервисы мобильной коммерции фактически вдохнули новую жизнь в токенизацию за счет снятия многих операционных рисков и сложностей, а также обеспечения высокого качества процессинга больших объемов соответствующих переводов [4]. Их использование предполагает эмуляцию образа банковской карты при помощи специального мобильного приложения и его дальнейшее использование для совершения NFC и онлайн-платежей. В зависимости от конкретного технологического решения, преобразованный образ банковской карты (токен) хранится в сертифицированном в соответствии с отраслевыми стандартами безопасном модуле устройства (например, Secure Element в смартфонах Apple), на защищенной облачной платформе или в специальном мобильном приложении. Также системы мобильных платежей обеспечивают однократность использования токенов или их элементов (динамических кодов безопасности транзакций).

При этом следует отметить, что разработчики соответствующего программно-аппаратного обеспечения стараются максимально дистанцироваться от администрирования систем токенизации платежных инструментов. Так, например, в Обзоре функций безопасности и конфиденциальности системы Apple Pay неоднократно указывается на то, что корпорация «не сохраняет исходные номера кредитных, дебетовых или предоплаченных карт, добавленных в Apple Pay, и не имеет к ним доступа» [5]. Однако, как описано в данном обзоре, Apple передает введенные пользователем данные банковской карты ее эмитенту или авторизованному им поставщику услуг по подготовке и выделению токенов. В дополнение к этому, корпорация получает от эмитента карты или авторизованного поставщика зашифрованный номер учетной записи (токен) и сохраняет его в Secure Element устройства.

Более того, система Apple Pay предусматривает возможность провайдера этого мобильного приложения отслеживать правомочность обращений к нему путем сбора сведений об использовании соответствующего устройства. При этом компания Apple заявляет, что полученные сведения могут быть переданы эмитенту карты пользователя или иным участникам расчетных отношений в целях предотвращения мошенничества [5]. Однако, фактически, поставщик мобильного приложения не берет на себя обязательств по взаимодействию с участниками платежной инфраструктуры, а лишь закрепляет за собой право на сбор информации о настройках устройства, характере его использования, а также о совершаемых с его помощью транзакций. Данные сведения впоследствии используются Apple для совершенствования собственных служб и продуктов, о чем корпорация прямо заявляет в рассматриваемом обзоре. Подобное положение дел порождает парадоксальную ситуацию, когда организация обладает доступом к конфиденциальной платежной информации, но при этом не обладает статусом участникам национальной платежной системы и не является лицом, деятельность которого подлежит оценке на соответствие требованиям банковского законодательства.

Ввиду очевидности того, что поставщик сервиса по осуществлению мобильных платежей принимает непосредственное участие в процессе токенизации платежной карты, вполне правомерной видится постановка вопроса о пределах его ответственности в свете обязанностей по обеспечению безопасности конфиденциальной информации, связанной с денежными

переводами. Анализ обозначенной проблематики следует начать с определения места платежного сервиса (и его поставщика) в системе безналичных расчетов. Представляется, что по своей природе подобные мобильные приложения наиболее близки к электронным средствам платежа (далее – «ЭСП»), к которым, согласно действующему законодательству, следует относить платежные карты, платежные приложения и иные интерактивные платежные инструменты, позволяющие составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств. Необходимо, однако, разграничивать ЭСП и средства доступа к ним, которые сами по себе в качестве ЭСП квалифицироваться не должны [6, с. 20]. Применительно к таким сервисам мобильной коммерции как Apple Pay и Samsung Pay, последние предполагают создание образа уже существующего ЭСП (банковской или иной платежной карты). При этом в отличие от платежных приложений вроде «Сбербанк Онлайн», данные сервисы не позволяют осуществлять операции непосредственно по банковскому счету, к которому привязана карта. Вместо этого, расчеты осуществляются как бы посредством карты (посредством ее токенизированного образа), но с применением дополнительных мер безопасности (например, ввод пароля при авторизации платежного распоряжения, использование Face ID или Touch ID и др.) в целях удостоверения права распоряжения денежными средствами [7].

Применение токенизации в контексте безопасности мобильных платежей представляется особенно уместным в связи с отсутствием сбалансированной системы противодействия осуществлению переводов денежных средств без согласия клиентов. На настоящий момент эта система основывается, в первую очередь, на положениях ст. 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – «Закон о НПС»). В соответствии с ним, устанавливается порядок информационного взаимодействия финансовых организаций и их клиентов в случае утраты контроля над предоставленными последними ЭСП, а также последствия соблюдения и несоблюдения данного порядка. Несмотря на формальную логичность предусмотренных ст. 9 правил, а также наличие особых, льготных условий по компенсации неправомерно списанных средств для физических лиц, их практическая реализация далека от идеала. Как уже отмечалось исследователями [8, с. 69], используемый на практике стандарт доказывания фактически исключает возможность лица получить какое-либо возмещение в случае проведения несанкционированных клиентом операций. Более того, для эффективной защиты своих прав держатель ЭСП вынужден обращаться в немногочисленные экспертные организации, специализирующиеся на компьютерно-техническом анализе мошеннических списаний денежных средств. Помимо того, что поиск компетентных экспертов для рядового клиента банка может оказаться весьма непростой задачей, само их привлечение с учетом соотношения расходов на их участие и размера похищенной суммы зачастую оказывается экономически нерациональным.

В отличие от описанных элементов системы безопасности расчетов с использованием ЭСП, токенизация является не ретроспективной, а превентивной мерой борьбы с соответствующими видами мошенничества. По своей сути она является механизмом, интегрируемым в информационные системы участников расчетных отношений и технически препятствующим совершению несанкционированных операций. Нельзя не отметить, что усиление роли превентивных мер в настоящее время является одним из основных направлений нормотворчества Центрального банка Российской Федерации (далее – «Банк России») в области информационной безопасности расчетов. К нему можно отнести и ужесточение требований к средствам защиты информации, используемым при осуществлении переводов денежных средств, и интенсивную стандартизацию требований к безопасности финансовых операций в целом. Следует также упомянуть о формировании системы мониторинга подозрительных операций на уровне всех операторов по переводу денежных средств. Данная система подразумевает принятие кредитными организациями и иными участниками расчетных отношений мер, необходимых для самостоятельного выявления мошеннических операций, а также их участие в информационном взаимодействии с Банком России, к полномочиям которого отнесено «формирование и ведение базы данных о случаях и попытках осуществления

переводов денежных средств без согласия клиента» [9]. Более подробно перечень мероприятий, которые кредитные организации обязаны реализовывать и порядок информационного взаимодействия определяются в Указании Банка России от 08.10.2018 N 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента».

Указанное движение к совершенствованию системы безопасности расчетов с использованием ЭСП закономерно поднимает вопрос о роли поставщиков приложений, обеспечивающих токенизацию расчетов, и разграничении их сфер ответственности со сферами ответственности эмитентов ЭСП. На сегодняшний день, в Государственную думу РФ уже внесен законопроект №603170-7, имеющий своей целью уточнить требования к использованию на территории РФ «электронных кошельков и других электронных средств платежа, эмитируемых иностранными поставщиками платежных услуг» [10, с. 1]. В данном проекте предлагается возложить на операторов по переводу денежных средств особые обязанности в случае привлечения поставщиков платежных приложений для осуществления расчетов. В соответствии с предлагаемыми дополнениями к ст. 8 Закона о НПС, подобный оператор обязан обеспечить изолированность платежного приложения и его поставщика от конфиденциальной платежной информации, а также выполнение поставщиком приложения законодательных требований по защите информации при совершении переводов денежных средств [11]. Однако представляется, что в отсутствии законодательства, прямо конкретизирующего степень участия сервиса мобильных платежей в осуществлении перевода денежных средств, данные требования вступают в определенное противоречие. Так, в отсутствии доступа поставщика сервиса к конфиденциальной платежной информации, применение к нему ст. 27 Закона о НПС видится необоснованным. Вместе с тем, описанный ранее порядок работы токенизирующих мобильных приложений предполагает их непосредственный доступ к такой информации (пусть и временный), что может выступать предпосылкой для применения ст. 27 и конкретизирующих ее нормативных актов [12], однако вступает в противоречие с положением законопроекта об изолированности приложения. Таким образом, в целях адекватного применения требований об обеспечении информационной безопасности банковских операций, степень участия токенизирующих платежных приложений и их провайдеров требует дальнейшего законодательного раскрытия.

Также, в рассматриваемом законопроекте предлагается установить обязанность операторов по переводу денежных средств, включать в договоры с клиентами о предоставлении ЭСП ряд условий, связанных с использованием ЭСП посредством сервисов мобильных платежей. Данная новелла логически продолжает концепцию привлечения поставщика платежного приложения оператором под свою ответственность. Однако, представляется, что с учетом масштабов поставщиков подобных сервисов, данного решения может оказаться недостаточно. Более эффективным видится определение конкретных требований к поставщикам приложений в области информационной безопасности, а также создание механизмов контроля их деятельности, например, путём закрепления требования по их локализации.

**Литература**

1. Стандарт безопасности данных индустрии платежных карт (PCI DSS) Требования и процедуры оценки безопасности Версия 3.2 Апрель 2016 год. – 180 с. // Совет по стандартам безопасности данных индустрии платежных карт [Официальный сайт]. URL: https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v3_2_RU-RU_Final.pdf (дата обращения: 25.05.2019).

2. Релиз корпорации «Shift4» о токенизации в форме углубленной белой книги. URL: https://web.archive.org/web/20140313203320/http://www.reuters.com/article/2008/09/17/idUS168810+17-Sep-2008+PRN20080917# (дата обращения: 25.05.2019).
3. Обзор несанкционированных переводов денежных средств за 2017 год // Банк России [Официальный сайт]. URL: http://www.cbr.ru/statichtml/file/ 14435/survey_transfers_17.pdf (дата обращения: 25.05.2019).
4. *Рольф А.* Падение и взлет токенизации. URL: https://www.paymentscardsandmobile.com/the-fall-and-rise-of-tokenization/ (дата обращения: 25.05.2019).
5. Обзор функций безопасности и конфиденциальности системы Apple Pay // Apple Inc. [Официальный сайт]. URL: https://support.apple.com/ru-ru/HT203027 (дата обращения: 25.05.2019).
6. *Иванов В.Ю.* Правовая природа и особенности договора об использовании электронного средства платежа. // Законодательство. – 2013. – №9. – С. 18–27.
7. «Положение о правилах осуществления перевода денежных средств» (утв. Банком России 19.06.2012 №383-П). Доступ из СПС «КонсультантПлюс» (дата обращения: 25.05.2019).
8. *Бажанов С.В.* Регистрация и использование электронных средств платежа. // Право и экономика. – 2018. – №1. – С. 64–71.
9. Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе». Доступ из СПС «КонсультантПлюс» (дата обращения: 25.05.2019).
10. Пояснительная записка к проекту федерального закона «О внесении изменений в Федеральный закон «О национальной платежной системе» от 07.12.2018 № 603192-7 // Система обеспечения законодательной деятельности Государственной думы Федерального собрания Российской Федерации [Официальный сайт]. URL: https://sozd.duma.gov.ru/bill/603192-7 (дата обращения: 25.05.2019).
11. Проект федерального закона «О внесении изменений в Федеральный закон «О национальной платежной системе» от 07.12.2018 № 603192-7 // Система обеспечения законодательной деятельности Государственной думы Федерального собрания Российской Федерации [Официальный сайт]. URL: https://sozd.duma.gov.ru/bill/603192-7 (дата обращения: 25.05.2019).
12. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П). Доступ из СПС «КонсультантПлюс» (дата обращения: 25.05.2019).