Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР БФБО-1.7-2023

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФИНАНСОВЫХ СЕРВИСОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ЦИФРОВЫХ ОТПЕЧАТКОВ УСТРОЙСТВ

МОСКВА
2023

ПРЕДИСЛОВИЕ

ПРИНЯТ И ВВЕДЕН в действие приказом Банка России от 01.03.2023 № ОД-335 «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Настоящий Стандарт устанавливает рекомендации, реализация которых направлена на обеспечение организациями банковской системы Российской Федерации и иных сфер финансового рынка Российской Федерации контроля идентификаторов доступа пользовательских устройств методом формирования и обработки цифровых отпечатков устройств при дистанционном предоставлении банковских и финансовых услуг пользователям.

Цифровой отпечаток устройства формируется с использованием методов, с помощью которых осуществляется сбор информации о конфигурации программного и аппаратного обеспечения пользовательского устройства для идентификации устройства, с целью:

- выполнения мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, в том числе для расследования инцидентов защиты информации;
- выявления цепочек связанных операций по переводу денежных средств, совершенных без согласия клиента;
- выявления устройств, неоднократно задействованных при реализации компьютерных атак/инцидентов, в том числе сетевых атак;
- использования в качестве фактора аутентификации.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий Стандарт рекомендован к использованию при реализации контроля идентификаторов устройств пользователей при получении ими банковских и финансовых услуг, устанавливает единые правила формирования уникальных цифровых отпечатков устройств, используемых в целях совершения банковских и финансовых операций.

Настоящим Стандартом предусмотрены случаи формирования уникального цифрового отпечатка пользовательских устройств с целью осуществления мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента (антифрод-мероприятий) при совершении банковских и финансовых операций с использованием недоверенных устройств, которые действуют не в полном соответствии с ожиданиями, при этом не выполняя то, что должны, выявления фактов мошенничества и цепочек связанных операций, разбора инцидентов защиты информации и операций, совершенных без согласия клиента.

Настоящий Стандарт рекомендован к использованию при совершении банковских и финансовых операций:

- кредитными организациями;
- некредитными финансовыми организациями.

Настоящий Стандарт рекомендован для применения путем прямого использования предусмотренных в нем положений при проведении деятельности по формированию, сбору и анализу цифровых отпечатков устройств, а также путем включения ссылок на него и (или) прямого включения содержащихся в нем положений во внутренние документы кредитных организаций и некредитных финансовых организаций.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Пользователь – лицо, использующее техническое устройство с целью проведения банковских и финансовых операций и получения банковских и финансовых услуг.

Цифровой отпечаток (Device Fingerprint) – идентификатор устройства, сформированный в виде производного значения из значений параметров устройства, позволяющий идентифицировать устройство пользователя при получении им банковских и финансовых услуг.

3. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

КО – кредитная организация

НФО – некредитная финансовая организация

ОС – операционная система

iOS – мобильная операционная система для устройств, которые разрабатываются и выпускаются компанией Apple

Android – мобильная операционная система для устройств, которые разрабатываются и выпускаются различными компаниями

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. СТРУКТУРА СТАНДАРТА

- Общее описание технологии цифрового отпечатка.
- Имеющиеся ограничения в использовании технологии цифрового отпечатка.
- Рекомендации по формированию и применению цифрового отпечатка.

4.2. ОБЩЕЕ ОПИСАНИЕ ТЕХНОЛОГИИ ЦИФРОВОГО ОТПЕЧАТКА

Цифровой отпечаток (Device Fingerprint) формируется с учетом таких параметров устройств, как идентификаторы аппаратной части, версия ОС, версия установленного на устройстве браузера и других системных и аппаратных параметров устройства. Основная сложность в формировании цифрового отпечатка состоит в поиске баланса между уникальностью цифрового отпечатка и частотой изменения параметров, которые применяются для его получения.

Для получения цифрового отпечатка, позволяющего более точно идентифицировать устройство, целесообразно использовать комбинацию значений различных параметров, которые уникальны для каждого устройства, а также значения параметров, которые не являются уникальными по отдельности, но в совокупности с другими параметрами создают уникальные значения.

В связи с тем что возможны изменения параметров устройства, в том числе из-за регулярных обновлений браузера и/или ОС, кредитным организациям и некредитным финансовым организациям целесообразно сохранять время получения цифрового отпечатка устройства и исходные значения параметров устройства вместе с полученным на их основе цифровым отпечатком. Данный метод позволит кредитным организациям и некредитным финансовым организациям проводить более точный анализ цифрового отпечатка в дальнейшем, при выявлении и проведении расследования операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента.

4.3. ОСНОВНЫЕ ОГРАНИЧЕНИЯ В ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ЦИФРОВОГО ОТПЕЧАТКА

При определении параметров, которые необходимо получать для формирования цифрового отпечатка, учитывалось следующее:

- в ОС iOS строго ограничено количество версий устройств, размеров экрана, операционных систем. Унифицированные устройства одной и той же модели практически невозможно различить между собой. Уникальных параметров, подходящих для формирования цифрового отпечатка, немного. Методы по получению параметров для цифрового отпечатка меняются редко;
- в ОС Android исходный код открыт, из-за чего существует большое количество разных версий операционных систем, в том числе и неофициальных (измененные пользователями операционные системы, пользовательские сборки). Параметров для формирования цифрового отпечатка намного больше, чем на ОС iOS. Методы по получению параметров для формирования цифрового отпечатка меняются чаще, чем в ОС iOS;
- вне зависимости от используемой ОС при попытке запроса некоторых параметров есть вероятность получить нулевые, пустые значения;
- в разных версиях ОС при извлечении одного и того же параметра могут быть получены разные значения, при этом для получения данных в новых версиях ОС могут быть дополнительно запрошены разрешения со стороны пользователя приложения, что приводит к невозможности получения параметров;
- к изменению параметров устройства могут привести, например, смена используемого браузера, переустановка мобильного приложения, перезагрузка устройства, сброс

устройства, обновление программного обеспечения устройства, смена сим-карты, комплектующих устройств;

- параметры для формирования цифрового отпечатка могут быть изменены, подделаны при помощи различных эмуляторов либо непосредственно пользователем. Часть параметров требует наличия у пользователя повышенных прав (Root, Jailbreak) для их изменения, другая часть параметров не требует при изменении привилегированных прав;
- из-за развития мобильных платформ и браузеров, изменения их настроек, изменения политик доступов состав параметров, необходимых для идентификации устройства, может меняться.

В этой связи в целях применения технологии цифрового отпечатка отбор параметров проводится с учетом следующих критериев:

- применяются параметры, являющиеся легкодоступными для их извлечения;
- применяются параметры, являющиеся наиболее сложными для изменения их значений пользователем;
- применяются параметры, являющиеся уникальными для конкретного устройства.

5. РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ И ПРИМЕНЕНИЮ ЦИФРОВОГО ОТПЕЧАТКА

Настоящим Стандартом рекомендуется применение единых правил формирования цифрового отпечатка кредитными организациями и некредитными финансовыми организациями.

5.1. АЛГОРИТМ ФОРМИРОВАНИЯ ЦИФРОВОГО ОТПЕЧАТКА

Рекомендуется применять следующий алгоритм формирования цифрового отпечатка с вычислением функции хэширования:

1. Приложение или веб-сайт кредитной организации, некредитной финансовой организации проводит сбор данных с устройства пользователя на предмет общих, особых и уникальных параметров и настроек, а также сведений о конфигурации аппаратного обеспечения (указаны в подпунктах 5.1.1 и 5.1.2 настоящего Стандарта).
2. Собранная информация об устройстве объединяется в одну строку[1] в заданном порядке[2] в формате JSON. Полученная строка (исходные параметры) сохраняется отдельно в неизменном виде.
3. Строка с исходными параметрами, собранными в соответствии с пунктом 1 настоящего алгоритма и сохраненными согласно пункту 2 настоящего алгоритма, используется для передачи в кредитную организацию, некредитную финансовую организацию для последующего вычисления функции хэширования (преобразование исходной строки в строку фиксированной длины, состоящую из цифр и букв (далее – хэш) в соответствии с ГОСТ Р 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования» с длиной хэш-кода 512 бит») и применения результата хэширования в качестве цифрового отпечатка устройства.

   Цифровые отпечатки по точкам сбора можно разделить на два основных вида:
   - цифровой отпечаток для браузера (Browser Fingerprint) (точка сбора – персональные компьютеры, мобильные устройства);
   - цифровой отпечаток для мобильного приложения (Mobile Fingerprint) (точка сбора – мобильные устройства).

5.1.1. Цифровой отпечаток для браузера

С учетом указанных в пункте 4.3 критериев в целях создания цифрового отпечатка при использовании браузера рекомендуется использовать параметры устройств, указанные в Таблице 1. Элементы параметров соответствуют определенному формату. При невозможности получения значения какого-либо параметра в значении указывается пустая строка в виде {«Имя_параметра»:»»}.

[1] Ко всем параметрам и настройкам применяется функция Trim (удаляется символ «пробел» (Space) с начала и конца строки).

[2] Рекомендуется соблюдать строгую очередность параметров, приведенную в Таблицах 1 и 2 настоящего Стандарта.

ЦИФРОВОЙ ОТПЕЧАТОК ДЛЯ БРАУЗЕРА *Табл. 1*

Параметр	Описание	Формат данных (Длина / Тип данных / Значения)	Пример
Audiocontext Data	Получение цифрового отпечатка осуществляется путем замера времени выполнения операций по обработке звука в ОС и звуковой карте	Длина: 18 символов Тип данных: строка	`"browserAudiocontextData":124.01347327512079`
Canvas Data	Данные отрисовки определенного изображения с помощью HTML5 Canvas	Длина: 32 символа Тип данных: строка	`"browserCanvasData":315480ccba81274cea2e9b1e215405a6`
CPU	Количество ядер процессора	Длина: 1–2 символа Тип данных: строка	`"browserCPU":2`
Java Enabled	Возможность запускать Java Applet в браузере	Тип данных: логический Допустимое значение: • true • false	`"browserJavaEnabled":true`
Language	Используемый язык	Длина: 1–8 символов Тип данных: строка	`"browserLanguage":"ru"`
Memory	Объем оперативной памяти	Длина: 1–2 символа Тип данных: строка	`"browserMemory":"8"`
Screen Color Depth	Глубина цвета экрана	Длина: 1–2 символа Тип данных: строка Допустимое значение: • 1 = 1 бит • 4 = 4 бита • 8 = 8 бит • 15 = 15 бит • 16 = 16 бит • 24 = 24 бита • 32 = 32 бита • 48 = 48 бит	`"browserScreenColorDepth":"24"`
Screen Height	Высота в пикселях экрана	Длина: 1–6 символов Тип данных: строка	`"browserScreenHeight":"400"`
Screen Width	Ширина в пикселях экрана	Длина: 1–6 символов Тип данных: строка	`"browserScreenWidth":"600"`
Time Zone	Смещение часового пояса в минутах от UTC	Длина: 1–5 символов Тип данных: строка Допустимое значение: значение возвращается из метода getTimezoneOffset ()	`"browserTZ":"0"`
User-Agent	Содержимое HTTP-заголовка User-Agent	Длина: максимум 2048 символов Тип данных: строка Допустимое значение: если общая длина принимаемого заголовка, отправленного браузером, превышает 2048 символов, лишнюю часть вырезать	`"browserUserAgent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0"`
WebGL Data	Данные отрисовки определенного изображения с помощью HTML5 Canvas и WebGL API	Длина: 32 символа Тип данных: строка	`"browserWebGLData":"a52176dabdc3150ee38ea14daf7b10ad"`
WebGL Renderer	Названия графического драйвера	Длина: максимум 128 символов Тип данных: строка	`"browserWebGLRenderer":"ANGLE (NVIDIA, NVIDIA GeForce GT 1060 Direct3D11 vs_5_0 ps_5_0, D3D11-29.0.11.5028)"`
WebGL Vendor	Названия графической карты	Длина: максимум 40 символов Тип данных: строка	`"browserWebGLVendor":"Google Inc. (NVIDIA)"`

5.1.2. Цифровой отпечаток для мобильного приложения

Аналогично цифровому отпечатку для браузера в целях создания цифрового отпечатка устройства в мобильном приложении рекомендуется использовать параметры устройств, указанные в Таблице 2. В ней отражены как универсальные параметры для всех платформ, так и дополнительные – в зависимости от ОС.

ЦИФРОВОЙ ОТПЕЧАТОК ДЛЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ *Табл. 2*

Платформа	Параметр	Описание	Формат данных (Длина / Тип данных / Значения)	Пример
Все платформы	Bluetooth – MAC Address	MAC-адрес Bluetooth устройства	Длина: 17 символов Тип данных: строка	`"Bluetooth_MAC_Address":"00:23:D6:B3:15:8A"`
	Device Model	Производитель и модель мобильного устройства	Длина: 32 символа Тип данных: строка	`"Device_Model":"Google Nexus 5"`
	Device Name	Имя устройства	Длина: 32 символа Тип данных: строка	`"Device_Name":"Google Nexus 5"`
	DeviceID	Идентификатор устройства	Длина: 15 символов Тип данных: строка	`"DeviceID":"862249578241655"`
	ICCID	Уникальный номер установленной сим-карты	Длина: 20 символов Тип данных: строка	`"ICCID":"8901260232714958936"`
	IMEI	Международный идентификатор мобильного оборудования	Длина: 15 символов Тип данных: строка	`"IMEI":"862249578241655"`
	IMSI	Международный идентификатор мобильного абонента	Длина: 15 символов Тип данных: строка	`"IMSI":" 310120265624299"`
	Latitude	Широта местоположения устройства	Длина: 9 символов Тип данных: строка	`"Latitude":"55.069152"`
	Locale	Параметры региональных настроек	Длина: 5 символов Тип данных: строка	`"Locale":"ru-RU"`
	Longitude	Долгота местоположения устройства	Длина: 9 символов Тип данных: строка	`"Longitude":"43.568157"`
	MAC-address	MAC-адрес устройства	Длина: 17 символов Тип данных: строка	`"MAC_address":"02:4E:48:25:23:04"`
	OS Name	Название операционной системы	Длина: 10 символов Тип данных: строка	`"OS_Name":"Android"`
	OS Version	Версия операционной системы	Длина: 10 символов Тип данных: строка	`"OS_Version":"6.0.1"`
	PhoneNumber	Исходный номер телефона	Длина: 10 символов Тип данных: строка	`"PhoneNumber":"9024910550"`
	Screen Resolution	Разрешение экрана	Длина: 10 символов Тип данных: строка	`"Screen_Resolution":"1080x1920"`
	SerialNumber	Серийный номер устройства	Длина: 16 символов Тип данных: строка	`"SerialNumber":"037abc3e09318c78"`
	Time zone	Часовой пояс	Длина: 32 символа Тип данных: строка	`"Time_zone":"Europe/Moscow"`
	Wifi – MAC Address	MAC-адрес Wi-Fi устройства	Длина: 17 символов Тип данных: строка	`"Wifi_MAC_Address":"02:4E:16:25:90:2A"`

Платформа	Параметр	Описание	Формат данных (Длина / Тип данных / Значения)	Пример
iOS	availableLocaleIdentifiers	Массив объектов NSString, каждый из которых определяет локаль, доступную в системе	Длина: 5 символов Тип данных: строка	`"availableLocaleIdentifiers": "ru-RU"`
	buttonFontSize	Стандартный размер шрифта, используемый для кнопок	Длина: 2 символа Тип данных: строка	`"buttonFontSize":"5"`
	familyNames	Массив имен семейств шрифтов, доступных в системе	Длина: 256 символов Тип данных: строка	`"familyNames":""`
	fontNamesForFamilyName	Массив имен шрифтов, доступных в конкретном семействе шрифтов, если используется семейство системных шрифтов	Длина: максимум 1024 символа Тип данных: строка	`"fontNamesForFamilyName":" Arial, Arial Black, Arial Narrow, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Comic Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3"`
	Identifier For Vendor	Буквенно-цифровая строка, которая однозначно идентифицирует устройство для разработчиков приложений	Длина: 16 символов Тип данных: строка	`"Identifier For Vendor":""`
	labelFontSize	Стандартный размер шрифта, используемый для компонента labels	Длина: 16 символов Тип данных: строка	`"labelFontSize":""`
	preferredLanguages	Перечисление языковых предпочтений пользователя в виде массива строк	Длина: 40 символов Тип данных: строка	`"preferredLanguages":"ru"`
	smallSystemFontSize	Размер стандартного мелкого системного шрифта	Длина: 16 символов Тип данных: строка	`"smallSystemFontSize":""`
	systemFont	Системный шрифт	Длина: 16 символов Тип данных: строка	`"systemFont":""`
	systemFontSize	Размер стандартного системного шрифта	Длина: 16 символов Тип данных: строка	`"systemFontSize":""`
	systemLocale	Идентификатор стандартной локали (generic locale), которая содержит фиксированные backstop-параметры, которые предоставляют значения для неопределенных ключей	Длина: 16 символов Тип данных: строка	`"systemLocale":"ru-RU"`
	UserInterfaceIdiom	Стиль интерфейса, используемый на текущем устройстве	Длина: 16 символов Тип данных: строка	`"UserInterfaceIdiom":""`

Платформа	Параметр	Описание	Формат данных (Длина / Тип данных / Значения)	Пример
Android	Build.BOARD	Название платформы, лежащее в основе ядра, например goldfish	Длина: 16 символов Тип данных: строка	"Build_BOARD":"hammerhead"
	Build.BOOTLOADER	Номер версии системного загрузчика	Длина: 16 символов Тип данных: строка	"Build_BOOTLOADER":" HHZ20h"
	Build.BRAND	Производитель устройства	Длина: 16 символов Тип данных: строка	"Build_BRAND":"google"
	Build.DEVICE	Код названия сборки у производителя	Длина: 16 символов Тип данных: строка	"Build_DEVICE":"hammerhead"
	Build.DISPLAY	Идентификатор сборки для отображения пользователю	Длина: 16 символов Тип данных: строка	"Build_DISPLAY":" M4B30Z"
	Build.FINGERPRINT	Строка, которая однозначно идентифицирует сборку	Длина: 100 символов Тип данных: строка	"Build_FINGERPRINT":"google/hammerhead/hammerhead:6.0.1/M4B30Z/3437181:user/release-keys"
	Build.HARDWARE	Название аппаратного обеспечения (из командной строки ядра или /proc)	Длина: 16 символов Тип данных: строка	"Build_HARDWARE":"hammerhead"
	Build.D	Номер изменения сборки или метка типа M4-rc20	Длина: 16 символов Тип данных: строка	"Build_ID":"M4B30Z"
	Build.MANUFACTURER	Производитель сборки	Длина: 16 символов Тип данных: строка	"Build_MANUFACTURER":"LGE"
	Build.PRODUCT	Название продукта	Длина: 16 символов Тип данных: строка	"Build_PRODUCT":"hammerhead"
	Build.RADIO	Номер версии прошивки модуля радио с помощью getRadioVersion ()	Длина: 16 символов Тип данных: строка	"Build_RADIO":"unknown"
	DisplayMetrics.density	Логическая плотность пикселей экрана	Длина: 3 символа Тип данных: строка	"DisplayMetrics_density":"2.0"
	DisplayMetrics.densityDpi	Плотность экрана, выраженная в точках на дюйм	Длина: 3 символа Тип данных: строка	"DisplayMetrics_densityDpi":"320"
	DisplayMetrics.scaledDensity	Множитель масштабирования шрифтов, отображаемых на дисплее	Длина: 3 символа Тип данных: строка	"DisplayMetrics_scaledDensity":"1"
	Package.Manager.getSystemAvailableFeatures	Получает список функций, доступных на устройстве	Длина: 3 символа Тип данных: строка	"Package.Manager_getSystemAvailableFeatures":""
	Package.Manager.getSystemSharedLibraryNames	Получает список общих библиотек, доступных на устройстве	Длина: 3 символа Тип данных: строка	"Package.Manager_getSystemSharedLibraryNames":""
	StatFs.getTotalBytes	Общее количество байтов, поддерживаемое файловой системой	Длина: 3 символа Тип данных: строка	"StatFs_getTotalBytes":""
	Telephony Manager.Group Identifier Level1	Group Identifier Level 1 для телефона GSM	Длина: 3 символа Тип данных: строка	"Telephony_Manager_Group_Identifier_Level1":""

5.2. ЦЕЛЕВЫЕ ТОЧКИ СБОРА ЦИФРОВОГО ОТПЕЧАТКА

Ориентировочные модели оказания банковских и финансовых услуг[3] с обозначением точек (участков) сбора цифрового отпечатка представлены в Приложении к настоящему Стандарту.

Сбор первичного цифрового отпечатка осуществляется кредитной организацией, некредитной финансовой организацией при первом обращении пользователя к функционалу дистанционного банковского обслуживания с использованием мобильного приложения или веб-браузера с целью проведения банковских операций, финансовых операций, получения банковских или финансовых услуг.

Первичный цифровой отпечаток вносится кредитной организацией, некредитной финансовой организацией в базу эталонных цифровых отпечатков устройств пользователя для последующей сверки с цифровым отпечатком устройства, полученным при инициировании пользователем новой операции в мобильном приложении или веб-браузере. Например, при подтверждении перевода денежных средств пользователем и успешном исполнении перевода денежных средств кредитной организацией цифровой отпечаток, собранный при совершении такой операции, становится эталонным и подлежит сохранению в базе эталонных цифровых отпечатков (с заменой предыдущего/первичного эталонного цифрового отпечатка) и так далее для последующих переводов денежных средств пользователя. Так как один пользователь может использовать несколько устройств для доступа к дистанционным сервисам кредитной организации, некредитной финансовой организации, допускается привязка нескольких эталонных отпечатков к одной клиентской записи в базе эталонных цифровых отпечатков устройств пользователя.

5.3. РЕКОМЕНДАЦИИ ПО ХРАНЕНИЮ ЦИФРОВОГО ОТПЕЧАТКА

Кредитным организациям, некредитным финансовым организациям рекомендуется вести базу эталонных цифровых отпечатков устройств пользователя и сохранять в ней:

- полученные цифровые отпечатки при выполнении операций пользователем вместе с данными по операциям;
- эталонные цифровые отпечатки в базе эталонных цифровых отпечатков устройств пользователя вместе с исходными значениями параметров устройства, использованными при формировании соответствующего цифрового отпечатка.

Кредитным организациям, некредитным финансовым организациям при хранении цифровых отпечатков рекомендуется реализовывать следующие мероприятия:

- обеспечить связку с уникальным идентификатором клиента без привязки непосредственно к его персональным данным;
- сохранить дату сбора цифрового отпечатка, наименование (тип устройства) и процент совпадения сравниваемого цифрового отпечатка с эталонным;
- сохранить исходные параметры, на основании которых формировался цифровой отпечаток;
- сохранить историю цифрового отпечатка с признаками актуальности, которая учитывается при анализе или сравнении цифровых отпечатков.

Кредитным организациям, некредитным финансовым организациям рекомендуется хранить собранные цифровые отпечатки устройств вместе с набором параметров, на основе которых они сформированы, а также результаты сверки цифровых отпечатков с эталонными не менее 5 лет с момента их последнего использования.

Кредитным организациям, некредитным финансовым организациям рекомендуется вести базы цифровых отпечатков устройств, замеченных в мошеннических активностях (в том числе неоднократно задействованных при реализации компьютерных атак/инцидентов, а также связанных с вредоносным воздействием на узлы компьютерной сети (боты) и сетевыми атаками).

---

[3] Без учета процесса приема клиента на обслуживание кредитной организацией, некредитной финансовой организацией и первого обращения пользователя к функционалу дистанционного банковского обслуживания с использованием мобильного приложения или веб-браузера.

5.4. ПРИМЕНЕНИЕ ЦИФРОВОГО ОТПЕЧАТКА

Собранные кредитными организациями, некредитными финансовыми организациями по единым правилам цифровые отпечатки устройств пользователей рекомендуется применять следующим образом.

5.4.1. При совершении операции по полученному от пользователя распоряжению выполняется сверка цифрового отпечатка устройства, с которого было получено распоряжение, с эталонным отпечатком для этого устройства (сверка хэшей). В случае если хэши совпадают, применение пользователем доверенного устройства считается подтвержденным. В случае несовпадения хэшей выполняется анализ совпадения параметров, из которых сформированы хэши (цифровые отпечатки). При проведении сверки параметров совпадением считается результат, при котором различие в значениях составляет не более 15% параметров при сравнивании эталонного отпечатка с направляемым, при этом кредитные организации, некредитные финансовые организации вправе устанавливать внутренними документами иные пороговые значения, которые будут коррелировать, например, с датой внесения цифрового отпечатка в эталонную базу.

Процент совпадения используется кредитными организациями, некредитными финансовыми организациями для качественной и количественной оценки, идентификации операционного риска, классификации операционных рисков и потерь от их реализации, в том числе согласно Положению Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

5.4.2. При реализации мероприятий по противодействию осуществлению переводов денежных средств, совершенных без согласия клиента, в том числе для расследования инцидентов защиты информации, цифровой отпечаток применяется для обнаружения подмены доверенного устройства пользователя. Кредитная организация при реализации подпункта 5.4.1 настоящего Стандарта проводит анализ нетипичного поведения пользователя (в том числе отличие совокупности параметров цифрового отпечатка и аутентификаторов) и в случае выявления признаков осуществления перевода денежных средств без согласия клиента приостанавливает исполнение распоряжения о совершении такой операции.

5.4.3. Цифровой отпечаток, полученный при выполнении операции пользователем, используется при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, мероприятий по выявлению и противодействию осуществлению операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, в соответствии с нормативными актами Банка России, принятыми на основании частей 4, 6 и 7 статьи 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», частей 2, 4 и 5 статьи 12 Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы». Кредитным организациям, некредитным финансовым организациям рекомендуется:

- выявлять компьютерные атаки, направленные на устройства пользователей, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента, операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, путем сравнения направляемых цифровых отпечатков с эталонными и выявления подозрительных аномалий, которые могут быть похожи на компьютерные атаки;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на устройства пользователей, в целях сбора данных об аномальных отклонениях в цифровых отпечатках для повышения эффективности реагирования на компьютерные атаки.

5.4.4. Цифровой отпечаток рекомендуется использовать в рамках выполнения требований о безопасности критической информационной инфраструктуры согласно Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»:

- информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации в установленном указанным федеральным органом исполнительной власти порядке;
- при реагировании на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5.4.5. Для выявления признаков осуществления перевода денежных средств без согласия клиента, предупреждения осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, кредитным организациям, некредитным финансовым организациям рекомендуется сравнивать цифровой отпечаток, полученный от потенциального злоумышленника, с имеющимися в базе отпечатками и выявлять совпадения, которые помогут при расследовании инцидентов.

5.4.6. Для выявления цепочек связанных операций по переводу денежных средств, выполненных в разных кредитных организациях, а также для выявления устройств, неоднократно задействованных при реализации компьютерных атак/инцидентов, в том числе связанных с вредоносным воздействием на узлы компьютерной сети (боты) и сетевыми атаками, рекомендуется включать информацию о цифровом отпечатке совместно с набором параметров, на основе которых он сформирован, в состав уведомлений, направляемых в ФинЦЕРТ Банка России в соответствии с нормативными актами Банка России, указанными в подпункте 5.4.3 настоящего пункта.

6. БИБЛИОГРАФИЯ

- Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Федеральный закон от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы».
- Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
- Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».
- Положение Банка России от 04.06.2020 № 719-П «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».
- Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
- Стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».
- Указание Банка России от 08.10.2018 № 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».
- Указание Банка России от 15.12.2020 № 5662-У «О форме и порядке направления операторами финансовых платформ в Банк России информации обо всех случаях и (или) о попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, и получения операторами финансовых платформ, финансовыми организациями от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, а также о порядке реализации операторами финансовых платформ мероприятий по выявлению операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, и противодействию в совершении таких сделок».
- EMV® 3D Secure SDK-Device Information – https://www.emvco.com/wp-content/uploads/documents/EMVCo_3DS_SDKDeviceInfo_1_4_102019.pdf.
- Межгосударственный стандарт ГОСТ Р 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». Дата введения – 01.06.2019.

- Стандарт Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации». Дата введения – 01.11.2018.
- Стандарт Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» (принят и введен в действие приказом Банка России от 30.11.2016 № ОД-4234).
- Национальный стандарт Российской Федерации ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». Дата введения – 27.12.2006. Переиздание – декабрь 2018 года.

ПРИЛОЖЕНИЕ

СХЕМА ПЕРЕВОДОВ В СИСТЕМЕ БЫСТРЫХ ПЛАТЕЖЕЙ (СБП)

Рис. 1

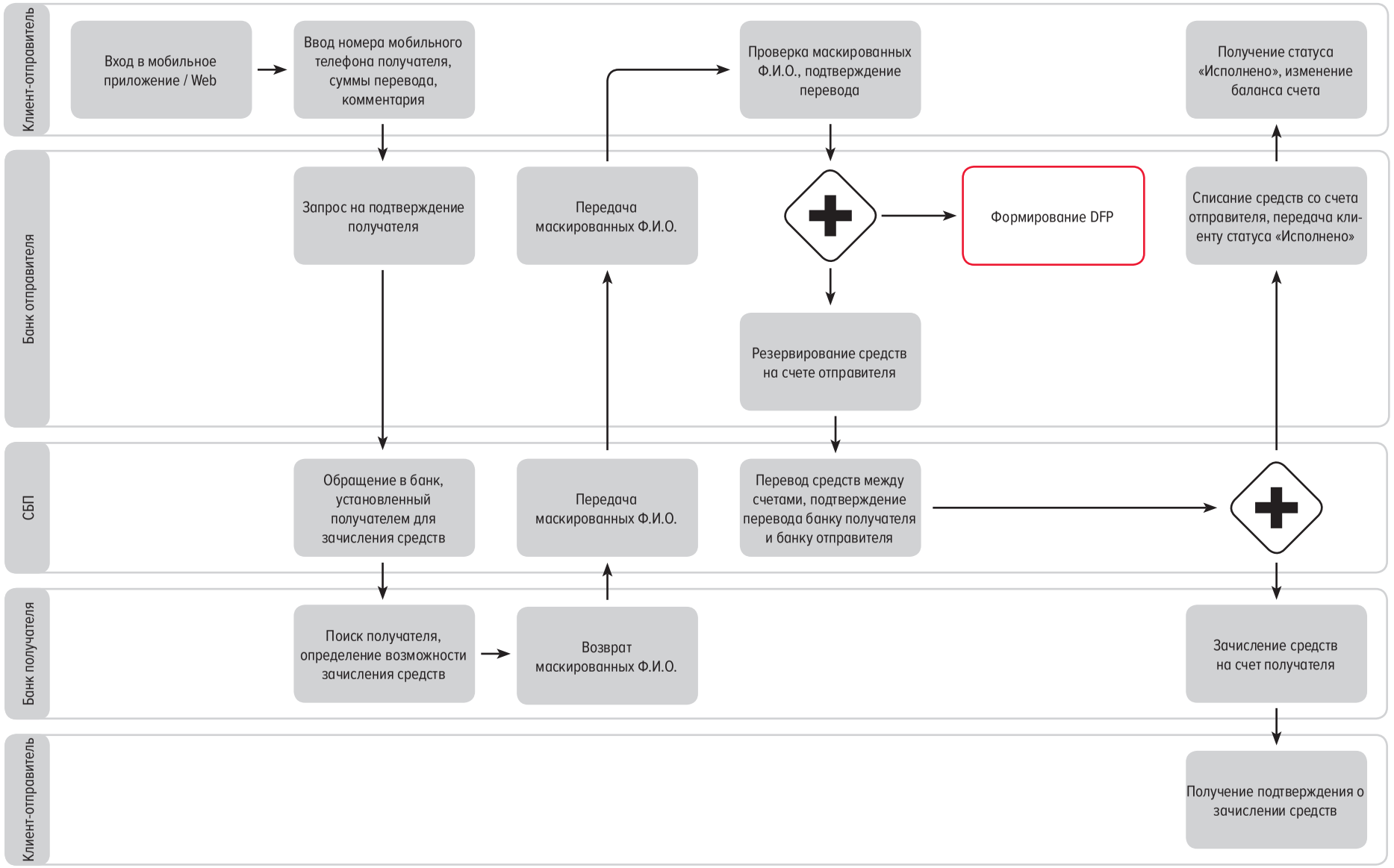

СХЕМА ПЕРЕВОДОВ В ДРУГОЙ БАНК

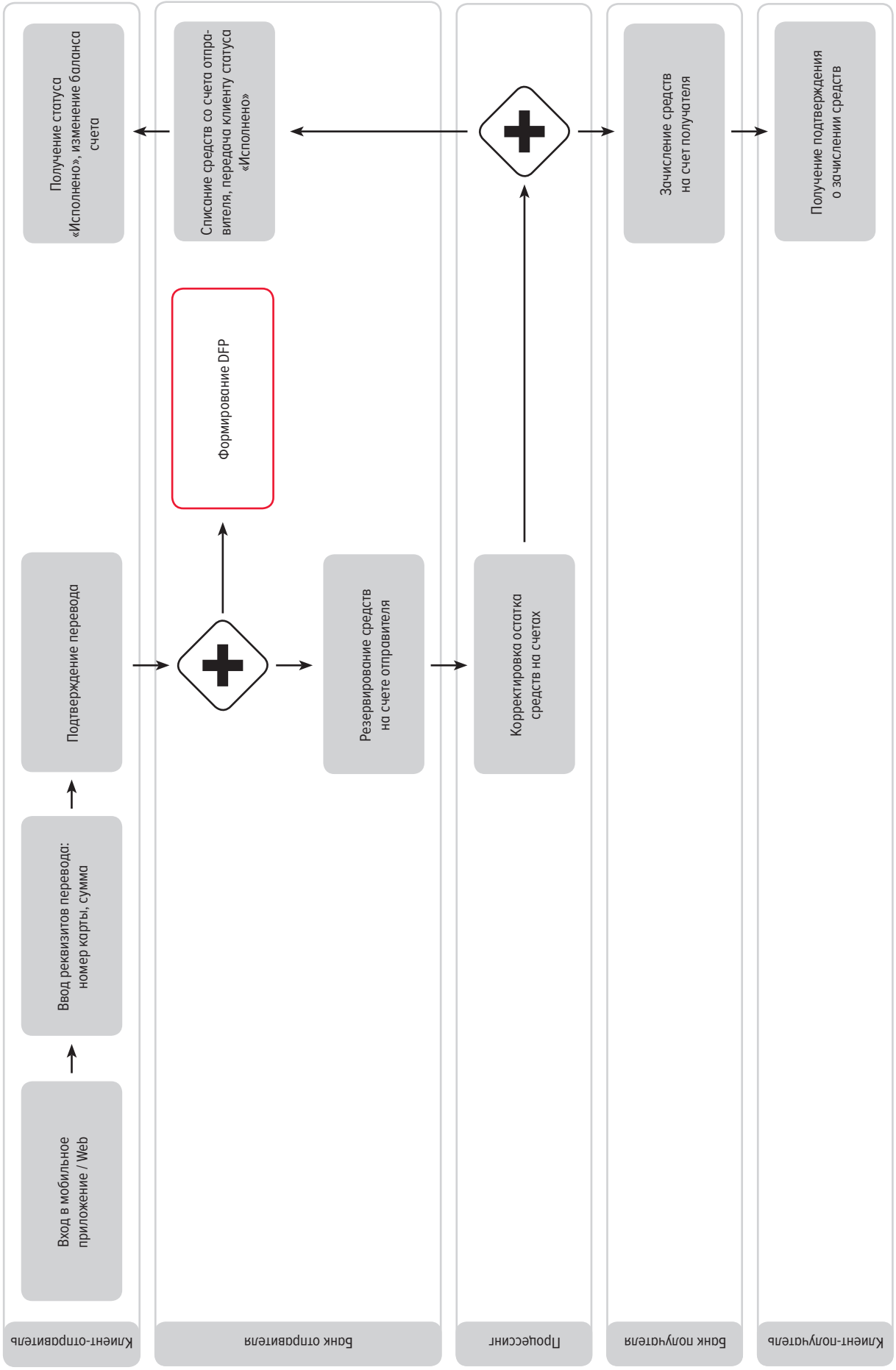

Рис. 2

Рис. 3

СХЕМА ПЕРЕВОДОВ В ПРЕДЕЛАХ ОДНОГО БАНКА

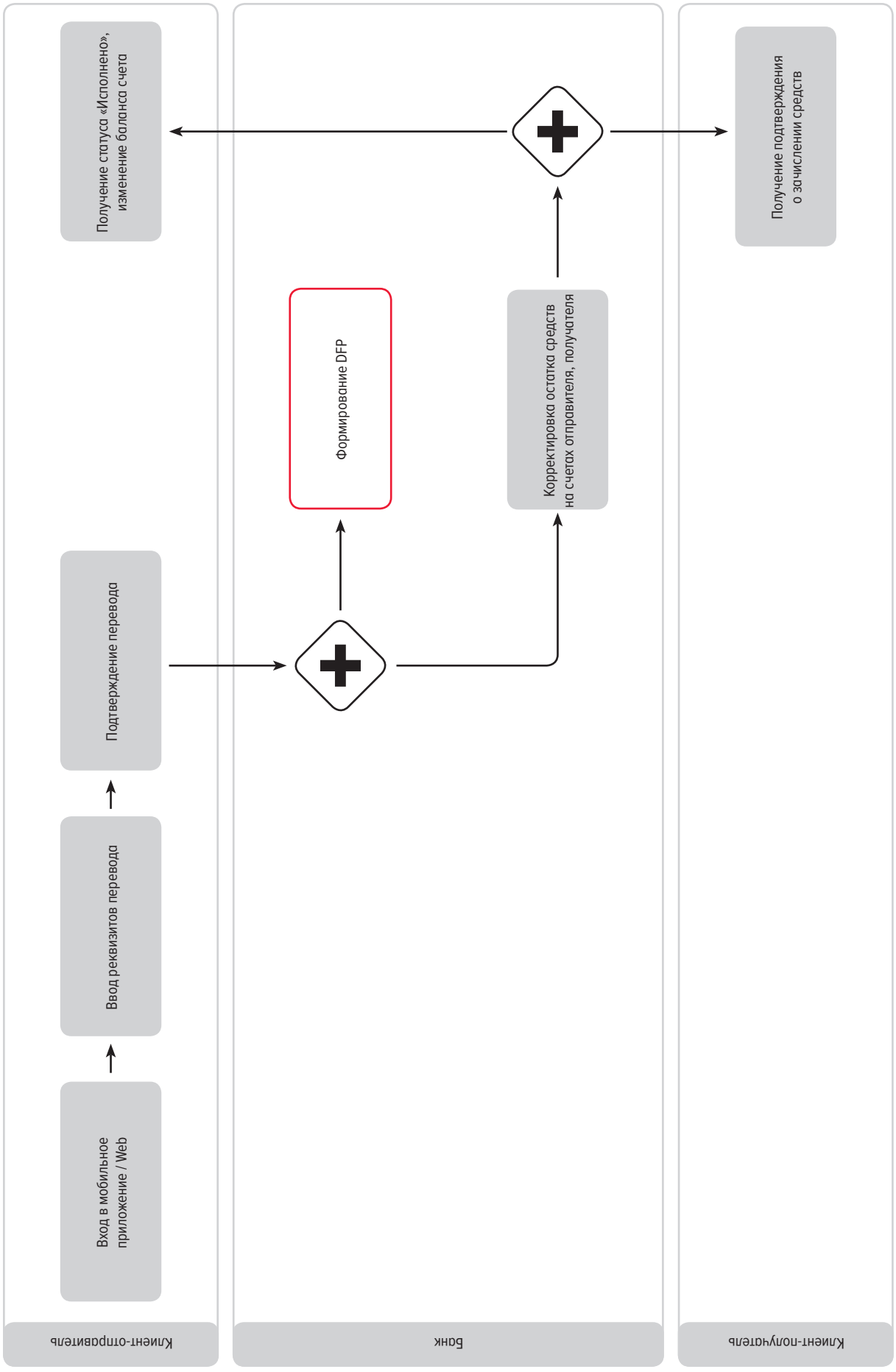

Рис. 4

СХЕМА ПЕРЕВОДОВ ЧЕРЕЗ ПОПОЛНЕНИЕ С КАРТЫ ДРУГОГО БАНКА

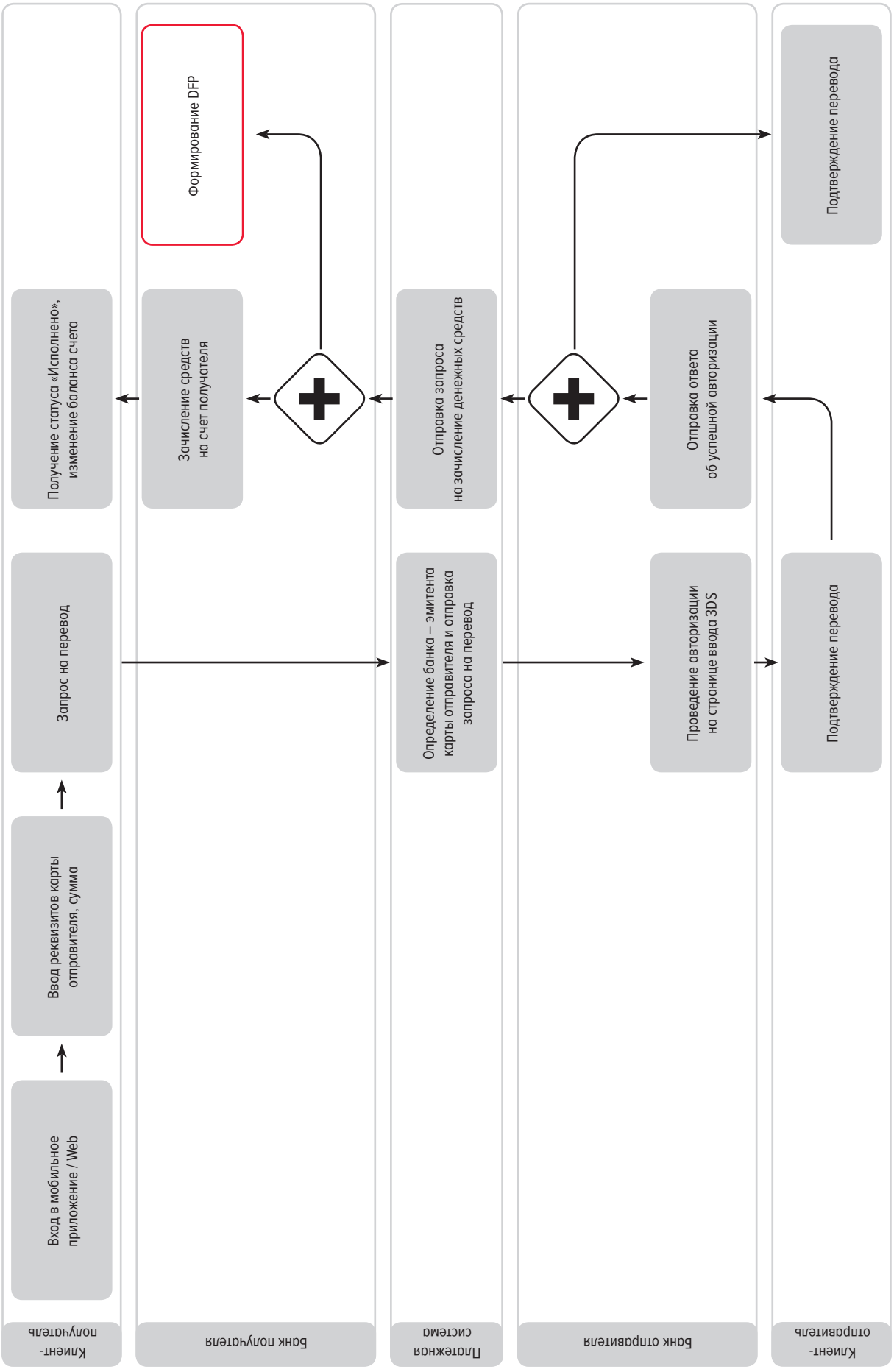

СХЕМА ПЕРЕВОДОВ НА СЧЕТ

Рис. 5