Информационная безопасность банковских безналичных платежей. Часть 2 — Типовая IT-инфраструктура банка

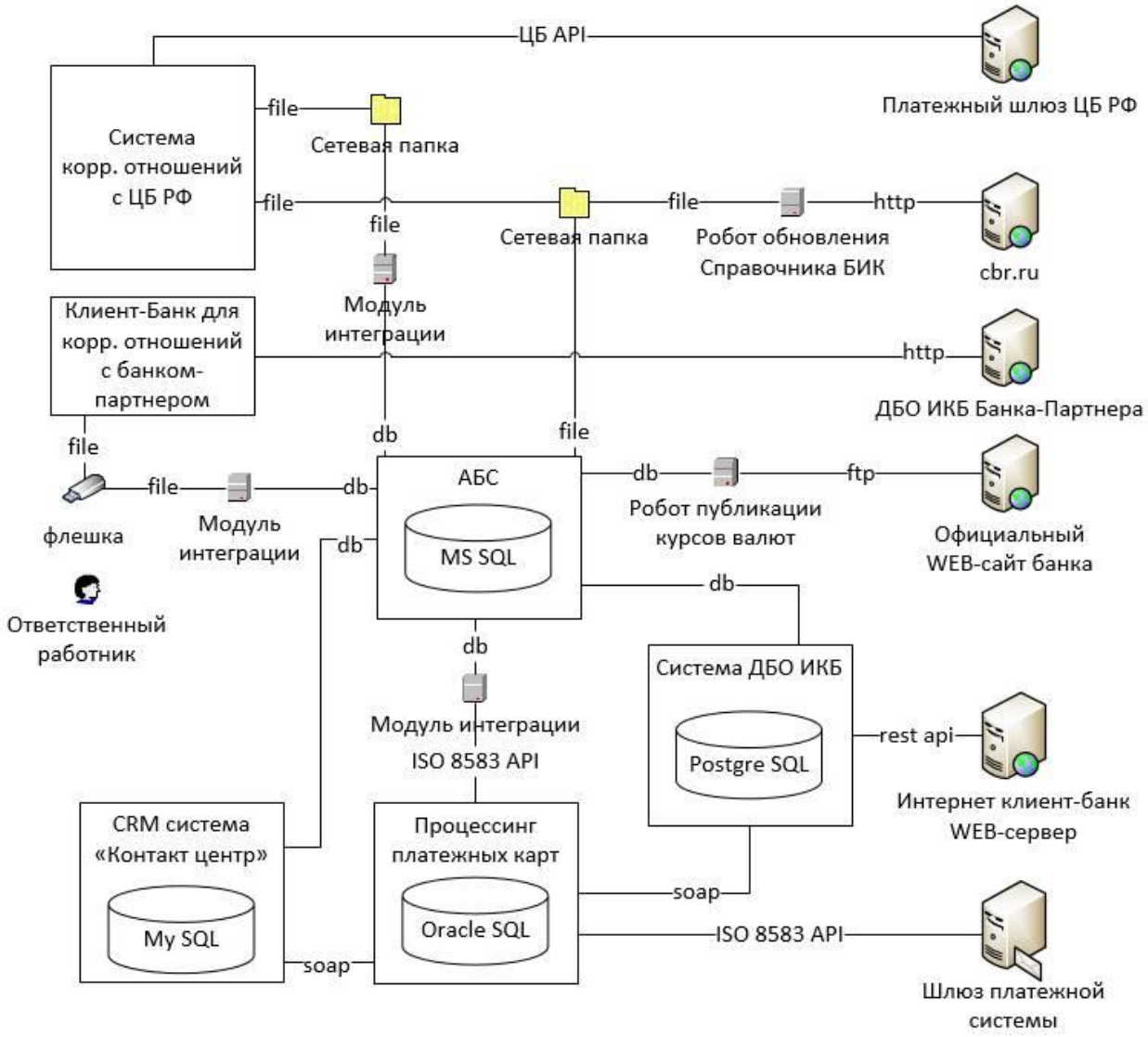

Рис. 1.

В первой части нашего исследования мы рассмотрели работу системы банковских безналичных платежей с экономической точки зрения. Теперь настало время посмотреть на внутреннее устройство ИТ-инфраструктуры банка, с помощью которой эти платежи реализуются.

Disclaimer

Статья не содержит конфиденциальной информации. Все использованные материалы публично доступны в Интернете, в том числе на сайте Банка России.

Глава 1. Общее описание ИТ-инфраструктуры

Основные термины

В 90-х годах прошлого века в ГОСТах и нормативных документах ФСТЭК России (тогда еще Гостехкомиссии при Президенте РФ) часто употреблялся термин — **автоматизированная система**. «ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» дает следующее определение данного термина:

автоматизированная система; АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Спустя некоторое время, в обиход вошел новый термин — **информационная система**. В п.3 ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» данный термин определяется следующим образом:

информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

В рамках данного исследования оба термина будут использоваться как синонимы.

Справедливость подобного подхода можно доказать тем, что в Приказе ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для защиты **информационных систем** госрегулятор предписывает руководствоваться ГОСТами по **автоматизированным системам**.

Помимо **информационных систем** в IT-инфраструктуре банка можно выделить еще один тип элементов — **информационные сервисы**, или, как их часто называют, роботы.

Дать определение понятию **информационный сервис** довольно сложно, поэтому просто перечислим его основные отличия от **информационной системы**:

1. **Информационный сервис** гораздо проще **информационной системы**, но в тоже время его нельзя назвать компонентом последней, поскольку результатами его работы могут пользоваться одновременно несколько **информационных систем**.
2. **Информационные сервисы** предназначены для автоматизации простых, рутинных задач.
3. **Информационные сервисы** не содержат в своем составе базы данных.
4. **Информационные сервисы** работают в автоматическом режиме без участия (или с минимальным участием) человека.

Автоматизированная банковская система

Ядром информационной инфраструктуры любого банка является **автоматизированная банковская система** или сокращенно **АБС**.

Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» определяет **АБС** следующим образом: автоматизированная система, реализующая банковский технологический процесс.

Данное определение позволяет подвести под него практически любую IT-систему в банке. В то же время обычные банковские служащие называют **АБС** ту систему, которая занимается учетом банковских счетов, проводок между ними (движением денежных средств) и остатков. Второе определение не противоречит первому и более четко его детализирует, им и будем пользоваться дальше.

В современных Российских банках наиболее распространенными являются следующие **АБС**:

- Diasoft FA#,
- Инверсия XXI век,
- RS-Bank,
- ЦФТ-Банк.

Некоторые, особо большие банки используют не тиражные, а специально разработанные под них **АБС**. Но подобные случаи единичны, собственно как и особо большие банки.

Иногда в банках параллельно используют несколько **АБС** различных производителей. Зачастую это происходит, когда банк пытается перейти с одной **АБС** на другую, но возможны и менее тривиальные причины.

Прикладные информационные системы

Несмотря на то что **АБС** автоматизирует довольно большое количество задач, она не покрывает все нужды банка. Есть задачи, которые **АБС** не делает вообще или делает не так, как хочет того банк. Поэтому к **АБС** подключаются (интегрируются) другие информационные системы, автоматизирующие отдельные бизнес-процессы. В дальнейшем подобные информационные системы будем называть — **прикладными информационными системами**.

Примерами **прикладных информационных систем** могут быть:

- системы дистанционного банковского обслуживания Интернет Клиент-Банк (**ДБО ИКБ**, например, iBank2, BS-Client, InterBank),
- процессинг платежных карт (например, TranzWare, SmartVista, Way4),
- системы автоматизации контакт-центров (например, Avaya Call Center, Cisco Unified Contact Center),
- системы автоматического скоринга заемщиков (например, FICO),
- и др.

В зависимости от размеров банка и оказываемых им услуг количество **прикладных информационных систем** может измеряться количеством от единиц до сотен.

Инфраструктурные информационные системы

Помимо **АБС** и **прикладных информационных систем**, автоматизирующих основные бизнес-процессы, в банках также присутствует приличное количество вспомогательных **инфраструктурных информационных систем**. Примерами подобных систем могу быть:

- служба каталогов Active Directory,
- служба доменных имен (DNS),
- корпоративная электронная почта,
- службы предоставления доступа работников в Интернет;
- системы контроля и управления доступом (СКУД) в помещения;
- IP-видеонаблюдение;
- IP-телефония;
- и многое другое.

Информационные сервисы

В банках используется гигантское количество различных **информационных сервисов**, выполняющих простые, рутинные функции, например, загрузка справочников БИК и ФИАС, публикация курсов валют на официальном сайте и т.д.

Клиентские части сторонних информационных систем

Отдельного упоминания стоят клиентские части внешних по отношению к банку **информационных систем**. В качестве примеров приведу:

- модули интеграции с государственными информационными системами: ГИС ГМП, ГИС ЖКХ;
- клиентские части внешних платежных систем;
- биржевые торговые терминалы;
- и так далее.

Типовые способы интеграции информационных систем

Для интеграции **информационных систем** обычно применяются следующие механизмы:

1. Интеграция через API (например, Web-сервисы).
2. Интеграция через СУБД:
   - путем предоставления доступа только к хранимым процедурам;
   - путем предоставления доступа к хранимым процедурам и таблицам баз данных.
3. Файловый обмен:
   - через компьютерную сеть;
   - через отчуждаемые машинные носители информации (ОМНИ, например – флешки).
4. Реализация сервис ориентированной архитектуры (SoA).

Модули интеграции

Под модулем интеграции будем понимать виртуальный элемент IT-инфраструктуры, реализующий интеграцию других элементов IT-инфраструктуры.

Данный элемент мы назвали виртуальным, потому что его функционал может быть реализован, как в виде отдельного специализированного элемента ИТ-инфраструктуры (например**, информационного сервиса**), так и в виде компонентов интегрируемых **информационных систем**. Более того, в качестве модуля интеграции может выступать даже человек, «вручную» переносящий информацию между интегрируемыми **информационными системами**.

Пример ИТ-инфраструктуры банка

На Рис.1 можно увидеть фрагмент типовой информационной инфраструктуры банка, содержащий рассмотренные выше типы элементов.

Глава 2. Инфраструктура безналичных расчетов

Если посмотреть на эту схему (Рис.1) с точки зрения осуществления безналичных расчетов, то можно увидеть, что банк реализует их при помощи:

- прямых корреспондентских отношений с банком-партнером,
- международной платежной системы (МПС) (например, VISA, MasterCard).
- корреспондентских отношений с Банком России.

Технически прямые корреспондентские отношения с банками-партнерами могут быть организованы с помощью:

- обычных систем **ДБО ИКБ**, применяемых банками для обслуживания юридических лиц (в рассматриваемом примере (Рис.1) используется именно этот способ);
- межбанковских платежных систем (например, SWIFT);
- специализированных систем обмена платежными сообщениями (например, REX400, TELEX);
- специализированного ПО, разработанного одним из взаимодействующих банков.

Подключение к платежным системам, обслуживающим пластиковые карты, осуществляется через стандартные модули, входящие в состав процессинговых систем.

Для успешного функционирования банк обязан обеспечивать у себя информационную безопасность всех перечисленных способов осуществления платежей. Рассмотреть их в рамках одного, даже крупного исследования весьма проблематично, и поэтому мы сконцентрируемся только на одном наиболее критичном, с точки зрения возможных потерь, направлении — платежном взаимодействии банка с Банком России.

Инфраструктура обеспечения платежного взаимодействия с Банком России

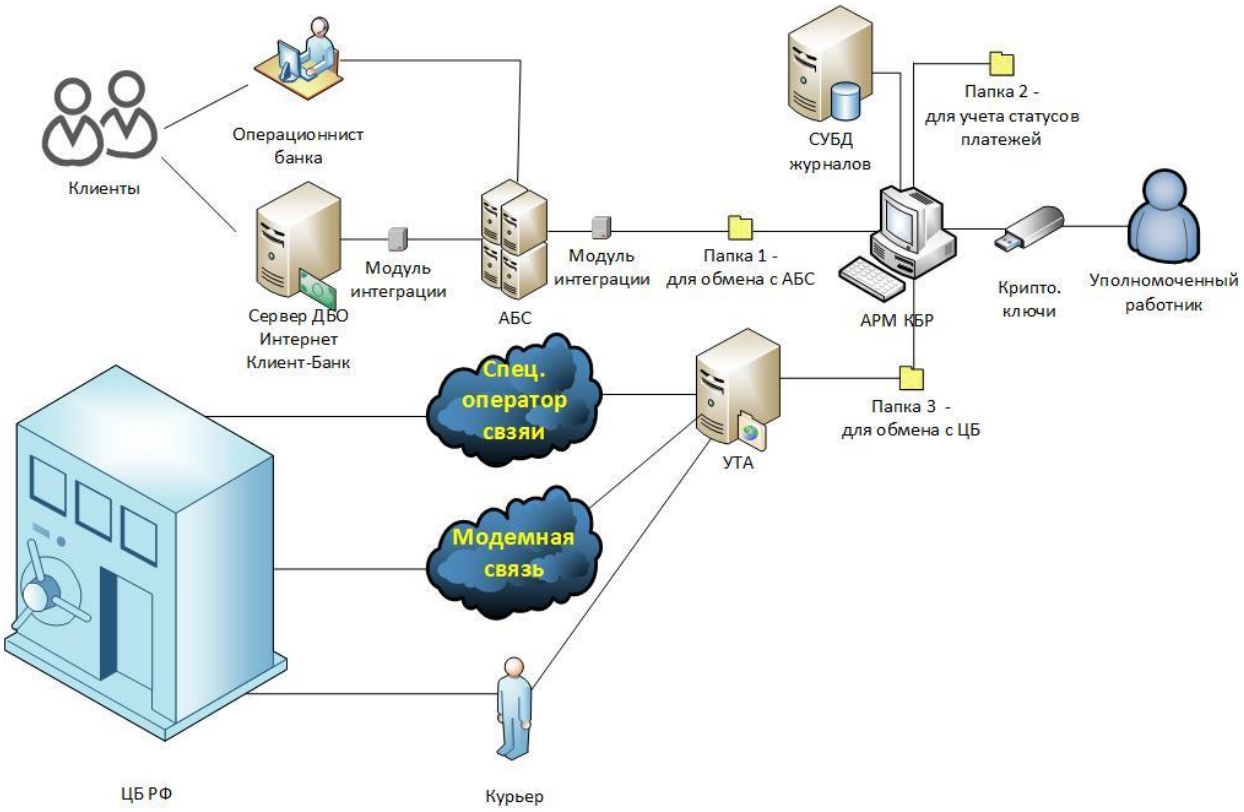

Рис. 2.

IT-инфраструктуру платежного взаимодействия банка с Банком России будем рассматривать на примере исполнения платежа, отправляемого в адрес клиента другого банка.

Как мы помним из первой части, вначале клиент должен передать в банк платежное поручение. Сделать это он может двумя способами:

1. Явиться лично в отделение банка и передать заверенное платежное распоряжение на бумажном носителе.
2. Направить платежное распоряжение через систему **ДБО ИКБ**.

Тут важно отметить, что системы **ДБО ИКБ** — это лишь системы, обеспечивающие юридически значимый электронный документооборот между клиентом и банком, самостоятельно они платежи не проводят. Именно поэтому, когда клиент открывает расчетный счет в банке, он обычно заключает два договора. Первый – договор обслуживания банковского счета, второй – договор на осуществление электронного документооборота с помощью системы **ДБО ИКБ**. Если второй договор заключен не будет, то клиент все равно сможет пользоваться своим счетом, но только при личном визите в отделение банка.

Если клиент передал платежное поручение на бумажном носителе, то работник банка на его основании делает электронное платежное поручение в **АБС**. Если распоряжение было подано через **ДБО ИКБ**, то через модуль интеграции оно попадает в **АБС** автоматически.

Доказательством того, что именно клиент сделал распоряжение о переводе денежных средств, в первом случае является лично подписанный им бумажный документ, а во втором, электронный документ в **ДБО ИКБ**, заверенный в соответствии с договором.

Обычно для заверения электронных документов клиентов — юридических лиц в **ДБО ИКБ** применяют криптографическую электронную подпись, а для документов клиентов — физических лиц коды SMS-подтверждений. С юридической точки зрения для заверения электронных документов в обоих случаях банки обычно применяют правовой режим аналога собственноручной подписи (АСП).

Попав в **АБС**, платежное поручение в соответствии с внутренними регламентами банка проходит контроль и передается для исполнения в платежную систему Банка России.

Технические средства взаимодействия с платежной системой Банка России

Технические средства (программное обеспечение), используемые для взаимодействия с платежной системой Банка России могут варьироваться в зависимости от территориального учреждения Банка России, обслуживающего корр. счет банка.

Для банков, обслуживаемых в Московском регионе, применяется следующее ПО:

- **АРМ КБР** – автоматизированное рабочее место клиента Банка России;
- **УТА** – специальное программное обеспечение файлового взаимодействия клиента Банка России (универсальный транспортный адаптер);
- **СКАД Сигнатура** — средство криптографической защиты информации (СКЗИ) «Аппаратно-программный комплекс Сигнатура-клиент» версия 5, сертификаты ФСБ России – СФ/114-2680 (уровень криптозащиты КС1), для уровня криптозащиты КС2 – СФ/124-2681 (уровень криптозащиты КС2). СКАД расшифровывается как система криптографической аутентификации документов.

АРМ КБР

АРМ КБР – это ПО, с помощью которого уполномоченные работники банка осуществляют шифрование и электронную подпись исходящих платежных документов, а также расшифровку и проверку электронной подписи платежных документов,

поступающих из Банка России. Но, если быть более точным, то **АРМ КБР** в своей работе оперирует не платежными документами, а электронными сообщениями (ЭС), которые бывают двух типов:

- электронные платежные сообщения (ЭПС), например, ED101 «Платежное поручение»;
- электронные служебно-информационные сообщения (ЭСИС), например, ED201 «Извещение о результатах контроля ЭС».

Перечень и форматы электронных сообщений устанавливает Банк России, путем выпуска Альбома унифицированных форматов электронных банковских сообщений (УФЭБС).

Для того чтобы **АРМ КБР** мог обработать платеж, он должен быть преобразован в файл, содержащий электронное платежное сообщение формата УФЭБС. За подобное преобразование отвечает модуль интеграции **АБС** с платежной системой Банка России. С технической точки зрения подобные преобразования довольно просты, поскольку формат УФЭБС основан на XML.

Файлы электронных сообщений покидают модуль интеграции **АБС** в открытом виде и помещаются в специальную папку файловой системы (обычно это сетевая папка), которая настроена в **АРМ КБР** для электронных сообщений, имеющих статус «Введенные». На ранее представленной схеме (Рис. 2.) эта папка обозначена как «Папка 1».

Затем в процессе обработки электронные сообщения меняют свои статусы на «Контролируемые», «Отправленные» и т. д., что технически реализуется путем перемещения файла с электронным сообщением в соответствующие папки, которые настроены в **АРМ КБР**. На схеме (Рис. 2.) эти папки обозначены как «Папка 2».

В определенный момент технологической обработки (установленный внутренними регламентами банка) исходящих электронных сообщений они шифруются и подписываются электронной подписью с помощью **СКАД Сигнатура** и закрытых криптографических ключей ответственных работников.

СКАД Сигнатура

СКАД Сигнатура, это СКЗИ, разработанное компанией ООО «Валидата» по заказу Банка России и предназначенное для защиты информации в платежной системе Банка России. Данного СКЗИ нет в открытом доступе (кроме документации, размещенной на

сайте ЦБ РФ), и оно распространяется Банком России только среди участников его платежной системы. К отличительным особенностям данного СКЗИ можно отнести:

1. Данное СКЗИ, в отличии от других распространенных в деловых кругах России СКЗИ (например, как Крипто-ПРО CSP, VIPNET CSP и др.), реализует собственную, изолированную от операционной системы инфраструктуру открытых ключей (PKI). Это проявляется в том, что справочник открытых ключей, содержащий сертификаты, список доверенных сертификатов, список отозванных сертификатов, и т. д. криптографически защищен на закрытом ключе пользователя, что не позволяет злоумышленнику внести в него изменения, например, установить доверенный сертификат без ведома пользователя.
Примечание. СКЗИ Верба-OW реализует схожую ключевую модель.
2. Следующая особенность вытекает из предыдущей. В СКЗИ для того, чтобы сделать рабочие ключи, необходимо сначала создать справочник сертификатов с помощью специальных ключей регистрации. По истечении срока действия рабочих ключей генерируются новые, но для того, чтобы их сгенерировать, нужно обладать действующими предыдущими рабочими ключами. Ключи создаются по децентрализованной схеме с участием Банка России в качестве Центра Сертификации.
3. СКЗИ поддерживает работу с функционально-ключевыми носителями (vdToken), выполняющими функции электронной подписи и шифрования у себя на борту, без передачи закрытых ключей в память ЭВМ.
4. Криптографические ключи, используемые для взаимодействия с платежной системой Банка России, бывают двух видов:
    - **«Только шифрование»** – позволяют зашифровывать / расшифровывать электронные сообщения.
    - **«Шифрование и подпись»** – делают то же самое, что и в первом случае, а также позволяют подписывать электронные сообщения.

УТА

Зашифрованные и подписанные электронные сообщения помещаются в специальную папку, на схеме (Рис. 2.) это «Папка 3». **УТА** непрерывно мониторит эту папку и, если он видит там новые файлы, передает их в ЦБ РФ одним из следующих способов:

- «По Интернет», хотя на самом деле это не совсем так. Вместо Интернет используется специализированный оператор связи, предоставляющий выделенные каналы связи до ЦБ РФ, но поскольку сеть IP-адресуемая то говорят, что отправка идет через Интернет.
- «По модему». На случай аварии первого вида связи есть резерв в виде модемного соединения по телефонной сети общего пользования.

- На случай выхода из строя всех каналов связи предусмотрена доставка электронных сообщений на ОМНИ (отчуждаемый машинный носитель информации) с помощью курьера. Кстати говоря, это один из способов, с помощью которого банки с отозванной лицензией проводят платежи во время своей ликвидации.

Достучавшись до ЦБ (первым или вторым способом), **УТА** передает электронные сообщения через публикуемый ЦБ API. Во время сеансов связи **УТА** также получает из **ЦБ** входные электронные сообщения.

Следует отметить, что все электронные сообщения, с которыми работает **УТА**, зашифрованы и подписаны электронной подписью.

Получив зашифрованное электронное сообщение, **УТА** перекладывает его в папку с входящими зашифрованными сообщениями. Уполномоченный работник с помощью своих криптоключей и **АРМ КБР** проверяет электронную подпись и расшифровывает сообщение.

Далее обработка производится в зависимости от типа электронного сообщения. Если это платежное сообщение, то оно через модуль интеграции передается в **АБС**, где на его основании формируются бухгалтерские проводки, изменяющие остатки на счетах. Важно отметить, что при взаимодействии **АБС** (модуля интеграции) и **АРМ КБР** используются файлы стандартного формата в открытом виде.

В процессе функционирования **АРМ КБР** ведет журнал своей работы, который может быть реализован в виде текстовых файлов или с помощью БД, работающих под управлением СУБД.

Альтернативные схемы обработки

Мы рассмотрели «классическую» схему работы системы. В реальности существует множество ее разновидностей. Рассмотрим некоторые из них.

Разновидность 1. Разделение контуров отправки и приема сообщений
Реализуется схема с двумя **АРМ КБР**. Первый работает с участием человека и выполняет только отправку сообщений, второй работает в автоматическом режиме и выполняет только прием сообщений.

Разновидность 2. Полный автомат
АРМ КБР настраивается на работу полностью в автоматическом режиме без участия человека

Разновидность 3. Изолированный АРМ КБР

АРМ КБР функционирует как выделенный компьютер, не подключенный к сети банка. Электронные сообщения передаются на него человеком-оператором с помощью ОМНИ.

Перенос электронной подписи из АРМ КБР в АБС

Банк России планирует перейти на новую технологическую схему обработки платежей, при которой электронные сообщения будут подписываться не в **АРМ КБР**, как было ранее, а в **АБС** (точнее в модуле интеграции **АБС — АРМ КБР**).

Для реализации данного подхода выпущена новая версия **АРМ КБР**, которая стала называться **АРМ КБР-Н** (новая). Все основные изменения можно увидеть, если сравнить схемы информационных потоков, проходящих через **АРМ КБР** старой и новой версии.

Рассмотрим схему информационных потоков в классическом АРМ КБР. Источник схемы – официальная документация на АРМ КБР «АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО КЛИЕНТА БАНКА РОССИИ. Руководство программиста. ЦБРФ.61209-04 33 01».

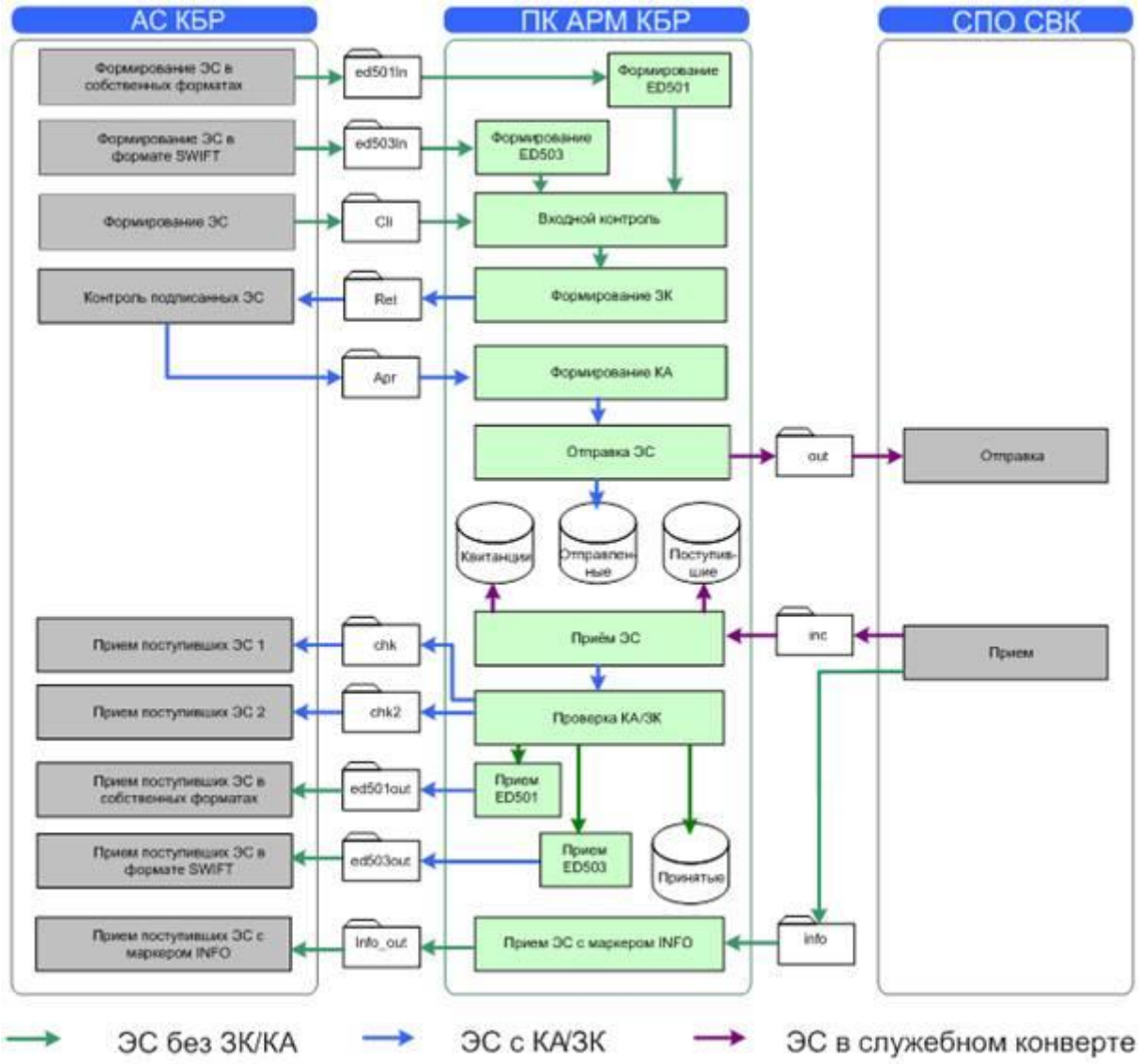

Рис. 3.

Примечания.

- *Условное обозначение «АС КБР» (автоматизированная система клиента Банка России) соответствует условному обозначению **АБС** на предыдущих схемах.*
- *Условное обозначение «СПО СВК» соответствует условному обозначению **УТА** на предыдущих схемах.*
- *КА – код аутентификации (электронная подпись) электронного сообщения.*
- *ЗК – защитный код еще один вид электронной подписи, но в отличии от КА, который формируется исходным сообщением без изменений, ЗК формируется только под значащими данными без учета разметки. Более подробно о технических нюансах КА и ЗК можно почитать в документации УФЭБС «Защита электронных сообщений (Пакетов ЭС)». С юридической точки зрения ЗК – технологическая мера защиты информации, в то время как КА, согласно договорам и правилам платежной системы Банка России, признается электронной подписью.*

Теперь взглянем на аналогичную схему для нового АРМ КБР-Н. Источник «АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО КЛИЕНТА БАНКА РОССИИ НОВОЕ. Руководство программиста. ЦБРФ.61289-01 33 01»

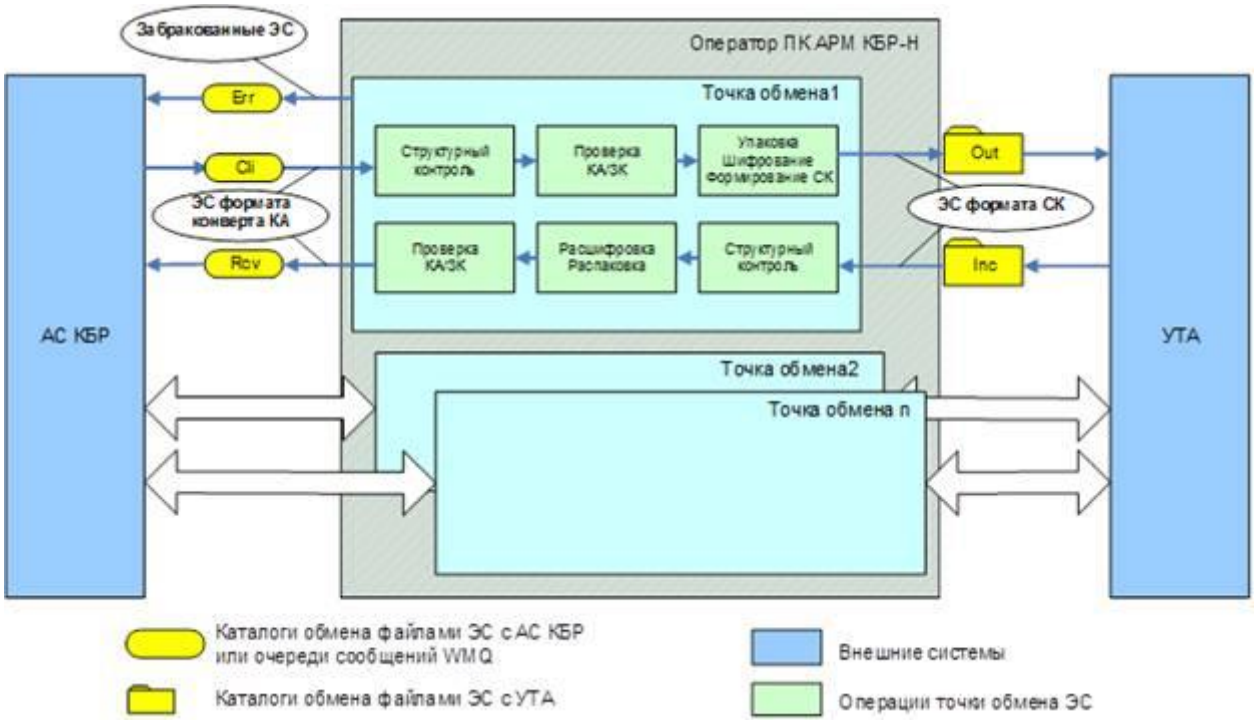

Рис. 4.

С точки зрения криптографии **АРМ КБР-Н** отвечает за шифрование / расшифрование электронных сообщений, а также за проверку электронных подписей на них. Формирование электронных подписей перенесено в модуль интеграции **АБС**.

Логично предположить, что данный модуль также должен будет проверять подписи под сообщениями, полученными из **АРМ КБР-Н**. С технической точки зрения это не является обязательным, но с точки зрения обеспечения безопасности имеет критическое значение, поскольку обеспечивает целостность сообщений, передаваемых между **АБС** и **АРМ КБР-Н**.

Помимо файлового интерфейса взаимодействия между **АБС**, **АРМ КБР-Н** и **УТА** добавлен интерфейс IBM WebSphere MQ, что позволяет строить сервис-ориентированную ИТ-инфраструктуру банка и решить проблему старой схемы с организацией одновременной работы нескольких операторов, ответственных за отправку платежей.

Заключение

Мы рассмотрели внутреннее устройство платежной ИТ-инфраструктуры банка. В следующих частях рассмотрим угрозы информационной безопасности, которые здесь возникают.