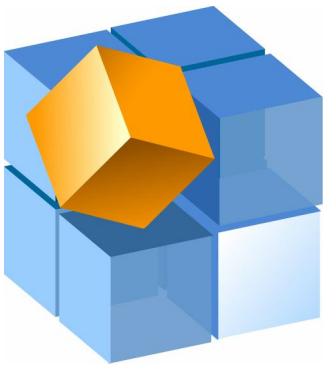
# СИСТЕМА АВТОМАТИЗАЦИИ ОНЛАЙНОВОГО ПРОЦЕССИНГОВОГО ЦЕНТРА



## Оглавление

# 1. ПРОЦЕССИНГОВЫЙ ЦЕНТР.

## 1.1. БЭК-ОФИС.

Система предназначена для использования**:**

• Банками – членами платежных систем VISA, MasterCard, Union Card, China Union Pay и д.р. решающими задачи:

- эмиссии платежных карт и обработки транзакций по эмитированным картам;
- эквайеринга карточных транзакций;
- работы с банками-агентами (субэмитентами и субэквайерами) участвующими в платежных системах от имени банка-спонсора.

• Банками, желающими эмитировать и обслуживать свои собственные карты, а также банками, желающими создать свою собственную (локальную) платежную систему;

• Процессинговыми центрами, осуществляющими обслуживание нескольких банков.

При этом система обеспечивает работу системы внутреннего учета, клиринга и расчетов, т.е. оффлайновой части технологического цикла работы, реализуемой в бэкофисах:

• эквайера,

• эмитента,

• эквайера-спонсора и эмитента-спонсора,

• расчетно-авторизационного центра (как главного РАЦ платежной системы, так и прочих РАЦ),

• стороннего процессора (сервис-центра) эквайера и эмитента.

Система обеспечивает весь набор стандартных работ операционного дня участника каждой обслуживаемой платежной системы:

• *регистрацию* обслуживаемых им участников и расчетных центров платежных систем, а также участников и расчетных центров, с которыми производится обмен сообщениями

• *прием, анализ и обработку* финансовых и прочих *сообщений*, приходящих в составе входящих (Incoming) клиринговых файлов из расчетно-клиринговых центров платежных систем в их форматах (ECCF, Base II, Union Card), корректно формируя отказы в обработке (Rejects) и исправленные сообщения (Post-Rejections) по правилам конкретной платежной системы;

• *формирование финансовых сообщений* (включая сообщения претензионного цикла - Chargebacks, Retrieval Requests/Responses, Second Presentments) в ручном либо пакетном режимах и их отсылку в составе исходящих (Outgoing) клиринговых файлов в расчетно-клиринговые центры платежных систем в соответствующих форматах. При формировании финансовых сообщений существует возможность *сверки параметров финансовых сообщений с авторизационными сообщениями*, выгруженными в систему бэкофиса из центра авторизации участника;

• *процессинг финансовых сообщений* от всех обслуживаемых платежных систем и ведение учета по ним на основе единой схемы;

• *расчет итоговой финансовой позиции* участника. При этом, если система установлена в расчетно-клиринговом центре, среди обслуживаемых им участников производится взаимный зачет требований/обязательств, причем возможны специальные схемы расчетов для конкретных пар участников по установленным для них индивидуальным ставкам комиссий;

• *формирование проводок по счетам* для банковской системы каждого участника по итогам процессинга транзакций. Проводки могут формироваться для расчетов с любыми объектами, участвовавшими в осуществлении карточной операции: держателями карт, торговыми фирмами, платежными системами, процессинговым центром и т.д. Помимо этого, могут автоматически генерироваться проводки, связанные с внутренним учетом банка:

проводки по счетам невыясненных сумм, счетам отложенных платежей, конверсионным, транзитным и прочим счетам в соответствии с настраиваемой схемой аналитического учета. Проводки могут выгружаться в файл проводок и других расчетных документов (поручений на конвертацию, платежных поручений для расчетов с торговыми фирмами и пр.) для экспорта в банковскую систему участника;

• *расчет суммарных оборотов по счетам*;

• *формирование инструкций* по переводу средств (Funds Transfer) *для* одного или нескольких *расчетных банков*;

• *выдача требуемой справочной информации* для обслуживаемых участников и расчетных центров в виде отчетов;

• *взаимодействие с авторизационными центрами* обслуживаемых участников и расчетных центров.

Система позволяет банку-участнику разрабатывать *свои собственные карточные проекты* для фирм-мерчантов и держателей карт на основе гибко настраиваемых схем комиссий и прочих параметров. При обслуживании ***эквайера*** в системе внутреннего учета, клиринга и расчетов выполняются все действия, необходимые для обслуживания *фирм-мерчантов.* Для ***эмитента*** система обеспечивает все необходимые действия по обслуживанию *держателей карточек*, при этом позволяет работать как с *дебетовыми*, так и с *кредитными* картами.

Для эмитентов, обслуживающих *организации* (например, по зарплатным проектам), предусмотрены *групповые операции*, позволяющие производить *массовые начисления и удержания* по карточным счетам на основе единой схемы, а также массовую выдачу карт. Для крупных банков-эмитентов предусмотрена возможность работы с филиалами банка *на основе единой карточной базы данных*

Система обеспечивает *подготовку данных для персонализации карточек* (в том числе микропроцессорных) по задаваемым эмитентом параметрам и в соответствии с требованиями платежных систем.

При обслуживании ***расчетного центра*** система , помимо стандартных действий по расчету позиций участников платежной системы, обеспечивает *контроль лимитов авторизаций обслуживаемых участников* по гибко настраиваемой схеме, что позволяет предотвратить возникновение неплатежей в платежной системе.

Специалисты нашей компании ведут постоянные доработки по развитию системы . Ниже приведен краткий перечень функциональностей:

**1.** Функциональность зарплатный проект. Данная функциональность решает следующие задачи:

- заявка на открытие счетов и изготовление карт, конвертация и прием исходного файла от клиентской организации;
- создание ответного файла протокола;
- ввод реестра платежных документов;
- создание ответного файла – протокола;
- работа с реестрами платежных документов;
- получение платежных поручений от АБС банка;
- назначение на расчет реестров платежных документов;
- расчет реестров платежных документов;
- отправка в АБС результатов обработки реестров;
- создание справок и отчетов по реестрам платежных документов и связанных с ними платежным поручениям.

**2.** Кредитные карты:

- револьверные;
- кредитные линии.
- использование GRACE-периода;
- автоматическое распределение резервов по ПОС (портфелям однородных ссуд);
- автоматическое распределение резервов по ПОТ (портфелям однородных требований).

**3.** При обслуживании договоров пластиковых карт можно осуществлять дополнительный контроль. Данный контроль осуществляется автоматически по настроенной маске где выбираются несколько критериев поиска клиентов по
Стоп – листам. Критерии поиска могут настраиваться для каждого заведенного в систему Стоп - листа:

- проверка клиентов по Стоп - листам предоставленных КФМ;
- проверка клиентов по Стоп - листам банка;

Проверка осуществляются при заведении отдельных договоров операционистом и при регистрации договоров через прием файлов на открытие новых.

**4.** Взаимодействие с НБКИ (национальным бюро кредитных историй).

- при получении согласия клиента по всем его кредитным договорам может осуществляться выгрузка в НБКИ;
- выгрузка осуществляется в XML – формате;
- используется стандартная операция для выгрузки файлов с последующей конвертацией.

**5.** Длительные поручения.

- в системе может быть зарегистрировано множество типовых длительных поручений;
- после выбора клиентом определенного длительного поручения оно привязывается к клиентскому договору;
- по одному клиентскому договору может быть зарегистрировано множество длительных поручений, поэтому каждому поручению заполняется категория выполнения, т.е. очередность и условия выполнения;
- при редактировании уже настроенных длительных поручений возможно редактирование следующих параметров, состояние, вид коммунального платежа, дата регистрации, дата начала действия, дата окончания действия, приоритет и условие выполнения.

**Примечание**: Все вышеперечисленные операции и виды карточных договоров имеют возможность тонкой настройки под требования банка, например:

- индивидуальные счета (резидент, не резидент, валюта, схемы начисления процентов, сроки начисления и выплаты процентов, и т.д.);
- метод кредитования;
- лимит выдачи;
- категория качества ссуды;
- счет для учета ссудной задолженности;
- счет для учета просроченной ссудной задолженности;
- параметры графика погашения;
- начало отсчета периода фиксации ссудной задолженности;
- период фиксации;
- день фиксации ссудной задолженности;
- период запрета погашения ссуды;
- начало отсчета периода погашения;
- такие же настройки могут осуществляться и для процентной составляющей договоров;
- также существуют настройки для погашения задолженностей, здесь можно выбрать тип задолженности и определить порядок, в котором данные задолженности будут гаситься при наличии средств на основном счете клиента.

Это только основные настройки, имея на вооружении такой мощный и имеющий большие возможности комплекс, как банк получает значительные преимущества
по обслуживанию клиентов, что позволяет использовать и внедрять разнообразные бизнес – процессы, продиктованные временем и потребностями банка и соответственно привлекать большее число клиентов.

## 1.2. ФРОНТ-ОФИС

По сравнению с аналогичными разработками конкурентов система автоматизации онлайнового процессингового центра имеет ряд неоспоримых преимуществ, делающих ее уникальным программным решением, наилучшим образом отвечающим запросам современного, динамично развивающегося банка:

1. В системе реализованы ***интерфейсы со всеми*** отечественными и зарубежными ***платежными системами***, представленными на территории России;

2. В системе реализованы ***интерфейсы со всеми*** важнейшими ***онлайновыми процессинговыми системами***, используемыми банками, и процессинговыми центрами на территории России (Base24, MCI, SmartVista, OpenWay, Compas+);

3. В состав подсистемы управления банкоматами кроме классического хоста входит ***редактор/отладчик сценария***. Редактор сценария позволяет с помощью удобного графического интерфейса создавать или модифицировать сценарий NDC, а отладчик сценария позволяет отлаживать созданный/модифицированный сценарий банкомата без банкомата, банкоматного хоста и системы авторизации.

4. ***Подсистема управления терминалами*** максимально простым способом подключает к процессинговому центру терминальное оборудование и рабочие места сторонних производителей для выполнения широчайшего спектра дебетовых, кредитовых и информационных операций с использованием пластиковых карт;

5. ***Подсистема мониторинга*** помогает гибко настраивать контроль именно тех, происходящих на терминалах событий, которые представляют интерес для контроля;

6. ***SMS–сервис*** позволяет моментально информировать держателей карт об операциях, совершенных по их картам. Множество операций, по которым происходит SMS-информирование, определяется самим держателем карты;

7. Модуль удаленного доступа к системе обслуживания физических лиц позволяет выполнять на терминалах банковские операции широчайшего спектра (открытие счетов, закрытие счетов, пополнение счетов, списание со счетов, погашение задолженности по кредиту, просмотр банковской выписки и т.д.). Таким образом, система становится составной частью ***Персонального Банковского Сервиса*** (ПБС).

Система автоматизации онлайнового процессингового центра предназначена для автоматизации процессов обмена и обработки авторизационных сообщений, связанных с обслуживанием пластиковых карт, в режиме реального времени. Система может осуществлять поддержание авторизационного процесса для одного или нескольких участников платежных систем, выступающих в роли эквайеров, эмитентов, а также межбанковских расчетно-авторизационных центров.

Основные компоненты системы отображены на рисунке 1.

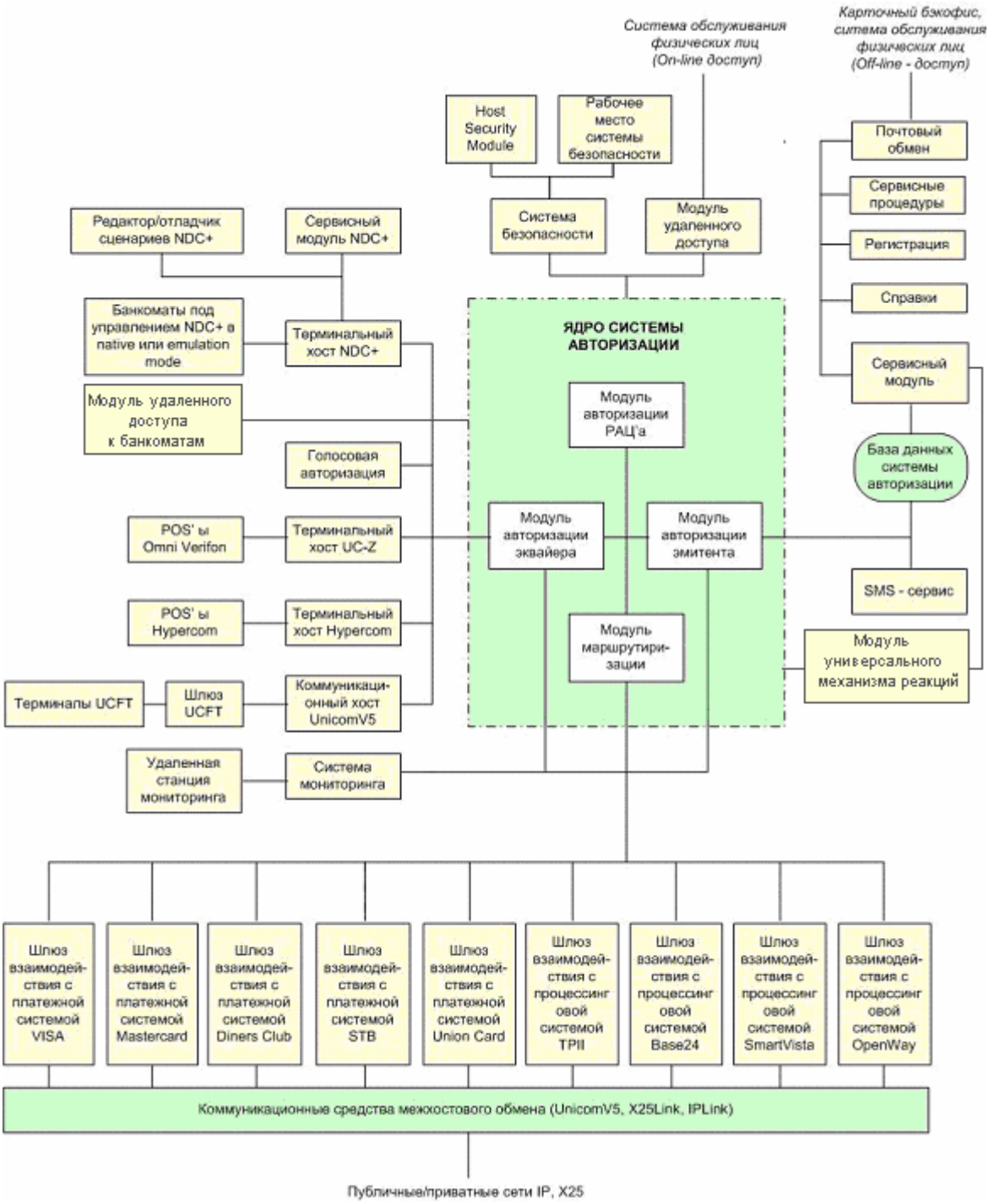



**Рис. 1. Основные компоненты 3Card-F**

### 1.2.1. ФУНКЦИОНАЛЬНЫЕ СОСТАВЛЯЮЩИЕ СИСТЕМЫ

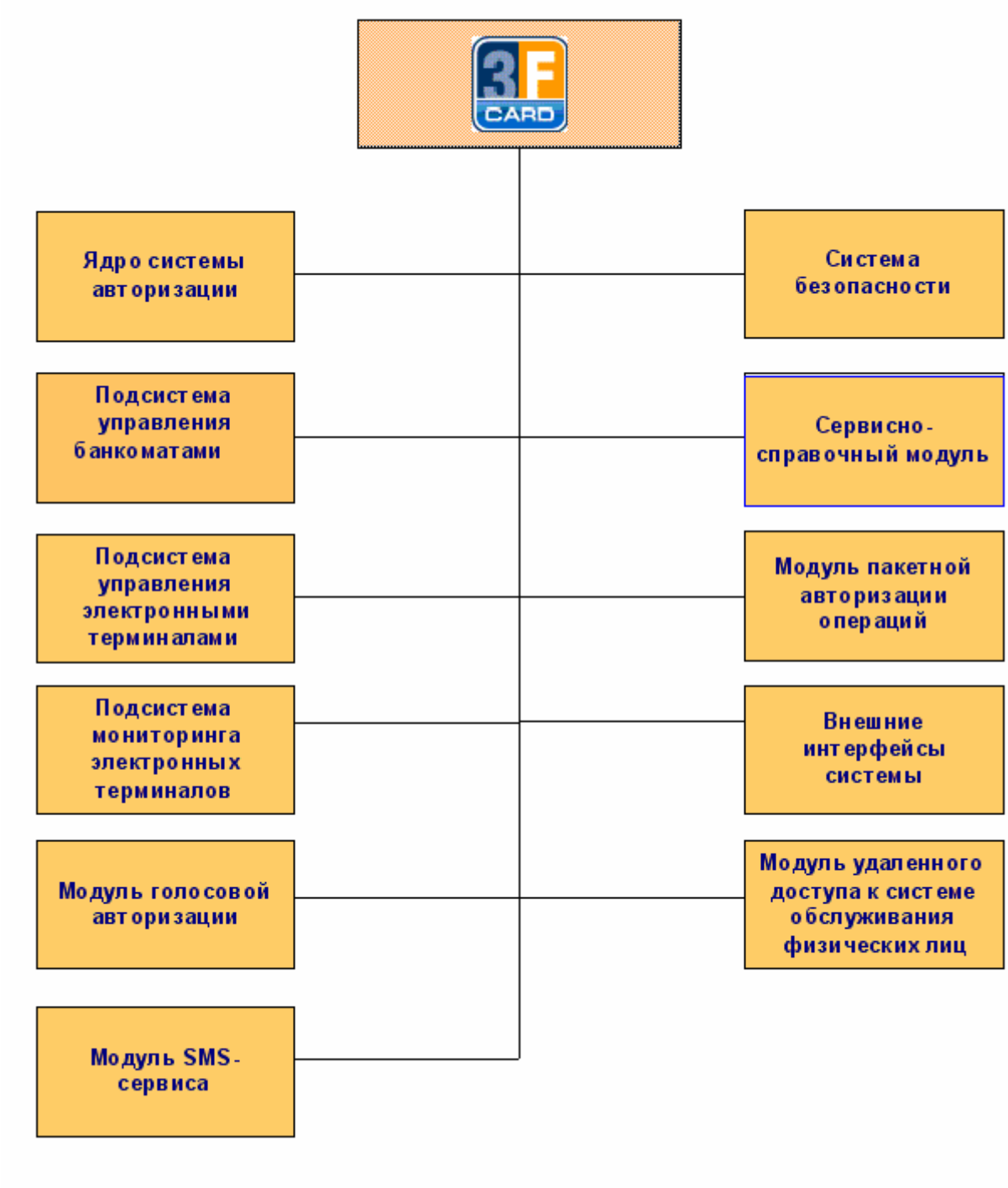



**Рис. 2. Функциональные составляющие системы.**

Он-лайновый процессинговый центр обладает значительным набором различных функционалов; важнейшие из них изображены схематично на рисунке 2:

- Ядро системы авторизации;
- Подсистема управления банкоматами;
- Подсистема управления электронными терминалами;

- Подсистема мониторинга электронных терминалов;
- Модуль голосовой авторизации;
- Модуль SMS-сервиса;
- Система безопасности:
  - Сервер безопасности;
  - АРМ администратора системы безопасности;
- Сервисно-справочный модуль;
- Модуль пакетной авторизации операций;
- Внешние интерфейсы системы:
  - Шлюзы для взаимодействия с платежными системами;
  - Интерфейс для взаимодействия в рамках локальной платежной системы;
  - Интерфейсы с авторизационными комплексами сторонних разработчиков;
  - Интерфейс с бэк-офисными системами обслуживаемых банков;
- Модуль удаленного доступа к системе обслуживания физических лиц (см. ПБС).

### 1.2.2. ЯДРО СИСТЕМЫ АВТОРИЗАЦИИ

Ядро системы авторизации является важнейшим функционалом, обеспечивающим базовую логику обработки транзакций в ходе авторизационного процесса для эквайера, эмитента и расчетно-авторизационного центра. В состав этой базовой логики в зависимости от конфигурации системы может входить:

- формирование авторизационных сообщений;
- маршрутизация авторизационных сообщений;
- обработка авторизационных сообщений – выполнение контрольных проверок, необходимых для эквайера, эмитента и расчетно-авторизационного центра;
- фиксирование результата завершения транзакции в базе данных.

Ядро системы авторизации имеет стандартизованные внешние интерфейсы:

a) Интерфейс с подсистемами управления терминалами и голосовой авторизации;
b) Интерфейс с сетями платежных систем;
c) Интерфейс, обеспечивающий взаимодействие с системой безопасности;
d) SOAP-взаимодействие с системой.

***Интерфейс с подсистемами управления терминалами и подсистемой голосовой авторизации*** построен на основе стандарта ISO-8583 и позволяет подключать к ядру различные подсистемы управления терминалами без изменения базовых функций ядра системы авторизации.

***Интерфейс с сетями платежных систем*** и внешними системами авторизации реализован в соответствии со стандартом ISO-8583. Сообщения, передаваемые в рамках этого интерфейса, содержат полный набор параметров, необходимых для реализации

взаимодействия с внешними системами с использованием протоколов платежных систем: VISA BaseI/SMS, EPS-Net v.5 и других; протоколов сторонних процессинговых систем: OpenWay, Base24, SmartVista и др.

***Интерфейс, обеспечивающий взаимодействие с системой безопасности***, позволяет реализовывать обращения к базовым функциям обеспечения безопасности (трансляция PIN-блока, верификация PIN-блока, верификация MAC'а, формирование MAC'а, шифрование/дешифрование сообщений, генерация и распределение криптографических ключей). Интерфейс поддерживает основные криптографические алгоритмы и соответствует требованиям международных платежных систем по безопасности.

***SOAP-взаимодействие с системой 3CardF,*** реализовано на основе XML протокола, расширяет возможности ядра системы авторизации, по обработке авторизационных сообщений, SMS информированию, изменению лимитов карты и др.


**Рис. 3. Ядро системы авторизации 3Card-F**

В состав ядра входят следующие компоненты:

---

***Обработчик транзакций эквайера*** является компонентой ядра системы авторизации, предназначенной для использования в авторизационном процессинговом центре, реализующем функции эквайера. Обработчик транзакций эквайера обеспечивает выполнение следующих функций:

- Прием сообщений-запросов о совершаемых карточных операциях от подсистем управления терминалами. В целях защиты целостности информации и противодействия возможному мошенничеству сообщения, передаваемые между терминалами и центром авторизации, защищаются контрольным кодом (MAC);
- Контрольные проверки по условиям, заданным для эквайеров, терминалов, филиалов и фирм; Контрольные проверки по таблице БИНов;

- Формирование авторизационных сообщений в формате ISO-8583 для дальнейшей обработки в системе;
- Формирование отказных сообщений для систем управления терминалами;
- Фиксирование в базе данных результатов обработки сообщений;
- Маршрутизация (после получения ответа со стороны эмитента) ответного сообщения подсистемам управления терминалами, от которых получено сообщение–запрос по карточной операции.

---

***Обработчик транзакций эмитента*** является компонентой ядра подсистемы авторизации, предназначенной для использования в авторизационном процессинговом центре эмитента. Обработчик транзакций эмитента непосредственно обеспечивает процесс авторизации карточных транзакций и выполнение следующих функций:

- Проверка параметров безопасности транзакции (PIN, коды CVC\CVV); Контрольные проверки по условиям, заданным для карт. Например, контролируется лимит авторизаций держателя карт (Open-To-Buy Limit), лимиты активности карты по сумме, по типу операции и по частоте использования, коды CVC\CVV и прочие параметры, используемые для контроля платежеспособности держателя, ограничения использования карты и противодействия возможному мошенничеству;
- Фиксирование в базе данных результатов обработки транзакции со стороны эмитента и формирование ответного сообщения.

---

***Обработчик транзакций расчетно-авторизационного центра*** является компонентой ядра системы авторизации, предназначенной для использования в авторизационном процессинговом центре, реализующем функции межбанковского маршрутизатора сообщений. Обработчик обеспечивает выполнение следующих функций:

- Маршрутизация авторизационных сообщений между центрами авторизаций эквайеров и эмитентов;
- Контрольные проверки по условиям, заданным для обслуживаемых эквайеров и эмитентов (в том числе контроль лимитов авторизации, установленных для эмитентов), формирование отказного ответного сообщения при неудовлетворительном результате проверок;
- Определение некоторых параметров сообщений-запросов авторизации перед направлением этих сообщений эмитенту (например, определение валюты карты и конвертация суммы операции в валюту карты);
- Фиксирование в базе данных результатов завершения обработки транзакции.

---

***Внутренний маршрутизатор*** – обязательная компонента ядра, обеспечивающая маршрутизацию сообщений между компонентами ядра. В функции внутреннего маршрутизатора входит:

- Анализ содержания сообщений, полученных от внутренних модулей ядра системы авторизации, и определение направления дальнейшей его маршрутизации;
- Дальнейшая маршрутизация сообщений, полученных от внешних систем посредством взаимодействия с внешним маршрутизатором;

- Трансляция PIN-блока, передаваемого в составе сообщения (если это требуется).

---

***Внешний маршрутизатор (Interchange Switch)*** – обязательная компонента ядра, обеспечивающая маршрутизация сообщений с внутренним маршрутизатором, а также по каналам взаимодействия (посредством шлюзов) с внешними системами. В функции внешнего маршрутизатора входит:

- Анализ содержания сообщений, полученных из внешних систем, и передача их во внутренний маршрутизатор;
- Взаимодействие с системой безопасности он-лайнового процессингового центра.

---

***Эмитентский и эквайерский пакеты***. В системе 3Card-F реализовано понятие «продукт», однако в базовой настройке указанный объект обладает ограниченными возможностями по настройке. Существенно расширить их позволяют новые программные функционалы системы - «эмитентский» и «эквайерский» пакеты, позволяющие установить дополнительные ограничения и комиссии на совершаемые по банковским картам операции.

В частности, в рамках «эмитентского пакета» возможно:

- Задавать тип поддерживаемой процессинговым центром операции, конфигурировать тип и принадлежность устройства (по коду эквайера). Задание этих параметров позволяет получить уникальный ключ лимита активности.
- Задавать размер комиссии для финансовых операций, устанавливать верхние и нижние пределы для суммы комиссии.
- Устанавливать ограничение на количество совершаемых держателем карты операций за период с возможностью настройки длительности самого периода.
- Устанавливать ограничение на общую сумму операций, которые держатель карты выполняет за период с возможностью настройки длительности самого периода.

Аналогичные ограничения на лимиты активности и параметры совершаемых операций можно установить и в рамках «эквайерского» пакета. Также в рамках «эквайерского» пакета поддерживается контроль лимитов активности по коду фирмы или по коду терминального устройства.

### 1.2.3. ПОДСИСТЕМА УПРАВЛЕНИЯ БАНКОМАТАМИ

Подсистема управления банкоматами обеспечивает управление банкоматами в соответствии с протоколом NDC, D912. Подсистема имеет стандартизованный интерфейс с ядром системы авторизации (интерфейс с обработчиком транзакций эквайера в составе ядра), осуществляющим обработку авторизационных запросов, подсистемой мониторинга терминалов, обеспечивающей отображение состояния (финансового и технического) банкомата (открытие, закрытие и загрузка конфигурации) и отдельных его устройств и, кроме того, осуществляющей управление банкоматами, а также модулем удаленного доступа, обеспечивающим выполнение на банкоматах коммунальных платежей и банковских функций. Редактор/отладчик сценария позволяет создавать и модифицировать сценарий NDC, и отлаживать его без использования каких-либо дополнительных средств и компонент системы авторизации.
Подсистема управления банкоматами обеспечивает работу: с банкоматами NCR, Siemens Wincor, Diebold, Hyosung; информационными киосками Siemens Wincor, ТерионМ и другими – по всем типам каналов связи. Реализует все виды расходных и вкладных операций по картам, допустимых для электронных устройств (АТМ), включая платежи без карт и переводы с карты на карту.

### 1.2.4. ПОДСИСТЕМА УПРАВЛЕНИЯ ТЕРМИНАЛАМИ



Подсистема управления терминалами включает в себя несколько коммуникационных серверов, обеспечивающих взаимодействие с терминальными устройствами по поддерживаемым каналам связи (коммутируемые телефонные линии, выделенные телефонные линии, каналы X.25, IP-каналы) и конвертеры терминальных протоколов, осуществляющие преобразование протоколов обмена с терминалами во входной протокол, соответствующий стандартизированному интерфейсу ядра системы авторизации (интерфейс с обработчиком транзакций эквайера в составе ядра). В подсистеме реализована поддержка протоколов: **Hypercom** (ISO-8583), собственного терминального протокола обмена **UC-Z**, который является модификацией протокола **VISA MDC**, а также собственного терминального протокола **UCFT**, позволяющего легко подключать к процессинговому центру терминальное оборудование, рабочие станции независимых производителей и выполнять при этом довольно большой спектр операций по банковским картам.

Подсистема управления терминалами обеспечивает обработку следующих типов транзакций:

- транзакции оплаты товаров (услуг);
- транзакции коммунальных платежей;
- транзакции выдачи наличных;
- транзакции запросов остатка;
- транзакции выписки из истории операций;
- транзакции банковского сервиса;
- транзакции внесения наличных;
- транзакции отмены операций выдачи наличных и операций оплаты товаров (услуг);
- транзакции разгрузки терминалов (Data Capture);
- транзакции мониторинга и управления, обеспечивающие получения информации о техническом и финансовом состоянии терминалов, а также обеспечивающих управление терминальными устройствами;
- технические транзакции, обеспечивающие загрузку на терминалы разнообразной информации.

Подсистема управления терминалами имеет интерфейс с подсистемой мониторинга терминалов, которая отображает текущее техническое и финансовое состояния терминалов и осуществляет управление терминалами, а также с модулем удаленного доступа, обеспечивающим выполнение на терминалах коммунальных платежей.

### 1.2.5. ПОДСИСТЕМА МОНИТОРИНГА ЭЛЕКТРОННЫХ ТЕРМИНАЛОВ

Подсистема мониторинга терминалов предназначена для оперативного контроля текущего технического и финансового состояния сети терминалов. Она позволяет отображать информацию о состоянии банкоматов, POS-терминалов и каналов связи, используемых для подключения терминального оборудования. Кроме того, система мониторинга предоставляет интерфейс управления банкоматами: открытие/закрытие банкомата, загрузка конфигурации, запрос финансового и технического статуса.

Кроме визуального отображения на экране состояния терминалов и их отдельных устройств существует возможность настройки подсистемы на обработку заданных критических событий (сбой каналов связи, переход терминалов в определенное состояние, возникновение ошибок в отдельных устройствах). Информация о фактах возникновения таких критических событий, а также информация о статусах устройств, поступающая от терминалов, может отображаться цветовым изображением на экранах мониторов, а также передаваться посредством почтовой подсистемы службам технической поддержки терминалов в обслуживаемых банках.

Подсистема мониторинга электронных терминалов включает в себя следующие компоненты:

1. ***Процессор запросов*** - модуль, обеспечивающий обмен информацией между системами управления терминалами, предоставляющими первичную информацию об их техническом и финансовом состоянии, и другими модулями мониторинга: базой данных и удаленными станциями мониторинга.

   Процессор запросов выполняет следующие функции:



- обновляет информацию в базе данных при получении соответствующих сообщений от терминальных хостов;

- осуществляет периодический просмотр содержимого базы данных на наличие управляющих команд для банкоматов и, в случае их наличия, посылает команды соответствующим терминальным хостам;

- взаимодействует с удаленными станциями мониторинга (принимает от удаленных станций команды управления терминалами, а также направляет им информацию о состоянии терминалов);

- формирует почтовые файлы с информацией о состоянии терминалов (работоспособность различных устройств терминала, наличие купюр в кассетах банкомата, наличие бумажной ленты в чековом принтере и т.п.) и посылает их по электронной почте в службы технической поддержки банков-эквайеров.

2. ***Модуль мониторинга*** - интерфейсный модуль, предоставляющий оператору следующие возможности:

- регистрация в базе данных объектов мониторинга;
- визуализация текущего состояния терминалов и каналов связи (по оперативной информации, хранящейся в базе данных);
- управление терминалами;
- регистрация операционистов, распределение прав доступа;
- формирование отчетов о состоянии терминалов.

3. ***Удаленная станция мониторинга*** - интерфейсный модуль, предназначенный для организации удаленного рабочего места оператора за пределами процессингового центра. Удаленная станция мониторинга позволяет контролировать состояние терминалов и управлять ими, предоставляя ограниченные по сравнению с модулем мониторинга возможности.

### 1.2.6. МОДУЛЬ ГОЛОСОВОЙ АВТОРИЗАЦИИ

Подсистема голосовой авторизации устанавливается на одной или нескольких станциях голосовой авторизации. Подсистема голосовой авторизации обеспечивает:

- формирование запроса авторизации посредством ручного ввода операционистом параметров карточной операции, которые передаются из пункта обслуживания банковских карт устно по телефону;

- обработку ответов на авторизационные запросы по карточным операциям и отображение результатов авторизации для устной передачи в пункт обслуживания банковских карт;

- отмена проведенных ранее авторизаций;

- ведение и возможность просмотра протокола авторизаций, обработанных на станции в текущем сеансе работы;

- получение справочной информации из базы данных о зарегистрированных пунктах обслуживания, фирмах, филиалах и терминалах, и их параметрах.

### 1.2.7. МОДУЛЬ SMS-СЕРВИСА

Модуль SMS-сервиса предназначается для информирования держателя карты о проведенных по его карте операциях (разрешенных и/или отказных) посредством направления ему SMS-сообщения с параметрами совершенных операций. По каким операциям держателю карты направляется SMS-сообщение и направляется ли оно вообще, конфигурируется для каждой карты в отдельности.



### 1.2.8. СИСТЕМА БЕЗОПАСНОСТИ

Система безопасности представляет собой программно-аппаратный комплекс, предназначенный для выполнения функций, связанных с генерацией криптографических ключей, защищенным хранением ключей, трансляцией ключей, генерацией параметров, используемых при персонализации карт (PIN, PVV, CVC/CVV), трансляцией PIN-блоков, верификацией PIN-блоков и других функций.

Система безопасности включает в себя следующие основные компоненты:

- *Сервер безопасности;*
- *Рабочее место системы безопасности*.

***Сервер безопасности*** обеспечивает выполнение всех криптографических процедур в рамках перечисленных выше функций. Он может обеспечивать работу с одним или одновременно с несколькими аппаратными модулями безопасности.

Сервер безопасности имеет стандартизованный интерфейс с внутренними компонентами ядра системы авторизации и другими прикладными подсистемами.

Все ключи, используемые в криптографических процедурах, хранятся в базе данных ключей в зашифрованном виде. Шифрование производится с помощью мастер-ключей. Мастер-ключи, хранятся внутри аппаратного модуля безопасности.

Сервер безопасности обеспечивает работу со многими существующими сегодня аппаратными модулями безопасности.

***Рабочее место (АРМ) системы безопасности*** обеспечивает диалоговый интерфейс пользователя (офицера безопасности) с системой безопасности для выполнения криптографических процедур – генерации ключей, обмена ключами.

### 1.2.9. СЕРВИСНО-СПРАВОЧНЫЙ МОДУЛЬ

Сервисный модуль системы авторизации предназначен для регистрации параметров, необходимых для работы системы авторизации, получения разнообразной справочной информации, инициирования технологических процедур, предусмотренных в рамках системы авторизации.

Состав функций сервисного модуля зависит от тех функций, которые должна выполнять система авторизации в процессинговом центре.

---

*В процессинговом центре эквайера сервисный модуль обеспечивает***:**

- Регистрацию обслуживаемых эквайеров, их фирм, филиалов и терминалов;
- Регистрацию ограничений, устанавливаемых для отдельных эквайеров, фирм, филиалов, и терминалов;
- Регистрацию списка блокированных карт и стоп-листа;
- Выполнение процедуры выгрузки в систему учета (бэк-офис эквайера) уведомлений об авторизованных операциях (авторизационные и финансовые параметры операции);
- Формирование справок по обработанным транзакциям с использованием различных фильтров поиска;
- Формирование различных отчетов по обработанным транзакциям;
- Запуск процедуры архивации и чистки базы данных подсистемы авторизации.

---

*В процессинговом центре эмитента сервисный модуль обеспечивает:*



- Регистрацию обслуживаемых эмитентов;
- Выполнение процедуры выгрузки в систему учета (бэк-офис эмитента) уведомлений о предоставленных положительных и отрицательных ответах на авторизационные запросы;
- Обработку поступивших из бэк-офиса эмитента файлов, содержащих параметры карт и условия авторизации операций с их использованием;
- Выполнение оперативной блокировки/разблокировки карт по заявкам держателей карт или обслуживаемых банков-эмитентов в случаях утери или кражи карт.
- Формирование справок по обработанным транзакциям с использованием различных фильтров поиска;
- Формирование различных отчетов по обработанным транзакциям.

---

*В процессинговом центре расчетно-авторизационного центра сервисный модуль обеспечивает:*

- Выполнение выгрузки в систему учета (бэк-офис) уведомлений об авторизованных карточных операциях (информация используется для расчета в бэк-офисной системе лимитов авторизации, устанавливаемых для эмитентов и эквайеров);

- Выполнение установки лимитов авторизации для эмитентов и эквайеров. Лимиты устанавливаются на основе данных, переданных из системы бэк-офиса;

- Формирование справок по обработанным транзакциям с использованием различных фильтров поиска.

### 1.2.10. МОДУЛЬ ПАКЕТНОЙ АВТОРИЗАЦИИ ОПЕРАЦИЙ

Модуль пакетной авторизации операций предназначен для обеспечения авторизации операций оплаты товаров/услуг и операций коммунального платежа, осуществляемых торгово-сервисным предприятием или банком-эквайером без присутствия держателя и его карты. В подобных ситуациях торгово-сервисное предприятие (фирма) или банк осуществляют операцию на основе разового или постоянно действующего поручения клиента на списание средств с его карты.

Торгово-сервисное предприятие или банк-эквайер формирует специальный файл-журнал, который может включать несколько пакетов для отдельных получателей платежей (исходный журнал с записями по операциям), необходимый для проведения авторизации операций. Банк-эквайер, обслуживающий торгово-сервисное предприятие, с помощью модуля пакетной авторизации операций на основании подготовленного исходного файла-журнала производит авторизацию каждой операции, содержащейся в журнале. В момент авторизации происходит выяснение наличия средств на карте клиента и блокирование суммы на карточном счете клиента. Данные по успешно авторизованным операциям заносятся в журнал финансовых транзакций, который направляется на обработку в бэк-офис.

Операции, не прошедшие авторизацию, делятся на две группы (в зависимости от полученного кода отказа):

- в случае отсутствия средств на карте банк-эквайер готовит возвратный реестр для передачи в торгово-сервисное предприятие для последующего разбирательства с клиентом;
- в случае если авторизацию невозможно было провести (например, не было связи с эмитентом, произошел системный сбой и т.д.), то информация о данных операциях через некоторое время будет отправлена на повторную обработку.

Для взаимодействия с центром авторизации в модуле пакетной авторизации операций предусмотрено три вида обмена:

1. Передача данных через разделяемую память;
2. Передача данных через файлы;
3. Передача данных по TCP/IP.

***Передача данных через разделяемую память*** - наиболее эффективный и защищенный канал обмена. Это максимально простой в использовании канал, имеющий ограничение на размещение модулей: они должны выполняться на одном компьютере.

***Передача данных через файлы*** позволяет обмениваться данными между модулями на одном компьютере и в рамках сети через разделяемые диски. Такой тип обмена наименее защищен и имеет много ограничений (скорость доступа к диску, размер свободного места на диске и т.д.).

***Передача данных по TCP/IP*** позволяет с высокой скоростью обмениваться данными модулям, находящимся как на одном компьютере, так и в рамках сети. Данный канал обмена обеспечивает достаточно высокую степень защиты данных.

## 1.3. ВНЕШНИЕ ИНТЕРФЕЙСЫ СИСТЕМЫ

### 1.3.1. ИНТЕРФЕЙСЫ С СЕТЯМИ ПЛАТЕЖНЫХ СИСТЕМ

Интерфейсы с сетями платежных систем обеспечивают преобразование между стандартизированным протоколом обмена ядра системы авторизации и протоколами, принятыми в сетях онлайнового обмена конкретных платежных систем. Интерфейс с каждой такой сетью платежной системы реализован в виде отдельного шлюза. В состав системы авторизации входят следующие шлюзы:

- Шлюз EPSN-Gate – шлюз с сетью платежной системы MasterCard;
- Шлюз VISA-Gate – шлюз с сетью платежной системы VISA;
- Шлюз DC-Gate – шлюз с сетью платежной системы Diners Club;
- Шлюз UNION-Gate – шлюз с сетью платежной системы Юнион Кард;
- Шлюз STB-Gate – шлюз с сетью платежной системы СТБ-Кард.

***Шлюз EPSN-Gate*** обеспечивает подключение к сети платежной системы MasterCard и поддерживает требования протокола обмена как для хоста эквайера, так и для хоста эмитента.

Подключение может осуществляться с использованием коммуникационных протоколов X.25 или IP по одной или нескольким логическим сессиям. При этом работа в рамках каждой из сессий может включать обработку как отдельно трафиков эквайера или эмитента, так и обработку смешанного трафика.

Кроме авторизационных сообщений, используемых в ходе авторизационного процесса, шлюз позволяет осуществлять работу с электронным стоп-листом Europay при помощи сообщений 0304/0314. Поддерживается полный спектр данных сообщений:

- постановка карты в стоп-лист,
- изменение состояния карты в стоп-листе,
- удаление карты из стоп-листа,
- запрос состояния карты, присутствующей в стоп-листе.

Шлюз осуществляет контроль за наличием физического соединения с ЕМ-модулем и, при разрыве коммуникационного соединения, осуществляет его автоматическую переустановку и возобновление всех логических сессий.

***Шлюз VISA-Gate*** обеспечивает подключение к сети платежной системы VISA и поддерживает требования обмена с сетью как в части хоста эквайера, так и в части хоста эмитента. Шлюз способен осуществлять обмен как на основе технологии двух сообщений (протокол Visa Base I), так и на основе технологии одного сообщения (протокол Visa SMS).

Шлюз осуществляет контроль наличия физического соединения с сетью и осуществляет автоматическую переустановку логического соединения в случае его разрыва при сбоях коммуникаций.

Подключение может осуществляться с использованием коммуникационных протоколов X.25 или TCP/IP.

***Шлюз DC-Gate*** обеспечивает подключение к внешней процессинговой системе в соответствии с протоколом, используемым для обмена между хостом эквайера и процессинговым центром платежной системы Diners Club.

Подключение может осуществляться с использованием коммуникационных протоколов X.25 или TCP/IP.

***Шлюз UNION-Gate*** обеспечивает подключение к процессинговым центрам платежной системы Юнион Кард по протоколу UC-ISO.

***Шлюз STB-Gate*** обеспечивает подключение к процессинговому центру платежной системы СТБ Кард по онлайновому протоколу внешних сообщений Base24 (BIC).

В рамках технологии 3Card-F также реализованы **интерфейсы для взаимодействия в рамках локальной платежной системы** и **интерфейсы для взаимодействия с бэкофисными системами обслуживаемых банков**.

#### 1.3.2. ИНТЕРФЕЙСЫ С ПРОЦЕССИНГОВЫМИ СИСТЕМАМИ СТОРОННИХ РАЗРАБОТЧИКОВ

Интерфейсы с процессинговыми системами сторонних разработчиков обеспечивают преобразование между стандартизированным внутренним протоколом ядра системы авторизации и протоколом, принятым в авторизационном комплексе стороннего разработчика. Интерфейс с каждой такой системой реализован в виде отдельного шлюза. Система авторизации имеет шлюзы для взаимодействия с системами TP-II, Base24, OpenWay, SmartVista, Compass+ и другими.

#### 1.3.3. ИНТЕРФЕЙС ДЛЯ ВЗАИМОДЕЙСТВИЯ В РАМКАХ ЛОКАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

Интерфейс для обеспечения взаимодействия в рамках локальной платежной системы может использоваться в том случае, если предполагается организовать локальный обмен (Domestic Interchange) сообщениями между несколькими банковскими процессинговыми центрами, использующими программное обеспечение 3Card-F и входящими в локальную платежную систему. Участники такой системы могут взаимодействовать друг с другом через данный интерфейс.

#### 1.3.4. ИНТЕРФЕЙС С БЭК-ОФИСНЫМИ СИСТЕМАМИ ОБСЛУЖИВАЕМЫХ БАНКОВ

Интерфейс с бэк-офисными системами обеспечивает передачу информации между системой авторизации и системами учета (бэк-офисными системами) тех банков, которые обслуживаются в системе авторизации. Через этот интерфейс осуществляется:

- Прием и обработка сформированных в системе учета сообщений-запросов на регистрацию в системе авторизации параметров карт и запросов данных об остатках средств по картам;
- Формирование и передача в систему учета ответных сообщений – результатов обработки сообщений-запросов;
- Формирование и передача в систему учета уведомлений об обработанных в системе авторизации транзакциях

### 1.4. ПЕРСОНАЛЬНЫЙ БАНКОВСКИЙ СЕРВИС В РАМКАХ СИСТЕМЫ 3CARD-F

#### 1.4.1. ПЕРСОНАЛЬНЫЙ БАНКОВСКИЙ СЕРВИС И ЕГО ПРЕИМУЩЕСТВА

«***Персональный банковский сервис***» (далее по тексту – ПБС) - это одна из последних разработок компании «Программные системы и технологии», основанная на технологии 3Card и направленная на расширение спектра предоставляемых банковских услуг за счет использования электронных устройств (АТМ). Иными словами, ПБС – это обеспечение возможности доступа клиента к управлению его денежными средствами через банкомат.

При внедрении ПБС на основе программного комплекса 3Card на принадлежащие ему АТМ, *банк-Заказчик* получает целый ряд ощутимых преимуществ, выгодно облегчающих повседневную деятельность кредитной организации:

- Расширение зоны обслуживания клиентов за счет установленных банком электронных устройств (АТМ), т.к. клиент (физическое лицо) избавляется от необходимости посещения офиса банка, например, с целью открытия депозита или погашения кредита;
- Значительное снижение расходов за счет экономии на организации и эксплуатации сети отделений/агентств;
- Снижение себестоимости банковских услуг за счет экономии на оплате труда сотрудников филиалов/отделений, функции которых выполняет банкомат;
- Увеличение объема привлекаемых денежных ресурсов и наращивание клиентской базы (за счет появившейся возможности клиента воспользоваться банковской услугой непосредственно около дома, места работы/учебы);
- Увеличение операционных доходов банка за счет комиссий за выполнение платежей и получения дохода от платежных систем в виде «interchange»;
- Снижение нагрузки на операционистов подразделений банков, решение вопроса очередей и недовольства клиентов из-за напрасной траты времени.

Свои преимущества от широкомасштабного внедрения ПБС получают также и *клиенты* банка-Заказчика:

- Круглосуточное управление своими счетами/картами, в том числе в выходные и праздничные дни;
- Независимость от территориального расположения офисов банка (удобство и экономия времени);
- Возможность доступа к новым видам услуг (различные виды платежей и переводов);
- Оперативное получение информации о состоянии своих счетов и движении денежных средств по ним;
- Надежность и безопасность совершения банковских услуг.

### 1.4.2. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ПБС

На основании детального изучения рынка банковских услуг, и исходя из анализа опыта сотрудничества с отдельными заказчиками, в основу ПБС были заложены следующие принципы построения:

1. ***Динамичность*** *построения дерева меню ПБС на банкомате.*

   Т.е. банк, исходя из потребностей клиентов и своих возможностей, самостоятельно определяет перечень и последовательность объектов и операций, участвующих в ПБС. К тому же клиент банка имеет возможность при обращении в банк «отключить» вывод на экран банкомата некоторых не нужных ему опций меню.

2. Важнейший принцип – ***расширяемость*** *системы*.

   В перспективе планируется значительно увеличить функциональность системы, и механизм ее построения позволяет это реально выполнить. Кроме того, гибкость системы позволяет легко адаптировать ее к требованиям отдельного заказчика.

   Существует возможность добавления в ПБС новых операций, в том числе выполняемых не в 3Card-R, а в другой сторонней системе. Гибкость ПБС позволяет организовать его взаимодействие с различными сервисами, автоматизирующими обслуживание физических лиц в режиме off-line и с различными карточными проектами. При этом не составляет труда организовать взаимодействие ПБС с несколькими сторонними розничными системами одновременно.

Расширения списка операций и списка типов объектов позволяет без существенной переделки настраивать систему на новые объекты банка. В частности, механизм ПБС настолько эффективен, что на него можно полностью перевести обслуживание коммунальных платежей, которые могут выполняться, в том числе и в произвольной сторонней системе.

«Персональный Банковский Сервис» на основе системы 3Card-F легко настраивается под индивидуальные требования конкретного банка-заказчика. Система позволяет контролировать производимые операции на всех этапах их выполнения и, при необходимости корректировки, гибко дополняется программным обеспечением (plug-ins) заказчика либо стороннего разработчика.

3. *Сокращение загрузки 3Card-R и снижение времени отклика банкомата*.

   При построении ПБС основополагающим моментом было условие создания такой схемы работы, которая бы максимально сокращала загрузку 3Card-R в режиме реального времени и снижала бы время отклика банкомата при обслуживании «своих» и «чужих» карт.

4. ***Безопасность*** *сервиса для клиента* (снижение риска мошенничества).

   Весь ПБС построен с учетом требований российского банковского законодательства и Правил платежных систем.

   При этом дополнительно, с целью максимально снизить потери клиентов и банка в результате мошеннических операций, особенно по украденным/утерянным картам, Компанией принято решение при внедрении ПБС ориентироваться не на массовость услуги, а на ее добровольность и индивидуальность.

   Таким образом, средства 3Card-R позволяют управлять включением/отключением от участия в ПБС на банкоматах определенных объектов (типовых и индивидуальных) по усмотрению банка и/или клиента.

5. *Схема построения меню ПБС - «от объекта», а не «от операции»* (как традиционно принято для банкоматов), т.е. первоначально на экран банкомата выводится тип и/или наименование объекта, затем предлагается выполнить набор доступных для данного объекта операций.

6. *Возможность использования банкоматной сети банка в качестве дополнительного средства «давления» на недобросовестных заемщиков*.

   Другими словами, работа ПБС начинается с поиска по идентификатору клиента – держателя загруженной в банкомат банковской карты, кредитных договоров, по которым допущена просрочка платежа. Если таковые имеются, на экран банкомата выводится информационная строка, сообщающая о факте наличия просроченной задолженности. Только после этого клиент может продолжить работу с меню ПБС. (С целью уменьшения времени отклика банкомата данная опция может быть банком отключена).

7. *Возможность манипулировать составом он-лайн запросов/ответов 3Card-F - 3Card-R по усмотрению банка и исходя из возможностей его коммуникаций*.

   С целью минимизации трафика при выборе клиентом объекта на банкомате, 3Card-F отправляет в 3Card-R запрос сразу же на все значения аналитических признаков данного объекта, независимо от типа выбранной пользователем операции над этим объектом. Иной вариант – формирование запроса на конкретную выбранную клиентом операцию.

8. ***Поддержка*** *максимально широкого спектра внешних устройств*.

   Основанный на онлайновой процессинговой системе 3Card-F «Персональный Банковский Сервис» поддерживает взаимодействие с различными типами банкоматов – NCR, Diebold, Wincor, а также всеми видами инфокиосков. Имеется возможность выполнения операций ПБС на POS-терминалах.

### 1.4.3. ОБЩАЯ СХЕМА РЕАЛИЗАЦИИ ПБС И РОЛИ СИСТЕМ.

Общая схема передачи информации представлена на рисунке 4:

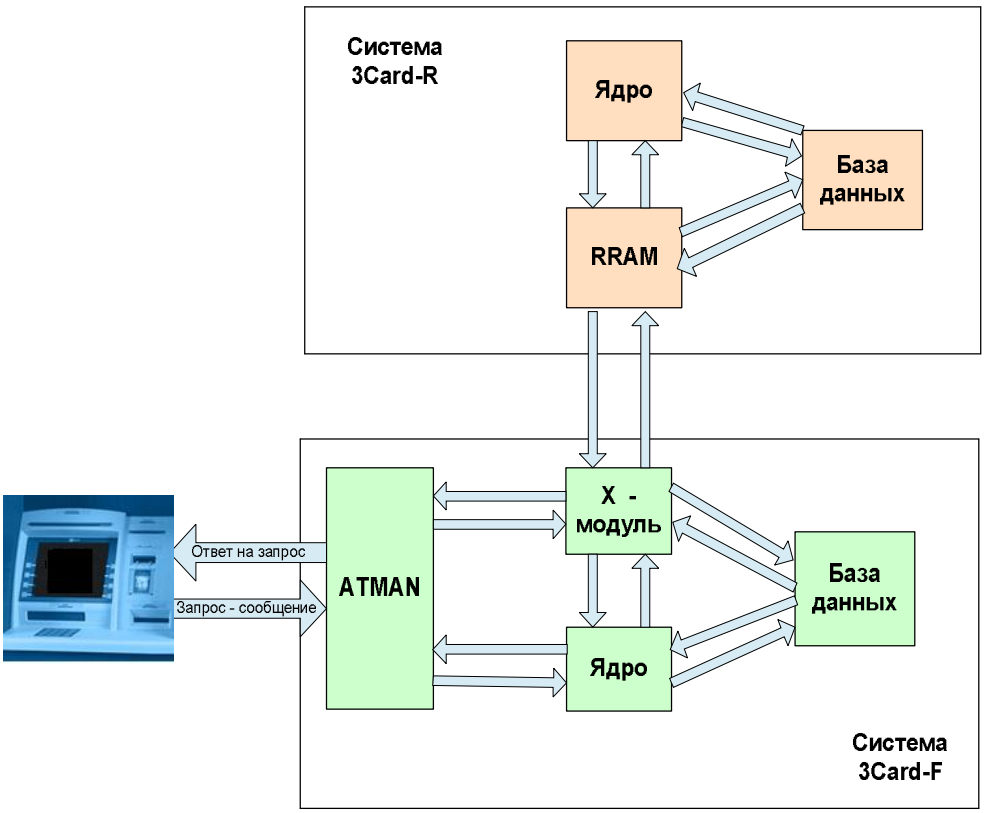



**Рис. 4. Общая схема реализации ПБС.**

1. **ATMAN** – это контроллер банкомата, который обеспечивает «диалог» с ним. Обмен с банкоматом производится в формате NDC.

   В функции ATMAN так же входит построение ***примитивов*** ПБС – последовательности экранов, отображающих объекты, операции и их результаты. Цепочки примитивов в общем случае строятся динамически и управляются внешними по отношению к банкомату системами (ATMAN, XModule, RRAM).

2. **X-модуль** - это основной модуль ПБС в 3Card-F. Он координирует работу остальных частей системы. Обмен с 3Card-R выполняется через модуль удаленного доступа к системе 3Card-R (RRAM). Цель всего этого взаимодействия: принять сообщение, сформировать объекты ПБС и/или провести операции в 3Card-R. Поскольку X-модуль рассчитан на расширение ПБС, он работает не с конкретными операциями и объектами, а с их типами.

3. **RRAM** – этот шлюз выполняет схожие с X-модулем задачи, но в 3Card-R. RRAM обрабатывает сообщения от внешних систем, формирует объекты и уведомляет ядро 3Card-R о необходимости совершения соответствующих операций.

4. **Ядра 3Card-F и 3Card-R** фактически выполняют все операции ПБС. Соответственно, они работают уже с конкретными операциями, а не с их типами. Все операции ПБС реализуются в ядре явно, поэтому, расширение ПБС требует, в первую очередь, поддержку этих операций в 3Card-F и 3Card-R.

*Необходимо подчеркнуть, что важнейшей функциональной частью ПБС является онлайновая процессинговая система 3Card-F, непосредственно взаимодействующая с АТМ банка. X-модуль системы 3Card-F может взаимодействовать с модулем удаленного доступа к системе 3Card-R (RRAM), но подобная связь не является единственно возможной. Ориентированность на работу с типами объектов и операций позволяет реализовать ПБС на основе 3Card-F не только в связи с 3Card-R, но и во взаимодействии со сторонними системами, проводящими собственный учет транзакций.*

### 1.4.4. СПИСОК ДОСТУПНЫХ ОПЕРАЦИЙ В РАЗРЕЗЕ ПБС.

**Пополнение депозита -** перевод средств с карточного счета на депозитный. Операция выполняется в 3CardF и уменьшает лимит карты. Из 3Card-F в 3Card- R поступает online уведомление, на основании чего в 3Card-R производится окончательная обработка операции.

**Списание части средств с депозита -** списание средств со счета, отличного от карточного (открытого для загруженной в банкомат карты). Операция выполняется в 3Card-R на основании уведомления из 3Card-F. Авторизационный лимит карты не меняется.

**Досрочное закрытие депозита -** операция выполняется в 3CardR, online уведомление от 3Card-F воспринимается как заявка на совершение операции. On-line кредитование лимита карты в 3CardF не производится.

**Справка по депозиту -** вывод общей информации по депозиту клиента (условия вклада).

**Выписка по депозиту -** вывод выписки по депозиту за период времени.

**Открытие вклада -** открытие депозита на условиях, предложенных банком. Операция выполняется в 3CardF и дебетует лимит карты. Непосредственно открытие депозита в 3CardR может проводиться в режиме offline, таким образом, online уведомление от 3CardF будет воспринято как заявка на совершение операции.

**Погашение задолженности по кредиту -** погашение кредита/его части за счет средств на карточном счете. Операция уменьшает лимит карты. И выполняется в 3Card-F. Погашение задолженности производится в 3Card-R на основании уведомления из 3Card-F.

**Погашение задолженности по кредиту (внесение наличных) -** погашение кредита/его части за счет за счет внесения наличных средств клиентом.

**Получение справки по кредиту -** получение информации об условиях открытого кредитного договора и его текущем состоянии. В рамках операции также выводится график погашения кредита.

**Получение справки по кредиту (без графика) -** выводится информация по кредиту и расшифровка по предстоящему платежу.

**Получение выписки по кредиту -** получение из 3Card-R списка проведенных операций погашения кредита с расшифровкой состояния выполнения.

**Просроченный кредит -** операция, которая автоматически запускается при выборе меню «ПБС» и информирует клиента о факте наличия у него просроченной задолженности (без расшифровки по договорам).

**Заявка на выдачу кредита -** оформляется заявка на выдачу кредита клиенту.

**Выписка по карте -** операция выводит перечень и содержание последних n- операций, произведенных по карте.

**Остаток по карте -** результат операции - вывод на экран/печать значения доступного баланса по карте и его расшифровка.

**Справка по карте -** выводится общая информация по карте.

**Блокировка карты -** операция предназначена для блокировки или разблокировки карты (в зависимости от текущего ее состояния, т.е. операция меняет состояние карты на противоположное). Код блокировки и срок настраиваются банком одинаково для всех клиентов.

**Перевод -** перевод средств с карточного счета по произвольным реквизитам, зафиксированным в шаблоне перевода. В результате формируется поручение на перевод по шаблону. Операция осуществляется в 3Card-F, затем передается уведомление в 3Card-R для окончательного исполнения. Лимит карты уменьшается.

**Платеж -** перевод средств в пользу получателя – юридического лица, зафиксированного в системе 3Card-F, за предоставленные услуги.

**Выписка по шаблону платежа/перевода -** в результате выполнения операции должна выводиться информация о дате платежа, сумме и состоянии выполнения в 3CardR. Уведомления о платежных операциях должны выгружаться в 3CardR в режиме online.

# 2. СИСТЕМА ПЕРСОНАЛИЗАЦИИ ПЛАСТИКОВЫХ КАРТ.

## 2.1 ОБШЕЕ ОПИСАНИЕ СИСТЕМЫ ПЕРСОНАЛИЗАЦИИ ПЛАСТИКОВЫХ КАРТ.

Включает в себя процесс подготовки пластиковой карты к ее использованию для осуществления карточных операций держателем, включающий присвоение платежной карте уникального номера, нанесение его на карту, указание на ней имени держателя и срока действия. Кроме того, при выполнении этой процедуры на магнитную полосу или в микропроцессор карточки записывается информация, необходимая для обслуживания карты в торговых фирмах, банкоматах и пунктах выдачи наличных, после чего карта считается готовой к использованию.

Персонализация и ввод карт в обращение включает в себя следующие этапы:

- регистрация параметров карт в системе внутреннего учета эмитента, подготовка исходных данных для персонализации и их передача в центр персонализации;
- персонализация карт в собственном или стороннем центре персонализации, обслуживающем эмитента;
- передача данных о персонализированных картах из центра персонализации в систему учета процессора-эмитента для регистрации;
- передача данных о персонализированных картах из системы внутреннего учета эмитента в обслуживающий его центр авторизации для начала осуществления авторизации по этим картам.

## 2.2 КОМПОНЕНТЫ СИСТЕМЫ.

### Генерация ПИН-кода и кодов PVV и CVV

Модуль персонализации по итогам обработки файла заявки на персонализацию дает команду модулю безопасности сгенерировать ПИН для персонализируемой карты. Модуль безопасности производит генерацию ПИНа в шифрованном виде и осуществляет его печать на принтере для печати ПИН-конвертов (PIN-mailer printer), если не задано использование отложенной печати. Кроме того, модуль безопасности передает Модулю персонализации следующие параметры, используемые в дальнейшем для проверки ПИН-кода:

- код проверки ПИНа (PVV - PIN Verification Value), который содержит в шифрованном виде связанные по специальному алгоритму значения номера карты (PAN), номера ключа проверки ПИНа (PVKI - PIN Verification Key Index) и ПИН-кода;

- код проверки карты (CVV - Card Verification Value), который содержит в шифрованном виде связанные по специальному алгоритму значения номера карты (PAN), сервис-кода (Service Code) и даты окончания срока действия карты (Expiration Date).

Сгенерированные модулем безопасности параметры используются Модулем персонализации при формировании файла данных для эмбоссинга и энкодинга.

## Подготовка файла данных для эмбоссинга и энкодинга

Файл, содержащий данные для эмбоссинга и энкодинга, формируется Модулем персонализации на основе данных, переданных в центр персонализации процессором эмитента в файле заявки на персонализацию, а также данных, полученных из модуля безопасности. Данные, сформированные для эмбоссинга и энкодинга карты, выгружаются в текстовой файл специального формата. Каждая строка этого файла содержит данные для персонализации одной карты. Файл содержит следующие данные:

- информацию для эмбоссинга карты в виде включающих специальные разделители групп символов, которые должны быть эмбоссированы на карте;

- данные, которые должны быть закодированы на магнитной полосе карты;

- дополнительные данные для персонализации чиповых карт (если персонализируется чиповая или комбинированная карта).

Следует отметить, что форматы файла данных для эмбоссинга и энкодинга могут различаться при персонализации карт разных платежных систем из-за отличий в правилах эмбоссинга и энкодинга, принятых в платежных системах. Модуль персонализации, разработанный ООО "Программные системы и технологии", позволяет производить настройку формата файла данных для эмбоссинга и энкодинга в зависимости от типа используемого для энкодинга и эмбоссинга оборудования (эмбоссера) и требований конкретной платежной системы.

## Подготовка файла для отложенной печати ПИН-конвертов

Если не требуется осуществлять печать ПИН-кода непосредственно при его генерации, то Модуль персонализации может сформировать *файл для отложенной печати*ПИН-конвертов, содержащий ПИН-коды в зашифрованном виде. Этот файл в дальнейшем направляется для обработки в отдельный Модуль печати ПИН-конвертов, который осуществляет печать ПИН-кодов на принтере для печати ПИН-конвертов внутри ПИН-конвертов, предназначенных для передачи держателям карт.

## Подготовка ответного файла для регистрации параметров персонализированных карт в системе внутреннего учета эмитента

По итогам персонализации Модуль персонализации формирует ответный файл, содержащий данные об итогах обработки в центре персонализации представленного эмитентом файла заявки на персонализацию карт. После обработки ответного файла система учета эмитента присваивает соответствующим картам состояние "Действующая" и включает данные о персонализированных картах в очередной исходящий файл обмена с центром авторизации для осуществления регистрации вновь персонализированных карт в центре авторизации эмитента.

## 2.3 ОБОРУДОВАНИЕ И СИСТЕМА БЕЗОПАСНОСТИ.

В составе системы 3Card-P система безопасности обеспечивает выполнение функций, связанных с генерацией секретных параметров, используемых при персонализации карт (PIN, PVV, CVC/CVV), печатью PIN-конвертов и других.

Система безопасности включает в себя следующие основные компоненты:

- Сервер безопасности;
- АРМ администратора системы безопасности.

**Сервер безопасности** обеспечивает выполнение всех криптографических процедур в рамках перечисленных выше функций. Он поддерживает работу с одним или одновременно с несколькими аппаратными модулями безопасности (Hardware Security Modules, HSM).

Все ключи, используемые в криптографических процедурах, хранятся в базе данных ключей в зашифрованном виде. Мастер-ключ, которым зашифрованы эти ключи, хранится внутри аппаратного модуля безопасности.

Поддерживаются следующие аппаратные модули безопасности:

- Racal 8000 (
- Racal 7400 (COM-интерфейс);
- Racal 7000 (Ethernet-интерфейс);
- Racal 6000 (COM-интерфейс);
- ESM (только персонализация).

Поддерживаются следующие криптографические алгоритмы:

- DES;
- Triple DES (кроме Racal 6000);
- RSA;
- ГОСТ 28147-89;
- ГОСТ Р 34.10-94.

Поддерживается генерация следующих криптографических кодов:

- PVV;
- CVV (CVC1/CVV1 и CVC2/CVV2);
- MAC;
- имитовставка (ГОСТ).

Каналы доступа к подсистеме безопасности защищены протоколом SSL, обеспечивающим взаимную аутентификацию сторон.

**Автоматизированное рабочее место (АРМ) администратора системы безопасности** обеспечивает диалоговый интерфейс пользователя с системой безопасности для работы с ключами (генерация, распределение, работа с БД ключей и т.п.), персонализации смарт-карт, используемых для транспортировки и загрузки ключей на терминалы.