

Управляемость и информационная безопасность персонализации

Дмитрий Сахаров технический директор,

Сергей Слепнев, директор по исследованиям и разработкам, компания ПРОНИТ (группа компаний КАРТХОЛЛ)



Дмитрий Сахаров



Сергей Слепнев

Как известно, “каркас безопасности”, физически охватывающий весь объем помещения банковского персобиюро, сертифицированного на эмиссию карт Visa International и MasterCard Worldwide, – это толстые стальные прутья, вмонтированные в стены, пол и потолок через каждые 15 сантиметров площади. Что же играет роль аналогичного “каркаса” информационной безопасности и оперативного управления персобиюро? Что делает персобиюро защищенным от злоупотребления конфиденциальной информацией, обеспечивает работу разнообразных устройств персонализации в единой системе, организует процессы персонализации и делает их управляемыми? В этой статье речь пойдет об информационной системе Octopus, которая создана для централизованного управления, учета, планирования, контроля и обеспечения информационной безопасности персонализационного бюро.

Новые условия работы

Давно миновали те времена, когда российские банки могли персонализировать платежные карты на одном эмбоссере в комнате размером с чулан, а персонализационные данные переносить на дискете 3,5 дюйма. Сегодня размерность задачи персонализации карт и требования к информационной безопасности значительно выросли. Если в 90-е годы прошлого века объемы эмиссии банка могли достигать 10 тыс. карт в месяц, то теперь ведущие персонализационные центры выпускают более 10 тыс. карт в час – как видно, потребности рынка возросли более чем на два порядка. Если раньше работу с чувствительными к компрометации данными можно было доверить двум-трем надежным и близким людям, то сегодня собственники бизнеса предъявляют жесткие требования к организации информационного обмена внутри банка и ответственности его сотрудников. Банки вступают в международные платежные системы, в связи с чем их персонализационные бюро должны удовлетворять целым томам

требований к организации операционной деятельности и информационной безопасности, и это соответствие должно успешно подтверждаться в ходе процедур технического аудита и сертификации.

Решаемые задачи

С развитием карточного бизнеса банка растут объемы эмиссии, увеличивается количество единиц оборудования в персобиюро, расширяется портфель выпускаемых карточных продуктов. Для некоторых эмитентов становится характерным оказание спонсорских услуг другим банкам, только начинающим продвигаться в направлении эмиссии международных карт. В связи с этим повышаются требования к качеству и оперативности решения целого ряда задач, стоящих перед подразделениями банка, занимающихся персонализацией карт и выпуском различной сопутствующей продукции (например, ПИН-конвертов и бумажных носителей для рассылки карт). К этим задачам относятся:

- **управление устройствами персонализации:**
 - оптимальная загрузка персонализационных устройств;
 - минимизация суммарного времени выполнения персонализационного задания;
 - оперативное переключение задач персонализации между устройствами различных типов с трансляцией персонализационных данных в требуемый формат;
 - параллельное использование различных устройств и технологий для персонализации одного и того же карточного продукта;
 - оперативное обнаружение брака карт и ошибок, произошедших как по вине персонала персобиюро, так и из-за сбоя

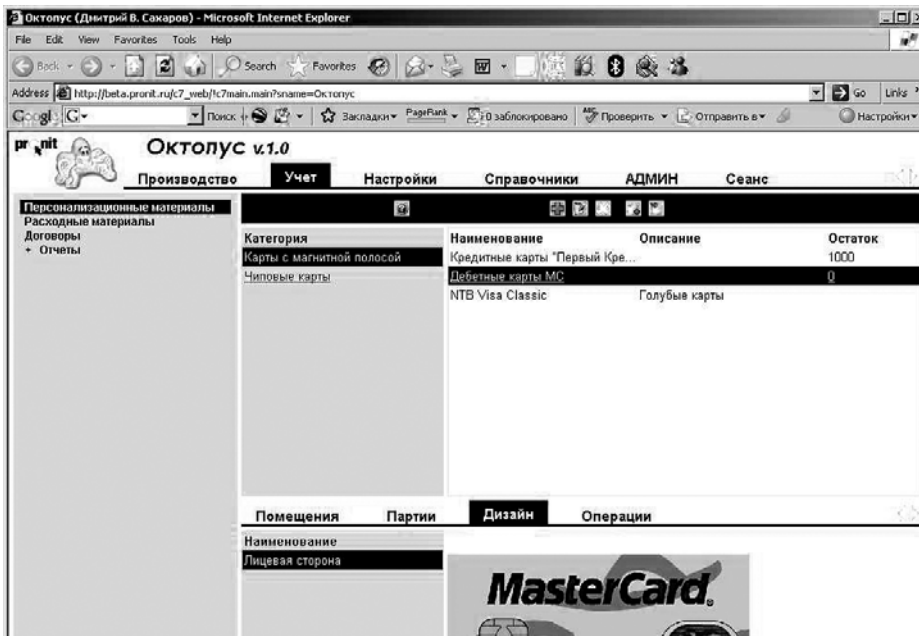


Рис. 1. Пример рабочего места системы Ostorus с группой функций “Учет”

в работе иных связанных с эмиссией подсистем;

• работа с данными:

– обработка и объединение входных файлов из нескольких источников и в различных форматах, с учетом того, что форматы данных подвержены изменениям с течением времени;

– объединение данных по сложным алгоритмам из нескольких видов входной информации;

– соблюдение слабо формализуемых временных ограничений и реализация бизнес-правил при взаимоотношениях с поставщиками персонализационных данных;

• задачи персонализации и рассылки:

– выпуск карт с индивидуальным дизайном;

– группировка персонализированных карт с дополнительными материалами (формами, письмами) в составе почтовой корреспонденции;

– персонализация карт с разрывом во времени и пространстве (при персонализации одной карты на нескольких персонализационных устройствах с выполнением ряда последовательных персонализационных операций);

• соответствие стандартам международных платежных систем:

– разграничение доступа к персонализационным данным на различных этапах персонализационного процесса;

• оперативное управление:

– получение детализированной адресной информации о том, кто, когда и на каком оборудовании какие карты выпускал, какие данные для этого использовал и откуда их получил;

– учет и отслеживание потоков персонализационных материалов, формирование оперативной информации о состоянии склада;

– отслеживание состояния заданий на персонализацию;

– отслеживание выполнения договоров с поставщиками и партнерами, мониторинг состояния выполнения обязательств;

– формирование производственной и аналитической отчетности.

Решить перечисленные задачи можно при помощи информационной системы, которая обеспечивает систематизацию и автоматизацию процедур и процессов, входящих в ежедневную деятельность персонализационных подразделений. Такая система, получившая название Ostorus, внедрена компанией ПРОНИТ (группа компаний КАРТХОЛЛ) в одном из крупных банков России с одним из самых высоко-

производительных наборов оборудования для персонализации и пакетирования карт.

Функциональность системы

В структуре функционала системы Ostorus можно выделить три больших множества выполняемых функций:

- автоматизация производственной деятельности;
- учет персонализационных и расходных материалов;
- планирование работ.

Рассмотрим важнейшие составляющие каждого из множеств подробнее.

Автоматизация производственной деятельности. Функциональный модуль автоматизации производственной деятельности решает следующие задачи:

- обеспечивает промежуточное хранение данных для персонализации;
- работает с данными, представленными в различных форматах;
- объединяет информацию, поступающую из различных источников;
- позволяет гибко делить эту информацию на группы (в терминах системы – на “персонализационные задания”) для последующего выполнения работ на различных персонализационных устройствах;
- позволяет, с одной стороны, гибко определять перечень работ, которые требуются для выпуска персонализированной карты, а с другой – выбирать устройства с требуемым набором функций из числа имеющихся в распоряжении персонализационного подразделения;
- осуществляет разграничение доступа различных пользователей системы в зависимости от присвоенных им ролей к тем или иным данным, позволяет разграничивать функции и учитывать на системном уровне, кто и когда какие действия выполнял;
- позволяет работать с устройствами различных типов, выгружая для них данные в требуемых форматах;
- позволяет загружать и обрабатывать протоколы работы персонализационных устройств, обеспечивая учет расхода пер-

сонализационных и расходных материалов, учет случаев выпуска бракованных карт, решение задач по повторному изготовлению карт, а также определение персонализационных заданий, выполнение которых необходимо продолжить в следующей производственной смену.

Учет персонализационных и расходных материалов. Модуль учета персонализационных и расходных материалов реализует группу функций, предназначенных для ведения учета, обеспечивающего потребности оперативного управления, планирования, контроля и составления отчетности о деятельности персбюро. Данный модуль позволяет:

- вести учет информации, описывающей договорные отношения с поставщиками персонализационных и расходных материалов;
- отслеживать перемещение персонализационных материалов между различными складами внутри персонализационного бюро;
- отражать в учете, какие персонализационные материалы для выполнения каких заданий использовались, кто получал и работал с конкретными партиями персонализационных материалов, куда поступили эти партии (например, в инкассаторскую или почтовую службу);
- учитывать факты уничтожения бракованной продукции, выдачи и использования заготовок карт для наладки и тестирования оборудования или выполнения ремонтных и профилактических работ.

Планирование персонализации. Функциональный модуль планирования персонализации предназначен для решения задачи оптимизации распределения процедур персонализации карт между различными устройствами в условиях многообразия исходных требований и функциональных возможностей персонализационных устройств. Такая задача актуальна для организаций, которые, с одной стороны, оперируют большим количеством персонализационного оборудования, каждая единица которого может обладать разви-

той функциональностью, с другой – выпускают различные типы пластиковых карт с разнообразным дизайном, что требует выполнения широкой номенклатуры персонализационных процедур.

Система оптимизации, реализованная в модуле построения планов, позволяет оперативно и качественно решать, какие карты с помощью какой последовательности технологических операций на каком наборе персонализационных устройств можно выпускать.

При формировании этого решения во внимание принимается широкий перечень параметров, включая статус персонализационного оборудования, поскольку:

- часть устройств может находиться в состоянии профилактических или ремонтных работ;

- часть устройств может не располагать требуемыми расходными материалами для выполнения процедур, необходимых в рамках конкретного задания.

Информационная безопасность и контроль

Система Octopus обеспечивает информационную безопасность по ряду направлений, которые согласуются с требованиями международных платежных систем Visa International и MasterCard Worldwide к организации работы с оборудованием и данными в персбюро.

Ограничение доступа к содержанию персонализационных файлов. Для обеспечения безопасности использования и хранения данных критически важно, чтобы операторы, инициирующие процедуры

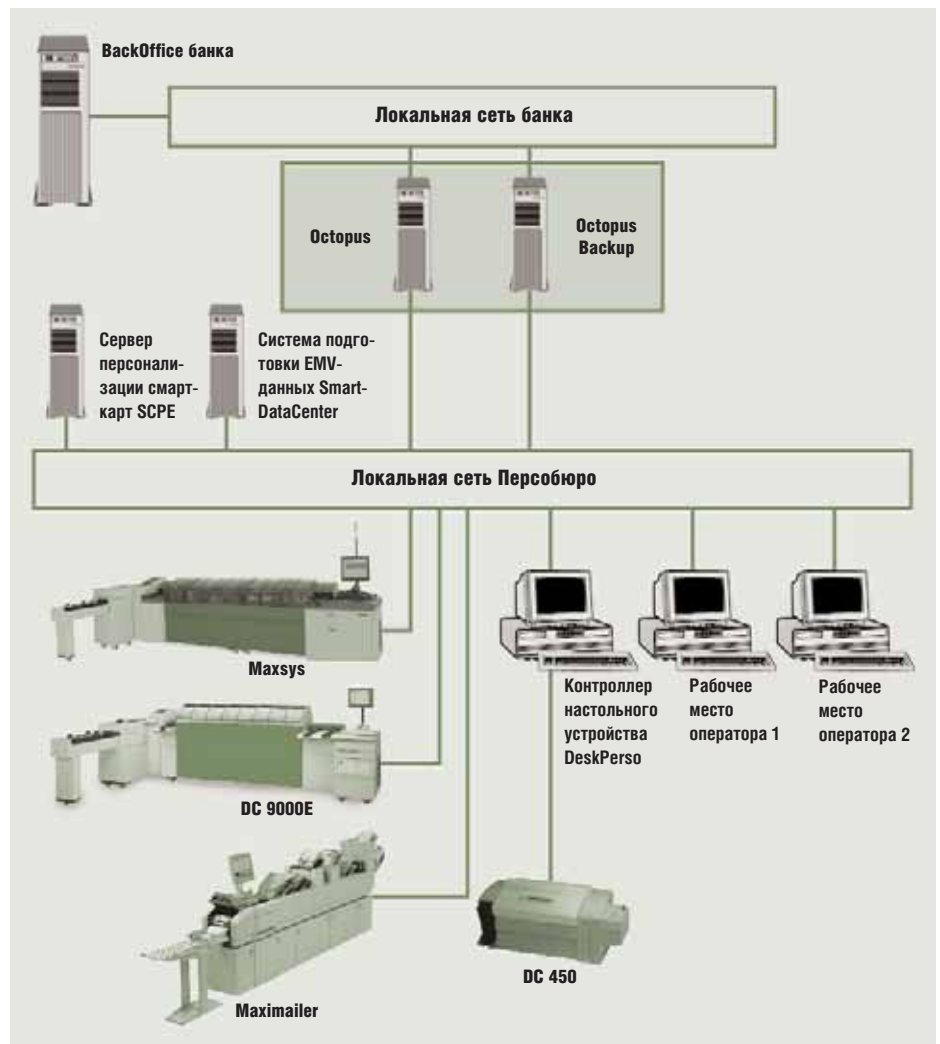


Рис. 2. Место Octopus в информационной системе банка

обработки данных и передачи их на персонализационные устройства, могли работать с файлами как с хранилищами информации, но при этом не имели доступа к данным, находящимся внутри этих файлов. Манипуляции с файлами осуществляются операторами в пользовательском интерфейсе системы Octorpus, где доступ-

В системе мониторинга можно в реальном времени увидеть данные о количестве карт, находящихся на той или иной стадии персонализационного процесса в рамках данного персонализационного задания

ны только имена файлов и при необходимости – ограниченный набор атрибутов записей в этих файлах. Распределение ролей внутри системы и назначение пользователям определенного набора полномочий в операционной среде системы Octorpus позволяет исключить доступ операторов к данным, хранящимся в файлах.

Octorpus – шлюз между системами подготовки данных и персонализационным оборудованием. Система, в которой подготавливаются персонализационные данные, должна быть физически и логически независима от системы персонализации – таковы требования Visa International и MasterCard Worldwide. Разграничение этих систем обеспечивается за счет того, что архитектурно система Octorpus располагается между этими сетями, и аппаратные средства, на которых работает система, подключены, со-

ответственно, и к той, и к другой сети (см. рис. 2).

Протоколирование. Полное информационное обеспечение контрольных процедур достигается за счет строгого учета того, кто, когда, в рамках каких заданий и какие операции выполнял в системе, и какие данные в этих операциях были задействованы. Эксплуатирующая систему Octorpus организация может получить детализированные отчеты о том, где, когда, кто, зачем и какие данные использовал, к каким данным имел доступ. В системе Octorpus на прикладном и системном уровнях ведется подробное протоколирование выполняемых операций, объектов, с которыми эти операции проводились, инициаторов и участников операций и времени их совершения.

Мониторинг в системе Octorpus. Для того чтобы отслеживать оперативное состояние системы персонализации как с рабочей станции руководителя подразделения, так и с рабочих станций операторов, в системе Octorpus реализована функция мониторинга, то есть динамического отображения происходящих в системе процессов. Пользователи, которым доступен блок функций мониторинга, мо-

гут в реальном времени наблюдать за действиями, которые выполняют операторы, за данными, присутствующими в системе и проходящими через различные стадии производственного процесса. В наглядной форме представляется следующая информация:

- какие персонализационные данные были получены системой и приняты к обработке с начала рабочей смены;
- какие персонализационные задания были сформированы из этих данных;
- каким образом задания были распределены между персонализационными устройствами.

В рамках конкретного задания по каждой стадии персонализационного процесса мониторинг отражает количество карт, прошедших через определенные стадии персонализационного процесса. Например, при использовании цветного принтера и эмбоссера для выпуска карт с индивидуальным дизайном карта последовательно проходит ряд технологических операций, включая печать изображения и тиснение. В системе мониторинга можно в реальном времени увидеть данные о количестве карт, находящихся на той или иной стадии персонализационного процесса в рамках данного персонализационного задания (см. рис. 3).

Отчеты в системе Octorpus. В системе Octorpus развиты функции подготовки разнообразной производственной и аналитической отчетности. В системе реализован ряд отчетов, которые позволяют получать информацию о различных аспектах операционной деятельности: реестры выпускаемых карт, файлы, обрабатываемые в течение рабочей смены, отчеты по движениям персонализационных и расходных материалов на складе, а также ряд вспомогательных документов, облегчающих работу операторов и исключающих ошибки, обусловленные человеческим фактором. Такие ошибки могут возникать при выполнении простых операторских задач и сводиться, например, к использованию загото-

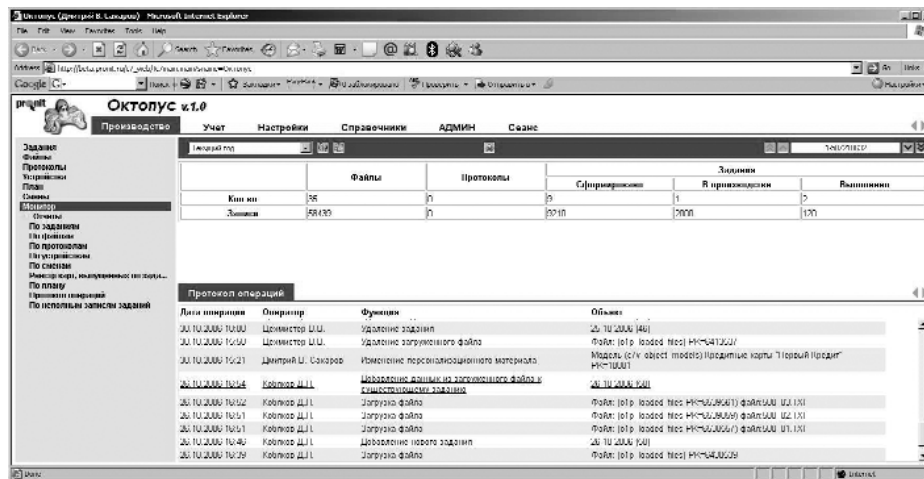


Рис. 3. Монитор системы

вок карт одного типа для выпуска карточного продукта другого типа.

Вероятность подобных досадных и простых ошибок минимизируется при использовании системы Ostorus. Оператор персобиюро получает от системы отчет с информацией о том, какой файл с данными нужно выбрать, сколько в нем записей, какими номерами ограничен пакет карт для задания, и как выглядит заготовка пластика, на которой нужно выпускать соответствующий карточный продукт.

Что касается управленческой отчетности, то руководство подразделения пластиковых карт получает интегральную информацию о выполненных операциях, статусе выполнения обязательств подразделения, состоянии склада на текущий момент, результатах текущего дня, месяца или другого периода (см. рис. 4).

Ряд отчетов используется при взаимодействии между отдельными группами или подразделениями внутри эксплуатирующей систему организации. Например, система Ostorus готовит документы, которые будут сопровождать персонализированные карты при их передаче в почтовое отделение или инкассаторскую службу.

Система Ostorus позволяет генерировать складскую отчетность в соответствии с потребностями различных подразделений. Примером использования возможностей Ostorus может послужить следующая ситуация: руководство персобиюро получает отчет, в котором содержится информация по картам Visa Electron, Visa Business, Visa Gold, Visa Classic, нескольким карточкам локальных платежных продуктов, карточкам MasterCard Mass, Maestro, Electronic, а для бухгалтерии готовится консолидированный отчет, в котором содержатся сведения о картах Visa, MasterCard и картах локальных платежных систем.

Отчеты могут быть представлены как в виде документа в формате html, который можно распечатать, скопировать и обрабатывать, так и в виде документа в формате Excel, который позволяет про-

Задание	Дата создания	Оператор
25-10-2006 (45)	25-окт-2006 13:21:29	Цезимстер В.В.
Продукт: MC Aeroflot	Процесс: MC Aeroflot DC + KirkRudy	

Файл	Всего	Записей		KirkRudy		DC 9000 777	
		Польз.	Непольз.	Выполнено	Не выполнено	Выполнено	Не выполнено
BSC-R888.ATB	4000	2000	2000	2000	2000	0	4000
1606-01-01-ALL-88.TXT	2000	2000	0	2000	0	0	2000
Итого	4000	2000	2000	2000	2000	0	4000

Рис. 4. Пример отчета системы

изводить последующую независимую обработку информации.

Дополнительные свойства и возможности

Операционная среда. Применение современных технологий, используемых в ходе разработки, внедрения и тестирования, позволило сделать систему Ostorus удобной в эксплуатации. Современные промышленные системы, такие, как СУБД Oracle, использование web-технологий для построения рабочих мест обеспечивают простую с точки зрения требований, предъявляемых к персоналу, сопровождающему систему, последовательность действий по инсталляции и разворачиванию системы, настройке рабочих мест. Практически никакие специальные действия, связанные с обеспечением эксплуатации системы, на рабочих местах не требуются. Рабочие станции с современными операционными системами, в том виде, в котором они инсталлируются с дистрибутивных носителей, уже имеют возможность выступать клиентскими рабочими местами системы Ostorus.

Взаимодействие с внешними системами. Важным свойством системы Ostorus является возможность взаимодействия при процедурах выпуска карт с внешними системами. Примером таких систем могут быть системы, агрегирующие и хранящие базы данных с фотографиями или изображениями, используемыми при вы-

пуске карт с индивидуальным дизайном (пример такой системы – на www.pronit.ru/orgux). Система Ostorus позволяет в реальном времени обращаться к таким системам и в момент подготовки данных для их передачи на устройство персонализации обеспечивает дополнение данных для персонализации карт требуемыми изображениями и фотографиями.

Другим характерным примером использования возможностей такого взаимодействия является обращение к системе, подготавливающей данные для персонализации EMV-приложений (пример такой системы – на www.pronit.ru/smartdatacenter), которая генерирует данные для персонализации EMV-приложений VSDC и M/Chip на основе данных для магнитной полосы, набора риск-параметров и зашифрованного ПИН-блока.

Применение системы

Система Ostorus позволяет обеспечить безопасность чувствительных к компрометации персонализационных данных, построить работу персобиюро в соответствии с требованиями и рекомендациями международных платежных систем по организации операционной деятельности и информационной безопасности в персобиюро, а при больших объемах эмиссии позволяет эффективно решать задачи оперативного управления выпуском карт и оптимизировать процессы персонализации.

ПЛАС