Системная архитектура взаимодействия модулей скриммеров, хопперов и монетоприёмников для АСУ банкоматов и кассовых узлов

Антти Эс

Банковская сфера с её клиент-ориентированными элементами – банкоматами традиционно является зоной повышенной ответственности и надёжности, обеспечивают которую с помощью в том числе электронных средств контроля и безопасности. Для того чтобы средства обеспечения банковских транзакций работали надёжно, средства и системы контроля объединяют в автоматизированные системы кеш-менеджмента, управления (АСУ), являющиеся модулями самообслуживания и дистанционного программирования по защищённому каналу. Современные архитектуры АСУ предполагают не только устойчивые к вызовам времени элементы защиты, блокировки и своевременного оповещения служб безопасности, но также обеспечивают полностью автоматизированный процесс контроля (расхода) наличности в банкоматах и планирование инкассации. В статье рассматриваются особенности АСУ «Банкомат», а также некоторые электронные модули банковского и вендингового оборудования (и терминалов) и способы их защиты.

История, устройство и риски

Изобретателем банкоматов считают Джона Шепарда-Баррона из Шотландии. По аналогии с автоматом по продаже шоколада он обосновал и предложил конструкцию по выдаче денег – монет и купюр. Случилось это в 1967 году в одном из лондонских банков. Деньги выдавали в обмен на специальный кассовый чек (авизо), но банкомат уже тогда имел форм-фактор, похожий на современные и привычные нам модели. Современный банкомат состоит условно из двух частей: верхняя предназначена для обмена информацией с клиентом, его идентификации, контроля и наблюдения за его действиями, а нижняя представляет собой «умный сейф». Банкоматы оборудуют внутренней системой защиты и тревожного оповещения, а стенки бронируют. Тем не менее среди опасностей для банкоматов остаются риски их механического повреждения (рис. 1). Однако система комплексной и автоматизированной защиты только за 5 последних лет фундаментально изменилась, а терминалы и кассеты в них стали оборудовать дополнительными замками. В нижней сейфовой части размещаются диспенсер и модуль приёма наличных (кеша).

Рис. 1. Иллюстрация одного из случаев механического воздействия – разрушение банкомата

Криминальные случаи все ещё происходят, однако их число заметно сократилось. Сократилось и время регламентного обслуживания банкоматов: теперь для этого не закрывают отделение банка и не ограничивают доступ. Регламентные работы специалист проводит за 7–10 минут (рис. 2).

С точки зрения безопасности – это самая критичная часть в возможном несанкционированном использовании банкомата. Однако, поскольку большинство банкоматов установлены в помещениях банков (отделениях), предполагается, что уровень безопасности специалиста во время регламента обеспечен всесторонне, как и защита «открытого» во время работы банкомата со

Рис. 2. Иллюстрация регламентных работ в открытой зоне

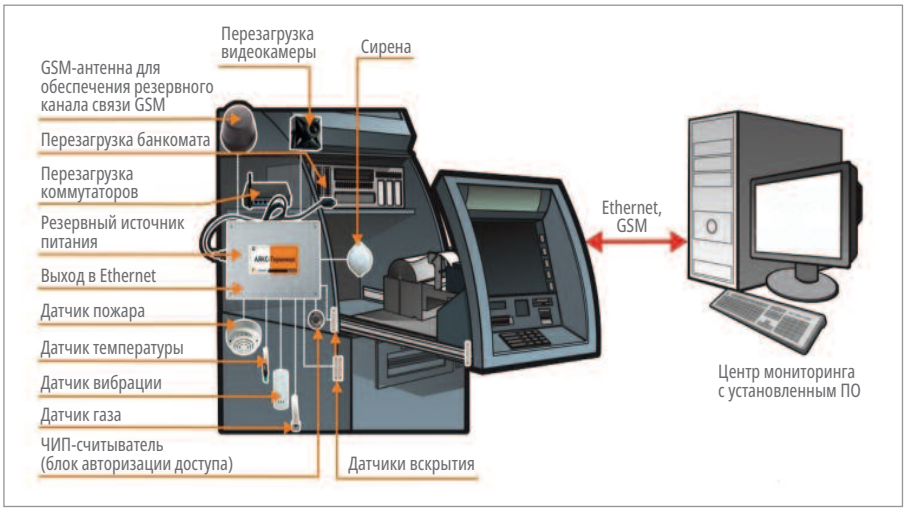

Рис. 3. Основные узлы и элементы безопасности типичного банкомата

всем его содержимым. Для понимания этих особенностей рассмотрим типичную архитектуру банковской системы управления на примере АСУ «Банкомат» (таких систем несколько).

Типичная архитектура АСУ и взаимосвязи банк-терминал

На рис. 3 представлены основные узлы и элементы безопасности типичного банкомата, а также иллюстративно – канал связи с сервером через Интернет.

Недалеко от передней стенки банкомата установлены датчики открытия и электронный вибродатчик «Шорох-2». При формировании сигнала тревоги он поступает в Fast Ehternet концентратор 10/100 Мбит и немедленно передаётся через радиоканал сотовой связи. При этом видеозапись с помощью видеорегистратора Mitsubishi Electric DX-TL304, установленного фронтально (камера направлена на пользователя банкомата) осуществляется постоянно, и запись видеопотока идёт на встроенный носитель памяти объёмом более 1 Тбайт. Поэтому даже при глушении сигналов сотовой связи запись остаётся в банкомате в цифровом виде. Наиболее популярные банкоматы, используемые в современных кредитных организациях, принадлежат к модельному ряду NCR (фирма-производитель) и имеют модели Self-Serf6632 (наиболее популярна в Сбербанке), мощность потребления 750 Вт/ч, а также модели для разного (уличного, встраиваемого и офисного) назначения, установки NCR5886 (вес 895 кг), NCR6676 (744 кг), NCR6631 (895 кг) и другие [1]. Поднять такое оборудование затруднительно, для установки банкомата используют труд 6 такелажников. Поэтому случаев механического повреждения и разрушения такого оборудования больше, чем случаев кражи и перемещения самих банкоматов. Защитная система типа АТ-433 (Lonta-202) работает по принципу радиоканальной СПИ в открытом канале 433 МГц мощностью 10 мВт и обеспечивает уверенную дальность распространения сигнала в зависимости от местности и прохождения радиоволн в радиусе 3…7 км. Вариативно и опционально используется оборудование Lohta Pro с радиусом 10…50 км, с действием на другом частотном диапазоне 403…479 МГц мощностью 5 Вт. Есть возможность использовать эти дублирующие сигнал тревоги системы одновременно. Тревожный сигнал поступает на пульт централизованной охраны вневедомственной охраны Росгвардии и в службу безопасности банка – с использованием модема сотовой связи и посредством сети Интернет. На рис. 4 представлена иллюстрация взаимодействия в цепи «кредитная организация (банк) – банкомат» посредством спутниковой связи (Интернет через спутник). Оба канала – сотовая связь с помощью модуля IMEI и привязки SIM и спутниковый Интернет – дублируют друг друга.

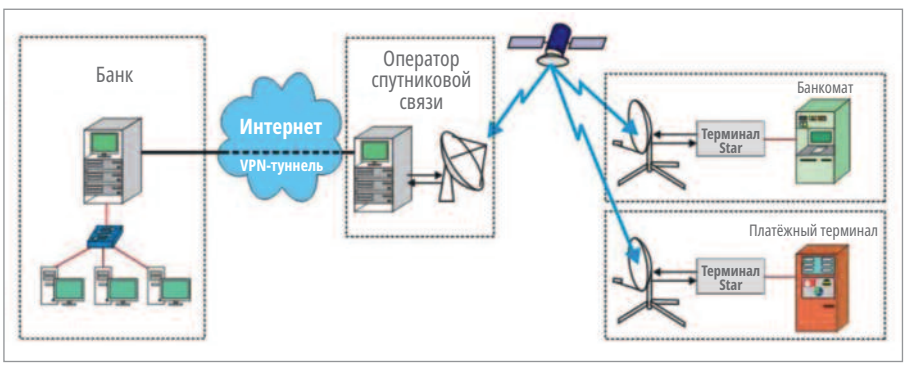

Рис. 4. Взаимодействие в цепи кредитная организация (банк) – банкомат посредством спутниковой связи

Фото: Максим Богодвид / РИА Новости

Рис. 5. Внешний вид сейфа диспенсера

Рис. 6. Внешний вид кассет для банкомата NCR

Внешний вид сейфа диспенсера представлен на рис. 5. Внешний вид кас-

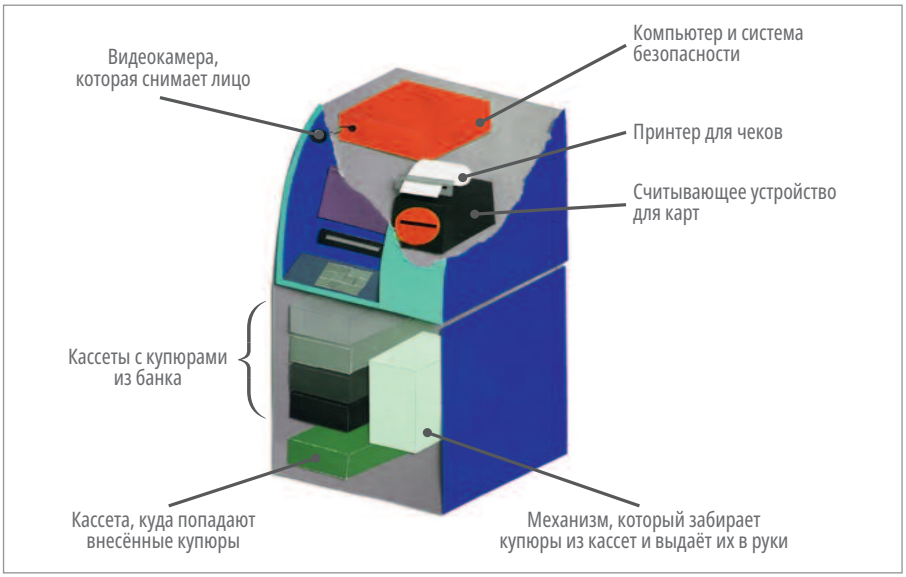

Рис. 7. Общий вид типичного банкомата

сет для банкомата NCR представлен на рис. 6.

Устройство для выдачи купюр – диспенсер состоит из презентера – верхнего модуля, через который происходит автоматическая выдача купюр клиенту, и модулей, в которые вставляются кассеты – одна с купюрами, другая пустая, называемая режект-кассетой. На каждый номинал купюр – свои кассеты. В кассету можно загрузить до 2000 купюр. Для извлечения купюр из кассет фрикционным методом используют ролики (альтернативно используется вакуумный метод – «метод присоски»). В разных типах банкоматов используются разные методы, но можно с уверенностью заявить, что в России по стандартам принят первый способ – фрикционный. Поэтому визуально можно наблюдать, что разнообразие моделей банкоматов в России невелико и ограничено определёнными типами. Стандартный банкомат (терминал), ориентированный только на выдачу, не верифицирует ни номинал купюр (забирая их для выдачи из конкретной кассеты), ни их подлинность; оба эти фактора в зоне ответственности только персонала банка. Поэтому для пущего контроля кассеты заряжают в присутствии двух сотрудников банка. Сотрудники инкассации доступа к купюрам (к открытию кассеты) не имеют.

По линии (пути) следования купюр от кассеты к презентеру (к клиенту) процесс контролируют несколько (обычно 4) электронных датчиков. Если купюра, предназначенная для выдачи, замялась или криво лежит – она автоматически отправляется в режект-кассету. Туда же попадают и забытые клиентом в презентере деньги. В банкоматах, осуществляющих не только выдачу, но и приём купюр – с кэш-ресайклингом (раскроем их значение ниже), производится определение номинала купюр и их подлинность по нескольким критериям. Поэтому банкоматы с ресайклингом более надёжны, но и более дорогостоящи; их в России в разы меньше, чем банкоматов «типичных», ориентированных только на выдачу денежных средств. Не будем путать те и другие с терминалами оплаты, принимающими купюры, столь популярными в Сбере, – это отдельный сегмент банковского оборудования.

Общий вид типичного банкомата представлен на рис. 7. Одно из заслуживающих интереса относительно новых (12 лет в России) устройств, появившихся в современных банкоматах, – бесконтактный модуль считыватель – картридер NFC ViVOPay Kiosk-III (рис. 8). Применение этого устройства дало возможность считывать банковские карты бесконтактным способом, без «прокатки» карты в устройстве стандартного картридера. Отчасти поэтому клиенты стали чувствовать себя более уверенно – пластиковую карту банкомат не может задержать или «съесть», и установка защитных экранов против скимеров карт в таких условиях также потеряла актуальность. С применением бесконтактного способа считывания банковской карты некоторая опасность её несанкционированного копирования сохраняется, так что полностью все риски пока снять невозможно. Однако с появлением автоматизированной системы управления «Банкомат» и аналогичных риски пользования банковскими инструментами несколько уменьшились.

Рис. 8. Картридер NFC ViVOPay Kiosk-III

Функции АСУ «Банкомат»

Важные функции АСУ «Банкомат»:

- мониторинг, позволяющий отслеживать состояние кэш-поинтов (точек обслуживания), объёмы наличности и сроки инкассации;
- учёт повышающих коэффициентов на услуги СИ в праздничные и выходные дни;
- возможность размещения кэш-поинтов в различных часовых поясах.

Инструменты и возможности АСУ «Банкомат» для банковской сферы представлены на рис. 9.

Так выглядит современная комплексная автоматизация управления наличностью. Упрощённое планирование инкассаций с использованием автоматизированной системы позволяет повысить эффект системы управления наличностью примерно в 4 раза [5]. В настоящее время в России АСУ «Банкомат» используется в сети, объединяющей более чем 8000 банкоматов и несколько сотен кассовых терминалов. По сути, это единый продукт, усовершенствованный с помощью многолетнего накопленного опыта в разных кредитных организациях (банках). Кроме того, что АСУ может работать на любом системном ПО, в том числе «свободном», SAP сертифицирована для работы в SAP Cloud Platform, она также включена в Российский реестр отечественного ПО как система, предназначенная для эффективного управления денежной наличностью. На рис. 10 представлена структура экономического эффекта от использования комплексной автоматизированной системы контроля и обеспечения наличных денег в банкоматах.

Экономический эффект обеспечивается за счёт снижения расходов на фондирование остатков наличности на

Рис. 9. Возможности и перспективы применения АСУ «Банкомат»

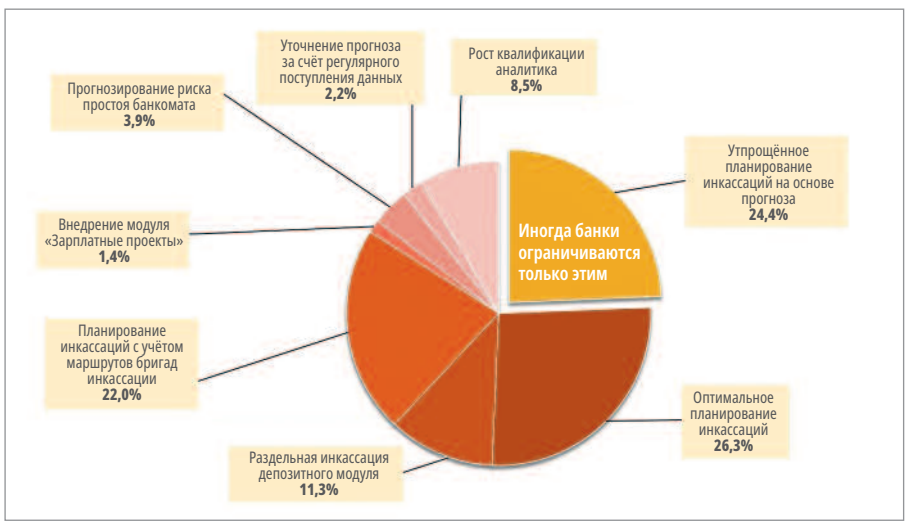

Рис. 10. Структура экономического эффекта кеш-менеджмента

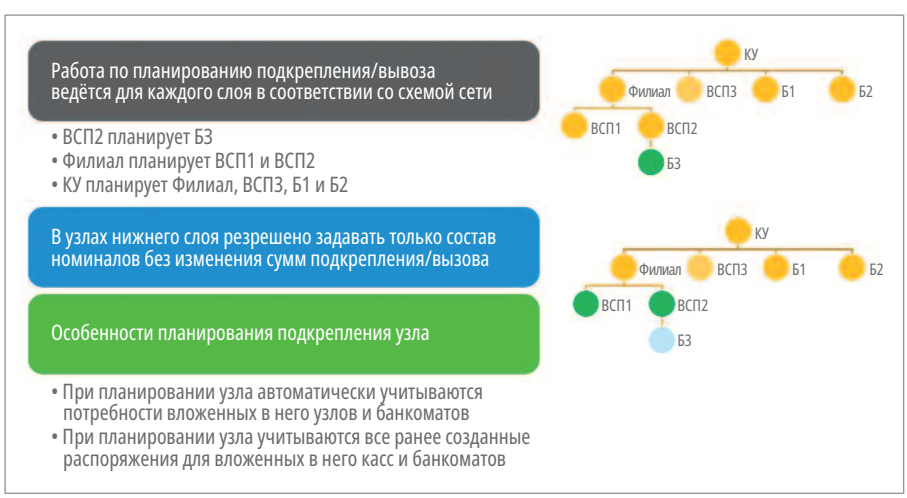

Рис. 11. Иллюстрация формирования и планирования распоряжений на инкассацию

15-25%, снижения количества выездов к территориально удалённым кэш-поинтам, сокращения трудозатрат на ввод и обработку в АБС бухгалтерских проводок и сокращения трудозатрат на актирование услуг сторонних организаций. Подтверждённый специалистами эффект – свыше 4 тыс. рублей в месяц на один банкомат (48 тыс. рублей в год) или от 45 тыс. рублей в месяц на одну кассу (540 тыс. рублей в год) [5]. Дополнительный эффект наблюдают в увеличении количества кэш-поинтов, равномерном распределении нагрузки на сотрудников КУ и инкассаторов, возможности реагирования на изменение макроэкономической ситуации и консолидация разрозненных данных из других электронных систем банковской организации.

Особенности АСУ «Банкомат»

Из выдающихся положительных свойств новой системы отметим настройку – планирование инкассаций и особенности формирования «остатков» банковской наличности на конец дня (настраиваемого периода), когда информация формируется автоматически и в виде: реальный остаток и загрузка, предложенная системой, – прогнозируемая выгрузка – фактический клиентский оборот. Также доступны настройка экономических параметров и расписаний и загрузка исторических данных. Удобно и то, что наряду с набором экономических параметров в автоматическом режиме предоставляется статистика (остатки и данные об инкассациях) за 6 месяцев.

Состояние банкомата постоянно анализируется с помощью самотеста, заявки (с подробностью необходимых пополнений разными купюрами) на инкассацию конкретного банкомата или сектора обслуживания (нескольких банкоматов) формируются автоматически и передаются в формате отчёта на пункт диспетчерского контроля за сутки. Это позволяет своевременно формировать фактические заявки в службу инкассации. Автоматизация обработки распоряжения на инкассацию обеспечивает снижение нагрузки на персонал и автоматическое актирование услуг внешних средств обеспечения. Система формирует распоряжение на инкассацию на основе плана инкассаций и по запросу аналитика. Оператор-аналитик в центре управления может откорректировать распоряжение на инкассацию, опираясь на аналитические данные и статистику, полученную в автоматическом режиме отчёта от АСУ «Банкомат», причём частоту отчёта можно программировать дистанционно. Так, на основе данных о клиентском расходе формируется и его прогноз, а соответственно, и график инкассаций.

Иллюстрация формирования и планирования распоряжений на инкассацию представлена на рис. 11.

При планировании учитывают информацию о заявках клиентов на снятие наличных, потребностях обслуживаемых (вложенных) касс и банкома-

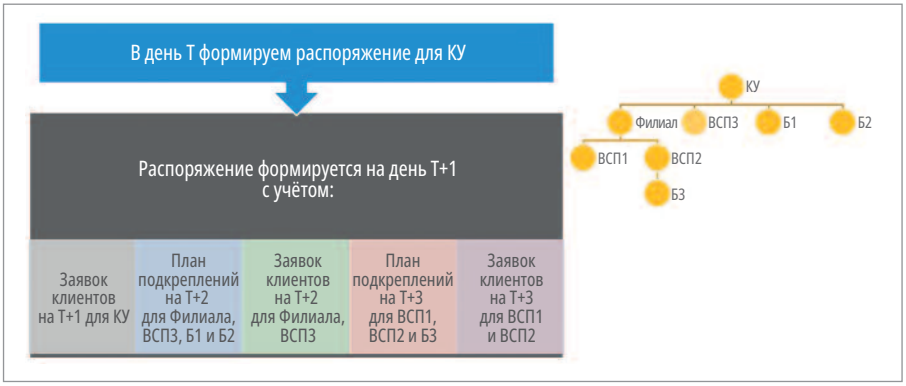

Рис. 12. Принципы планирования обслуживания банкоматов

тов, распоряжения на инкассацию банкоматов и подкрепление касс, находящиеся на этапе исполнения, статистику по клиентским операциям в кассах. На рис. 12 подробно обозначены принципы планирования обслуживания банкоматов.

Из этого следует, что одна касса может иметь несколько источников подкрепления наличностью, а «топология» сети касс может иметь несколько уровней (корпоративное управление КУ – филиал – дополнительный офис). Обеспечение бесперебойного функционирования сети кэш-поинтов обеспечивается на этапах от формирования распоряжения, ввода результатов формирования кассет, контроля расходной КО до передачи в автоматизированную банковскую систему (АБС) данных для формирования расходных ордеров. Формирование и обработка распоряжения на инкассацию последовательна: от передачи в АБС информации о поступлении наличности, фактической доставки наличности в банкомат и до зачисления поступивших средств на счёт банкомата в АБС [5].

Планирование работы современных банкоматов с кэш-ресайклингом существенно отличается от планирования банкоматов, работающих только на выдачу денежных средств. Автоматизированная система контроля качественно решает и эту задачу. К слову, ресайклинг, или рециклинг (recycling), в буквальном переводе с английского, – это «повторное использование». Тезис и термин задействован не только в банковской сфере и с годами набирает всё бóльшую популярность на манер «доходы из отходов». В банковской сфере термин имеет специальное значение, а именно: банкоматы с ресайклингом осуществляют почти все виды финансовых операций, а особенностью является поддержка выдачи денежных средств из принятых, без промежуточного этапа инкассирования.

Особенности механизма аутентификации

Механизмы аутентификации обеспечиваются поддержкой AD FS (Microsoft Active Directory Federation Services) и механизма SSO. Технология единого входа SSO (Single sign-on) – это метод аутентификации, позволяющий пользователям безопасно аутентифицироваться одновременно в нескольких приложениях и сайтах, используя один набор учётных данных. Авторизация действий пользователя выполняется на уровне серверной бизнес-логики на основе механизма сквозной авторизации. Управление видимостью кэш-поинтов и объектов внутренних структурных подразделений (ВСП) и с использованием списка управления доступом ACL (Access Control List), определяющим доступность к объекту (программе, процессу или файлу) [1]. Аудит событий обеспечивается электронной фиксацией всех действий пользователя, влияющих на результаты планирования инкассаций, возможен просмотр событий в разрезе кэш-поинтов, системных событий, дат конкретных транзакций и данных профилей пользователей. На рис. 13 представлена схема внешней архитектуры [5].

Таким образом обеспечена прозрачная интеграция с большим количе-

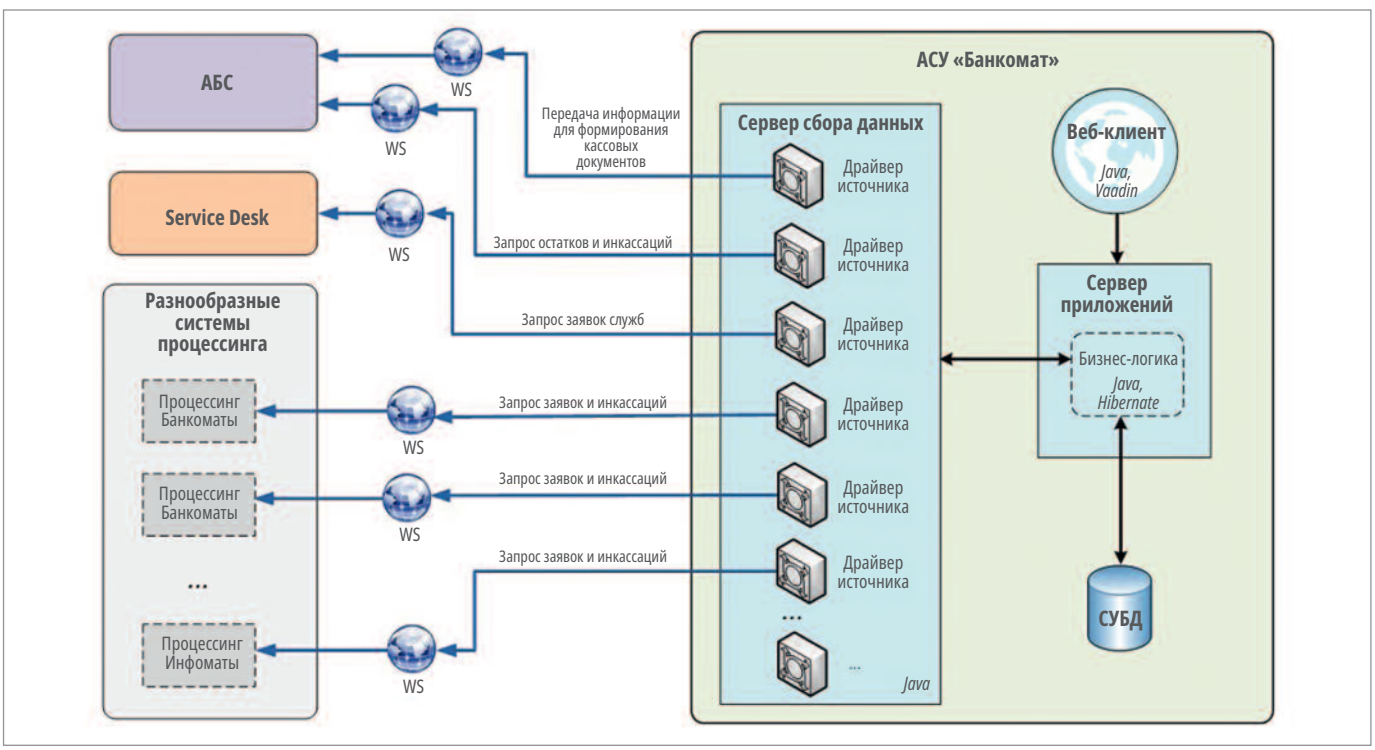

Рис. 13. Схема внешней архитектуры для АСУ в банковской сфере

ством внешних систем, устойчивых к внешним санкциям и ограничениям, так как можно использовать коммерческое и свободное системное ПО от разных поставщиков.

Плюсы многоуровневой архитектуры

Плюсы многоуровневой архитектуры для автоматизированных банковских терминалов и устройств в её доступном и расширенном функционале (дополнительная отличительная черта – хорошая масштабируемость и высокая производительность):

- СУБД (MS SQL Server, или Oracle, или PostgreSQL, или SAP HANA)
- Сервер приложений (любой, совместимый с Apache Tomcat)
- Серверная бизнес-логика (на Java)
- Презентационный уровень (веб-клиент)

Использование только открытых технологий и стандартов предполагает возможность внедрения облачного сервиса:

- Java-технологии в основе системы
- Серверная бизнес-логика использует Hibernate, Vaadin
- Система отчётности: Jasper Reports

Далее рассмотрим некоторые особенности электронного банковского оборудования.

Подключение купюроприёмника по протоколу Pulse

На примере купюроприёмника для вендингового оборудования и для систем автоматических депозитариев типа Alagard рассмотрим работу устройств по протоколу Pulse. На рис. 14 представлен вид купюроприёмника, а на рис. 15 – схематичное расположение его частей.

Рис. 14. Внешний вид купюроприёмника

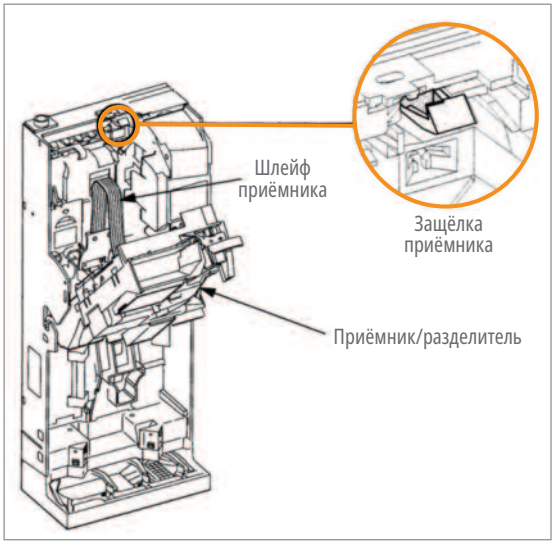

Рис. 15. Схематичное расположение элементов купюроприёмника

В корпусе купюроприёмника расположены 2 колодки микропереключателей-джамперов: большая SW1–SW8 и малая SW1–SW4. В комплекте для подключения купюроприёмника к автомату имеется гибкий шлейф WEL-RV701. С одного конца шлейф имеет продолговатую разъёмную колодку 2×15 выводов, с другой стороны – разъём 3×3. При первом включении все микропереключатели SW1–SW8 устанавливают в положении OFF при подключённом на штатном месте стекере (бокс для денег). Мощность источника питания не менее 36 Вт. После подключения питания («плюс питания» к контакту «+12V», общий провод – GND) КП проведёт самодиагностику и выйдет в «Режим 1» (при исправном купюроприёмнике – начальный режим): светодиоды на лицевой панели купюроприёмника не горят, купюры не принимаются, 2 раза мигает светодиод, расположенный на задней части КП. Это означает, что купюроприёмник работает, но заблокирован. «Режим 2» доступен после программирования с помощью SW1–SW8: светодиоды на лицевой панели купюроприёмника мигают, купюры принимаются [2]. Для перевода купюроприёмника в протокол PULSE в передней нижней части устройства необходимо сдвинуть крышку (по направлению указанной стрелки) колодки микропереключателей SW1–SW4. Переключатель SW2 переводят в режим ON (Pulse Mode). Дальнейшая настройка устройства зависит от одной из трёх типичных схем управления. Под каждую из них можно настроить купюроприёмник с помощью DIP-микропереключателей (джамперов). Если DIP SW1 в положении ON (Credit-Pulse Normal HIGH), на выводе Signal купюроприёмника постоянно будет присутствовать высокий логический уровень, а в момент внесения (приёма) купюр на этом выводе уровень меняется на низкий. Такова наиболее популярная схема взаимодействия. В большинстве случаев применяют настройку: SW1 и SW2 микропереключатели в состояние ON, а SW3 и SW4 – в OFF. Для противоположной реакции устройства – в режиме покоя низкий уровень, а при внесении купюр – высокий SW1 устанавливают в положение OFF (Credit-Pulse Normal LOW). Подробнее об этом в [7]. Схема подключения подходит к купюроприёмникам ICT U70, P70, B70 и аналогичным. Подключение других купюроприёмников, работающих в протоколе PULSE, аналогично, однако цвета проводов в шлейфе подключения могут отличаться. Типично разрешение на приём купюр управляется состоянием низкого логического уровня («минусом» питания). У устройства есть управляющий выход «INHIBIT» – функция и одновременно контактный вывод для запрета/разрешения приёма купюр. Для управления высоким логическим уровнем необходимо перевести микропереключатель SW8 в положение ON (Inhibit Active HIGH). Если на выход «INHIBIT» (зелёный провод) купюроприёмника подавать низкий логический уровень, запрет на приём купюр будет снят. В ином случае купюроприёмник будет заблокирован. В управлении аналогичных по принципу работы купюроприёмников может быть задействована другая схема управления (к примеру, если для устройства не предусмотрен выход «INHIBIT»): зелёный провод подключают постоянно к общему проводу, а переключатель SW8 устанавливают в положение OFF (Inhibit Active LOW), при этом жёлтый провод подключают к выходу «INHIBIT».

Типичная схема подключения описана далее.

Типичная схема и варианты подключения

Электропитание устройства («автомат») и КП осуществляется от одного (общего) источника питания, иначе совместная работа устройств не гарантируется. Красный провод подключается к «плюсу питания» +12 В; оранжевый GND, зелёный и фиолетовый – к «общему проводу». Для обеспечения посто-

Таблица 1. Сведения об ошибках системы с их расшифровкой

Светодиод горит постоянно	Купюроприёмник исправен
1 вспышка	Замятие купюры
2 вспышки	Заблокирован
3 вспышки	Проблема с сенсорами распознавания
3+2 вспышки	Проблема с механизмом «антифишинга»
4 вспышки	Проблема с датчиком «Антилеска»
5 вспышек	Отсутствует стекер
6 вспышек	Неисправен или заполнен стекер
7 вспышек	Ошибка электропривода

Рис. 16. Автоматический депозитарий типа Alagard

янного сигнала высокого уровня жёлтый подключается к «плюсу питания» +12 В через ограничительный резистор 1 кОм. Этот вывод «INHIBIT+» отвечает за блокировку/разрешение приёма купюр. На вход «Pulse» поступают импульсы сигналов управления, здесь подключается фиолетовый провод шлейфа. Выход импульсов «Signal» подключают к проводнику синего цвета. Такие особенности необходимо уточнять в документации конкретной модели. Подключения и настройки необходимо производить при отключённом питании купюроприёмника.

Для индикации состояния и ошибок КП используется один зелёный светодиод, расположенный сзади. Подробнее о вариантах подключения в [2]. В табл. 1 представлены сведения об ошибках системы с их расшифровкой.

На рис. 16 представлен вид оборудования, где применяются КП рассмотренного типа.

КП и МП с функцией выдачи сдачи

Купюроприёмник (КП) и монетоприёмник (МП) с функцией выдачи сдачи условно старых типов (выпуска до 2015 года) работали на протоколе MDB (1993 года). Несмотря на условную «древность», Serial-протокол MDB был хорошо защищён и отличается последовательной передачей данных (serial), то есть данные передаются последовательно по каналам «монетоприёмник – автомат» (Tx) и «автомат – монетоприёмник» (Rx). Неудивительно, что почти все вендинговые аппараты работали с интерфейсом Executive. Подробнее о протоколе, взаимодействии с ОС Android в вендинговых аппаратах и программировании можно уточнить в [6, 10]. Протокол можно было бы имитировать (заменить), если бы не минимальная задержка между формированием команды и ответом (не должна превышать 5 мс), иначе контроллер расценивает акцию как ошибку (timeout), а организовать работу с помощью «прерываний» не всем доступно. Но решение и польза есть во взаимозаменяемости модулей C-MDB, работающих даже с последовательным COM-портом.

Особенности современных купюроприёмников

Купюроприёмник (КП) – это платёжный модуль торгового автомата, обеспечивающий идентификацию денежных банкнот. С помощью специального набора электронных датчиков происходит определение подлинности купюр и их номинала. При сравнении используются оптические и магнитные характеристики каждой купюры. Современные КП оснащены функционалом выдачи сдачи из тех же купюр. Преимущества можно обозначить в высокой скорости работы, безошибочной верификации подлинности банкнот, надёжности и долговечности оборудования (средний срок службы составляет 10 лет), устойчивости к нагрузкам, понятному для использования функционалу и возможности установки увеличенной ёмкости для банкнот, а также замке безопасности. Точность проверки подлинности банкнот достигается благодаря набору установленных датчиков, среди которые диэлектрические, ультрафиолетовые, оптические, индуктивные и комбинированные. Устойчивость к постоянным нагрузкам – это важный параметр, определяющий безошибочную верификацию количества купюр, проходящих через устройство в день. Современные модели купюроприёмников на примере устройства «CashCode» и аналогичных способны обработать более 200 000 банкнот разных номиналов в день, что является относительно высоким – по современным требованиям – показателем. Лёгкость при эксплуатации КП в том, что его не нужно программировать или кодировать вручную, так как в комплекте от производителя необходимые прошивки имеются, их можно установить при помощи ПК и флеш-накопителя, непосредственно через слот в КП.

Особенности современных монетоприёмников

Типичное определение монетоприёмника (МП) – устройство, способное при помощи набора электронных датчиков определить номинал и подлинность монеты. Распространены несколько типов МП: компараторный, микроконтроллерный, распределяющий и комбинированный. И каждый тип имеет свои достоинства и недостатки.

Разработки в начале XX века начались в США с создания эталонных монетоприёмников, они функционировали по условно простому принципу. Внутри приёмного модуля расположена монета (эталон, ординар), её физический вес известен, и он электронным методом сравнивается с принимаемой в оплату товаров или услуг монетой. К примеру, таким образом функционировали «автоматические» системы проигрывания музыки, заменившие тапёров в тавернах и ресторациях. Затем систему усовершенствовали. При прохождении другой монеты через рабочую зону датчика индуктивности происходило сравнение электромагнитных параметров обеих монет по условию: заброшенная монета является подлинной, если её параметры максимально близки к эталонной монете [6]. В МП устанавливали простейшие элементы безопасности, такие как защита

от «монеты на нитке/леске» (способ получил название «зимняя рыбалка»), и механизм, осуществляющий возврат монеты в случае, если она не была определена датчиком.

Подробности разных способов «работы с банкоматами», а в частности, проблемное поле относительно пластиковых банковских карт предложил ещё в 2001 году финский правозащитник Йохан Бекман (ныне и давно живущий в Москве). Доцент социологии права в 1995–2001 годах работал научным сотрудником в криминологическом отделе научно-исследовательского института правовой политики при министерстве юстиции Финляндии и позже в книгах отразил полученный опыт [4]. Под защитой от «рыбаков» понимается механизм, исключающий возврат монеты путём вытягивания за привязанную нитку. Главная проблема электронного компаратора в основе МП состоит в неспособности определять более одного номинала монеты. Эталонные МП такого типа можно встретить в «дозировочных» (вода, лимонад) или ранее – в игровых автоматах.

Второй тип монетообрабатывающих устройств идентифицирует монету с помощью запрограммированного устройства, в электронной памяти которого заложены необходимые данные о характеристиках разных монет. Можно получить для идентификации и сравнения геометрические размеры монеты (диаметр, толщина), вес и электромагнитные параметры монеты (к примеру, проницаемость). Распределяющий или сортировочный тип МП используют в торговых автоматах, в том числе осуществляющих выдачу вещей и продуктов в упаковках (бутылки и банки с напитками, шоколадные батончики и др.), для выдачи сдачи. При распределении монет каждый номинал хранится отдельно в специальных трубках, в случае переполнения которых происходит сброс в общую ёмкость. Комбинированный МП по определению сочетает следующие возможности: идентификация монет, распределение монет по номиналам, возврат монет в случае несоответствия, выдача сдачи в корректной форме. Такой МП использует электронный (с помощью датчиков, формирующих сигнал на микроконтроллер) способ идентификации, оправданный при необходимости работы с монетами разных номиналов. После определения подлинности монета попадает в соответствующую трубку, а при отрицательном результате идентификации возвращается через специальный канал. Сдача рассчитывается и формируется порционно с помощью электронного устройства – диспенсера для монет или хоппера.

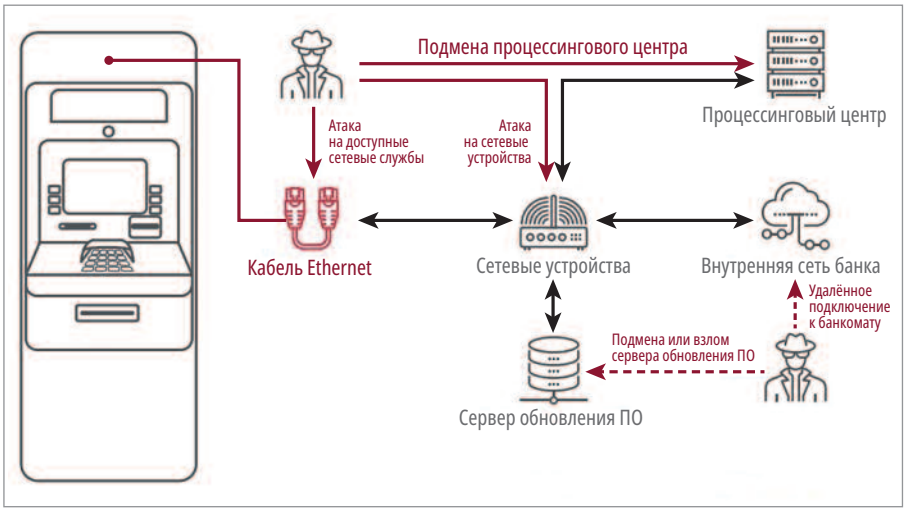

Рис. 17. Сценарии логических атак на банковское оборудование

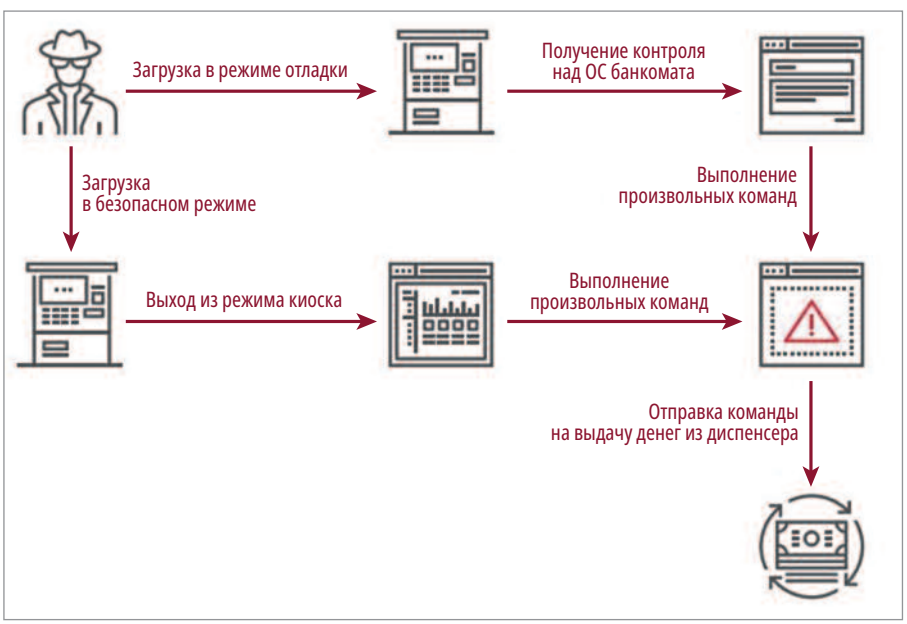

Рис. 18. Вариант сценария атаки на банковское оборудование

Особенности, выводы, перспективы

Сегодня и всегда вопрос безопасности транзакций весьма актуален. Сценарии логических атак на банковское оборудование (рис. 17, 18) изменяются и совершенствуются параллельно с совершенствованием защитных функций [4]. Эта «конкурентная борьба» будет всегда. Поэтому все результативные меры защиты – комплексные. О том, как было бы безопасно работать с банкоматом, на который можно было бы свалить всю ответственность за ошибки человеческого фактора, вспомним, обратившись к иллюстрации на рис. 19. Совершенно понятно, что такое в нынешних реалиях уже невозможно – прогресс и эволюция не имеют обратного хода. Поэтому конкурентная борьба разработчиков систем банковского оборудования сегодня происходит по нескольким направлениям. Пытаются удешевить конструкции с сопоставимым качеством исполнения (надёжностью, требованиям к верификации купюр), форм-фактором и, главное, функционалом. Проблемными вопросами остаются возможные погрешности при распознавании купюр с незначительными повреждениями, погрешности при идентификации банкнот и механическое несовершенство приёмных узлов, ведущее, к примеру, к застреванию купюр в КП.

Средняя скорость обработки банкноты, по современным требованиям, не более 2 секунд, в то время как у банко-

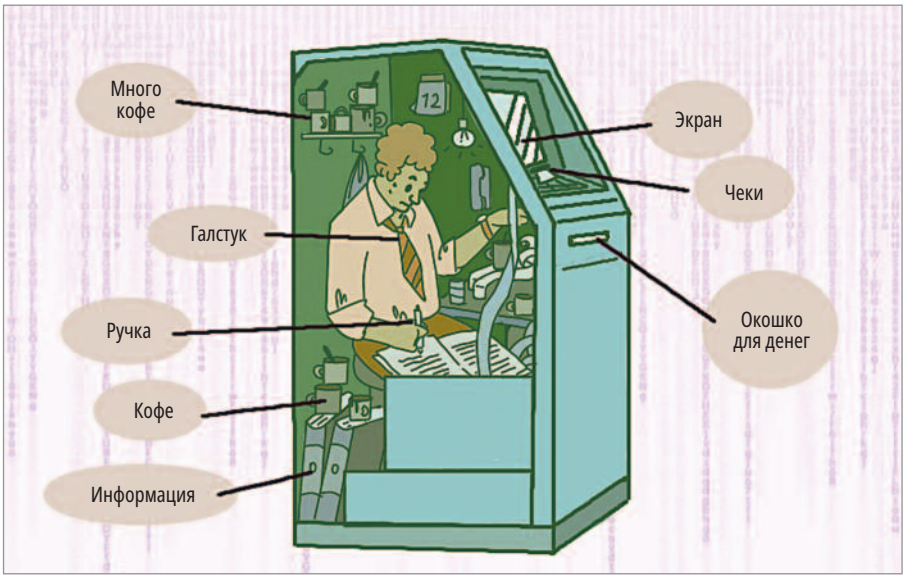

Фото: https://habr.com/ru/companies/gazprombank/articles/654235/

Рис. 19. Безопасный банкомат

матов (оборудования) старых типов, к примеру, с купюроприёмниками Cashflow 560, она в 2–3 раза дольше. Один из трендов развития КП в сфере услуг направлен в сторону уменьшения сроков корректной верификации принимаемых денежных знаков (для МП это касается монет и жетонов соответствующего назначения, к примеру, метро), идентификации купюр, расчёта и быстрой выдачи сдачи или заявленной пользователем суммы.

Ещё одна любопытная особенность состоит в том, что банкоматы серверы в системе накопления данных объединяют в сеть сотни камер банковских терминалов, а сами видеокамеры уже несколько лет доступны в режиме реального времени аттестованным сотрудникам специальных служб. Образно говоря, камера банковского терминала, установленного в магазине, обращённая ко входу, в реальном времени (при условии стеклянных входных дверей) считывает «картинку» того, что происходит в кафе через улицу напротив магазина. Да, качество картинки оставляет желать лучшего, но силуэты на таком расстоянии она различит. Все эти данные, за неимением более качественных и достоверных, могут являться доказательной базой и corpus delicti. Кроме того, серверы, аккумулирующие видеоконтент с камер, установленных в корпусе банкомата, сохраняют данные не менее чем 3 месяца.

Мы показали актуальные особенности и риски применения РЭА, сконструированной для банковской сферы. В этой области особое значение придаётся внедрению комплексных процедур контроля наличности в банкоматах, электронных способов и автоматических алгоритмов обеспечения для граждан высокого качества жизни и безопасности транзакций, работы с деньгами.

Несмотря на многочисленные анонсы философов и досужие размышления о ненужности денег и всеобщем безденежном «рае», купюры и монеты как средство универсального платежа пока ещё никто не отменял. Этого пока не предвидится. ●

Литература

1. Аксессуары для банкомата Fujitsu F53, F56. URL: https://russian.alibaba.com/product-detail/ATM-machine-spare-parts-accessories-Fujitsu-1600495768124.html.
2. Инструкция подключения для купюроприёмников типа ICT. URL: https://super-automat.ru/docs/ICTA7V7BS7manual.pdf.
3. Коммуникационный протокол MDB. URL: https://smartpossdk.gitbook.io/cloudpossdk/cloudpos-sdk/mdb-communication-protocal.
4. Преступления, связанные с платежными картами: Исследование злоупотреблений с банковскими и кредитными картами и обвиняемые в этих злоупотреблениях / пер. с фин.; А. Киннунен, Х. Ниеми, Р. Сирен. СПб.: Институт Йохана Бекмана, 2001.
5. Система кэш-менеджмента «АСУ Банкомат». URL: https://servicemodel.ru/bankomat./
6. Хопперы и монетоприёмники. URL: https://sensis.ru/cat/sale/komplektuyuschie/hoppery-i-monetopriemniki/.
7. *Экземплярский В.* Биометрические системы, информационные киоски (БИК), турникеты и шлюзы с АСО. Обзор оборудования, компонентов и особенностей установки. URL: https://www.cta.ru/articles/cta/obzory/tekhnologii/169244/.

кордер через переднюю панель FMC-субмодуля TORNADO-FRS1 и поддерживает «горячую» замену без выключения питания AMC-модуля рекордера. Длительность записи/воспроизведения для картриджа 8 Тбайт составляет около 4 ч 40 мин для потока одноканального АЦП/ЦАП 16 бит 250MSPS или квадратуры 16 бит 125MSPS и 1 ч 10 мин для потока 16 бит 1MSPS.

Форматы потоков данных рекордера для АЦП/ЦАП выбираются из 16, 8, 4, 2 или 1 бит в соответствии с требованиями конкретного приложения и соотношения точность-длительность. Входные и выходные потоки данных рекордера коммутируются с AMC-портов 4-7/8-11 Fabric-DEFG стандартов AMC.2 Ethernet, AMC.1 PCIe или AMC.4 Serial RapidIO, которые маршрутизируются к другим AMC-модулям ЦОС (TORNADO-A6678/FMC, TORNADO-AZU+/FMC+ и др.) в шасси MicroTCA/iMTCA с установленными на них FMC-субмодулями АЦП/ЦАП.

Рекордер TORNADO-ARS1 управляется по интерфейсу 1GbE Ethernet через AMC-порты 0–1 Fabric-A как дистанционно с ПК и устройств Android через сети LAN/WAN, так и локально от других AMC-модулей TORNADO-A и модулей MCH/iMCH фирмы МикроЛАБ Системс внутри шасси MicroTCA/iMTCA, причём пользователь может также создавать свои собственные управляющие приложения.

При необходимости фирма МикроЛАБ Системс может модифицировать ПО рекордера TORNADO-ARS1 в соответствии с требованиями заказчика.

Дополнительные конфигурации рекордера используют в качестве «несущего» высокопроизводительные AMC-модули ЦОС TORNADO-A6678/FMC и TORNADO-AZU+/FMC+, что позволяет совместить функции ЦОС и рекордера в одном AMC-модуле и повысить пропускную способность сменного носителя.

Вся продукция фирмы МикроЛАБ Системс разрабатывается и производится на территории РФ и имеет пожизненную гарантию и техническую поддержку.

http://www.mlabsys.ru
+7(499) 900-6208
info@mlabsys.ru