Насколько и как надо защищать банкоматы, до сих пор остается вопросом дискуссионным, особенно в свете требований к защите критических информационных инфраструктур (КИИ)[1]. Обычно защищается канал между процессинговым центром и компьютером банкомата, и того, как он защищается, зачастую недостаточно для удовлетворения требований к КИИ. В статье описаны средства, при помощи которых можно защитить каналы как от процессингового центра к компьютеру, так и от компьютера к диспенсеру и обеспечить целостность программно-аппаратной среды компьютера.

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

Возможные атаки

1. Атака на канал взаимодействия с процессинговым центром.

Атака может быть реализована примерно так: вставляется любая карточка, вводится любой PIN, из процессингового центра приходит сигнал отказа в авторизации, но он подменяется сигналом успешной авторизации. При этом злоумышленнику достаточно иметь возможность вмешаться в работу канала, изменять логику работы банкомата необходимости нет.

2. Атака имитацией сигнала на выдачу денег.

Команда на выдачу денег, которую исполняет диспенсер, формируется компьютером банкомата. А почему бы тогда злоумышленнику не использовать другой компьютер? Например, принести с собой ноутбук, отключить USB-кабель диспенсера от компьютера банкомата, подключить его к принесенному ноутбуку и подавать команды вида «дай 5000 рублей»? Естественно, диспенсер выполнит команду,

Светлана КОНЯВСКАЯ, *ОКБ САПР, заместитель директора*

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Закон о КИИ).

Светлана КОНЯВСКАЯ

если ее подать в нужном формате. Но это, конечно, дело техники и никакого труда не представляет.

Эта же атака может быть реализована и по-другому. Так, злоумышленник может внедрить закладку в компьютер банкомата (это несложно сделать, например, при выполнении профилактических работ). Логика работы вредоносной программы может быть любой: например, при предъявлении определенной легальной карты может запрашиваться подтверждение на выдачу 100 руб., а выдаваться вполне может значительно больше.

Казалось бы, разные атаки, но они отличаются только нюансами реализации. Суть одна — на диспенсер подается команда, сформированная нештатными программными средствами.

3. Атака имитацией сигнала на прием денег.

Можно смоделировать следующую несложную, но очень опасную атаку: предположим, клиент вносит 100 руб., а действиями закладки на его счет заносится значительно большая сумма, например 100 000 руб. Даже не ясно, можно ли будет этого клиента привлечь к ответственности (если поймают) — денег-то он не брал.

В части защиты сетевой коммуникации все специфичное в требованиях к КИИ сводится к тому, что при взаимодействии с использованием сетей общего доступа каждый узел должен быть защищен СКЗИ высокого класса.

4. Сбор критичной информации пользователей.

Если вредоносная программа внедрена, то что может помешать ей запомнить все номера карт и PIN в один день и все запросы на выдачу денег повторить в другое время по внешней команде — например, по предъявлении какой-то конкретной карты? Или просто передать эту информацию злоумышленникам?

Представляется, что такое перечисление возможных атак уже содержит ответ на извечный вопрос «Что делать?». Надо защитить каналы — как от процессингового центра к компьютеру, так и от компьютера к диспенсеру — и обеспечить целостность программно-аппаратной среды компьютера.

В действительности, как правило (не станем утверждать, что всегда), защищается только канал между процессинговым центром и компьютером банкомата. И того, как он защищается, зачастую недостаточно для удовлетворения требований к КИИ.

Фактически в части защиты сетевой коммуникации все специфичное в требованиях к КИИ сводится к тому, что при взаимодействии с использованием сетей общего доступа каждый узел должен быть защищен средством криптографической защиты информации (СКЗИ) высокого класса. Все остальное — следствия из этого обстоятельства или детали сертификационных требований.

Применение СКЗИ высоких классов предписано и отраслевыми стандартами финансовой сферы. Так, согласно п. 3.1 Положения

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

№ 683-П[1], системно значимые кредитные организации, а также кредитные организации, значимые на рынке платежных услуг, должны *реализовывать усиленный уровень защиты информации* по ГОСТ Р 57580.1-2017[2]. В данном ГОСТе *для усиленного уровня защиты информации предписывается использование СКЗИ, имеющих класс не ниже КС2*. Эти требования в первую очередь касаются именно контуров банковской инфраструктуры, предназначенных для банкоматов, взаимодействия с территориальными отделениями и других коммуникаций.

Как оборудовать каждый банкомат СКЗИ, сертифицированным на высокий класс?

Неприемлемо использовать для этого установленный на компьютер в банкомате программный VPN. Даже в случае, если для него создана и поддерживается среда функционирования криптографии (СФК), это неприемлемо потому, что при обслуживании в ПО этого компьютера могут быть внесены изменения, нарушающие СФК, а проведение в каждом случае соответствующих проверок просто невозможно организационно, работа остановится. Более того, нет никаких гарантий, что непредсказуемые изменения — например, замена компьютера на свой, специальный, — не будут произведены злоумышленником при работах вообще не с компьютером, а, например, с диспенсером.

Ситуация выглядит несколько лучше при использовании аппаратного шлюза, однако, если смотреть правде в глаза, отечественные сертифицированные устройства в этом качестве не используются, поскольку они дороги, избыточны по своим характеристикам, очень велики по размеру и подвержены множеству уже хорошо разработанных и постоянно появляющихся новых атак.

Использование же импортных устройств подходящего размера неприемлемо по причине их несоответствия требованиям регуляторов.

Выполнение еще одного требования регулятора к СКЗИ высокого класса — работа с неизвлекаемым ключом — в КИИ также характеризуется существенными особенностями.

«Неизвлекаемость» — это свойство, описывающее связь ключа с некоторым его физическим хранилищем, то есть, говоря о том, что ключ

Модуль работы с неизвлекаемым ключом в таких технических средствах, как банкомат, должен быть реализован как часть резидентного компонента безопасности, размещенного непосредственно на плате компьютера, а не как отчуждаемый персональный носитель ключа.

[1] Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

[2] ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Светлана КОНЯВСКАЯ

неизвлекаем, необходимо уточнять, откуда. Неизвлекаемые ключи обычно неизвлекаемы из токена, который, как правило, представляет собой USB-устройство, смарт-карту или Touch Memory. О реализации этого требования в документах на СКЗИ для защиты канала высоких классов сертификации сообщается следующее: «Требование неизвлекаемости ключа выполняется применением токена…» Требование выполнено, однако токен с неизвлекаемым ключом является инструментом решения задачи, существенно отличающейся от защиты сетевого взаимодействия объектов КИИ.

Токен предназначен для того, чтобы ключ пользователя был *отчуждаем* от средства вычислительной техники, на котором пользователь осуществляет те или иные операции с ключом. В случае банкомата отчуждаемость не только избыточна, но и вредна: с одной стороны, она делает возможными сценарии атак с подменой или иными вариантами компрометации ключа за счет отчуждаемости его носителя, а с другой — подключенное к порту USB-устройство резко снижает надежность решения при вибрации, ударах, нагревании и прочих особенностях условий, в которых работают технические средства на объектах КИИ. Самое же главное — решение с отчуждаемым ключом не может обеспечивать автоматический старт без нарушения условий эксплуатации, так как требуется подключение ключевого носителя человеком, его авторизация для доступа к ключу.

Использование таких решений в банкоматах требует адаптации, сводящейся по существу к обходу документированных правил пользования.

Модуль работы с неизвлекаемым ключом в таких технических средствах, как банкомат, должен быть реализован как часть резидентного компонента безопасности, размещенного непосредственно на плате компьютера, а не как отчуждаемый персональный носитель ключа.

Наконец, существенная задача, которая стоит перед производителем криптошлюза для объекта КИИ (в частности, банкомата), связана уже не с требованиями, а с техническими особенностями этих объектов: она заключается в том, чтобы поддержать множество разнообразных интерфейсов.

Примеров таких СЗИ для защиты сетевой коммуникации в инфраструктуре, включающей разнообразное оборудование, взаимодействующее разнообразным образом по различным каналам, на сегодняшний день немного, но они есть.

Так, недавно с положительным результатом завершены исследования соответствия СКЗИ Dcrypt 1.0 v.2 классу КС2 (вариант испол-

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

нения 29) и КС3 (вариант исполнения 30) при исполнении на специализированном компьютере с аппаратной защитой данных m-TrusT[1].

Положительное заключение регулятора свидетельствует о том, что данный специализированный компьютер обеспечивает среду функционирования криптографии для СКЗИ высоких классов и аналогичные заключения могут быть получены и для других СКЗИ, если на то будет желание вендора.

Специализированный компьютер с аппаратной защитой данных

Решение проблем адаптации СКЗИ к разнообразному оборудованию, на котором оно должно функционировать, обеспечивает конструктивная особенность данного компьютера. Сложность этой задачи в том, что адаптация СКЗИ — это повторная сертификация. Поэтому при необходимости защитить «нестандартное» (т.е. отличающееся от офисного компьютера) техническое средство мы сталкиваемся с необходимостью временных и финансовых затрат на пересертификацию или с необходимостью адаптации защищаемого технического средства к средству защиты, чтобы не тронуть сертифицированное.

Задача решается путем декомпозиции: разделения СЗИ на то, что должно быть неизменным, чтобы не требовалось повторной сертификации, и то, что может меняться для того, чтобы интегрироваться с очередным техническим средством на очередном объекте КИИ (например, с банкоматом другой модификации или с инфокиоском, терминалом эквайринга).

Так, должно быть выделено аппаратное ядро, а встраивание должно выполняться за счет создания несложных интерфейсных плат, обеспечивающих транспорт и необходимый форм-фактор, но не связанных с выполнением криптографических функций.

Ядро проектируется как универсальное, а множество интерфейсных плат может включать любые форм-факторы, набор которых зависит только от особенностей объектов КИИ.

Сам специализированный компьютер одноплатный и представляет собой «мезонин», устанавливаемый непосредственно в защищаемый объект или подключаемый к нему с помощью интерфейсной платы — не выполняющей никаких преобразований информации, а лишь обеспечивающей технологическую и конструктивную совместимость.

[1] Криптошлюз на базе этих исполнений СКЗИ носит в линейке производителя (компании «ТСС») название МКСЗ «Diamond VPN/FW» (версия VPN, серия 0).

Светлана КОНЯВСКАЯ

Каждый такой компьютер является точкой сбора информационных и (или) управляющих сигналов от ПКО, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровки[1].

Новая гарвардская архитектура как основа построения СФК

Новая гарвардская архитектура подробно описана в других работах[2], здесь же остановимся только на тех ее особенностях, которые обеспечивают так называемый «вирусный иммунитет» — невозможность внедрения извне какого-либо кода, способного повлиять на исполняемую устройством информационную технологию. В компьютерах традиционных архитектур, как фоннеймановской, так и гарвардской (любой архитектуры, являющейся реализацией машины Тьюринга), заложена уязвимость, делающая возможными атаки с целью перехвата управления. Это уязвимость универсального исполнителя: средство вычислительной техники, предназначенное для выполнения любых задач, неизбежно выполнит вредоносную.

В компьютерах традиционных архитектур, как фоннеймановской, так и гарвардской (любой архитектуры, являющейся реализацией машины Тьюринга), заложена уязвимость, делающая возможными атаки с целью перехвата управления.

Блокирование этой уязвимости возможно двумя путями:

— установкой комплекса дорогих и сложных в настройке средств защиты информации (а значит, умножением точек потенциального отказа) либо

— изменением архитектуры вычислительной машины.

Такой измененной архитектурой, лишенной базовой уязвимости и запатентованной[3], является разработанная в России Новая гарвардская архитектура.

Соответствие требованиям нормативной методической базы

Компьютер с аппаратной защитой данных, как любой универсальный защищенный компьютер, может использоваться для реализации

[1] Подробные характеристики m-TrusT и обеспечиваемые ими защитные механизмы опубликованы в специализированных статьях и книгах, а сам компьютер запатентован. См.: Щербаков А.Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды. Автореф. дис. ... д-ра техн. наук. М., 1997; Konyavsky V.A., Ross G.V. Secure computers of the new Harvard architecture // Asia Life Sciences. August 2019. Issue 1. P. 33–53; Konyavsky V.A., Ross G.V. Computer with changeable architecture // Journal of Mechanical Engineering Research and Developments. 2019. Vol. 42. Issue 3. P. 19–23.

[2] Konyavsky V.A., Ross G.V. Secure computers of the new Harvard architecture // Asia Life Sciences. August 2019. Issue 1. P. 33–53; Konyavsky V.A., Ross G.V. Computer with changeable architecture // Journal of Mechanical Engineering Research and Developments. 2019. Vol. 42. Issue 3. P. 19–23.

[3] Батраков А.Ю., Конявский В.А., Счастный Д.Ю., Пярин В.А. Специализированный компьютер с аппаратной защитой данных. Патент на полезную модель № 191690. 15.08.2019, бюл. № 23.

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

всех технических мер обеспечения безопасности значимых объектов КИИ, включая:

— идентификацию и аутентификацию;
— управление доступом;
— ограничение программной среды;
— защиту машинных носителей информации;
— аудит безопасности;
— антивирусную защиту;
— предотвращение вторжений (компьютерных атак);
— обеспечение целостности;
— обеспечение доступности;
— управление обновлениями программного обеспечения.

Наиболее же эффективно использовать его для обеспечения группы мер защиты информационной (автоматизированной) системы и ее компонентов.

При использовании данного компьютера в составе ИС важно соответствие его собственных свойств требованиям регулятора. Этому посвящена табл. 1. В табл. 2 приведены те меры, которые обеспечиваются в системах КИИ.

Таблица 1

Соответствие m-TrusT техническим мерам Требований по обеспечению безопасности значимых объектов КИИ[1]

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие требованиям ФСТЭК России	Примечание
I. Идентификация и аутентификация (ИАФ)			Меры ИАФ.0, ИАФ.3, ИАФ.4 организационные. Мера ИАФ.6 необязательная
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	
ИАФ.2	Идентификация и аутентификация устройств	+	
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	
ИАФ.7	Защита аутентификационной информации при передаче	+	

[1] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. Приказа ФСТЭК России от 26.03.2019 № 60).

Светлана КОНЯВСКАЯ

Продолжение табл. 1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие требованиям ФСТЭК России	Примечание
II. Управление доступом (УПД)			Меры УПД.0, УПД.4, УПД.5 организационные. Меры УПД.7, УПД.8, УПД.12 необязательные
УПД.1	Управление учетными записями пользователей	*	Не имеет пользователей, так как обычно работает в автоматическом режиме
УПД.2	Реализация модели управления доступом	*	Управление доступом осуществляется ключевой системой
УПД.3	Доверенная загрузка	+	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	
УПД.9	Ограничение числа параллельных сеансов доступа	*	Ограничивается ключевой системой
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	
УПД.13	Реализация защищенного удаленного доступа	+	Защита удаленного доступа обеспечивается СКЗИ
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	
III. Ограничение программной среды (ОПС)			Меры ОПС.0 и ОПС.2 организационные. Мера ОПС.3 необязательная
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	+	
IV. Защита машинных носителей информации (ЗНИ)			Меры ЗНИ.0–ЗНИ.2 организационные. Меры ЗНИ.3 и ЗНИ.4 необязательные
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. В системе обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»
ЗНИ.7	Контроль подключения съемных машинных носителей информации	**	Отсутствует возможность подключения съемных машинных носителей информации. Обеспечивается использованием СЗИ «Секрет Особого Назначения»

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

Продолжение табл. 1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие требованиям ФСТЭК России	Примечание
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	–	
V. Аудит безопасности (АУД)			Меры АУД.0–АУД.2, АУД.10 и АУД.11 организационные
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	Обеспечивается собственной системой времени
АУД.4	Регистрация событий безопасности	+	
АУД.5	Контроль и анализ сетевого трафика	–	
АУД.6	Защита информации о событиях безопасности	+	
АУД.7	Мониторинг безопасности	+	
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	
АУД.9	Анализ действий отдельных пользователей	–	
VI. Антивирусная защита (АВЗ)			Меры АВЗ.0 и АВЗ.5 организационные
АВЗ.1	Реализация антивирусной защиты	+	
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	–	Электронная почта и внешние сервисы не используются
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	–	
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	–	Не требуется
VII. Предотвращение вторжений (компьютерных атак) (СОВ)			Мера СОВ.0 организационная
СОВ.1	Обнаружение и предотвращение компьютерных атак	**	Обеспечивается внешними средствами СОВ
СОВ.2	Обновление базы решающих правил	**	Обеспечивается внешними средствами СОВ
VIII. Обеспечение целостности (ОЦЛ)			Мера ОЦЛ.0 организационная. Меры ОЦЛ.2 и ОЦЛ.6 необязательные
ОЦЛ.1	Контроль целостности программного обеспечения	+	
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	+	
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	+	
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	+	

Светлана КОНЯВСКАЯ

Продолжение табл. 1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие требованиям ФСТЭК России	Примечание
IX. Обеспечение доступности (ОДТ)			Меры ОДТ.0–ОДТ.2 организационные. Мера ОДТ.7 необязательная
ОДТ.4	Резервное копирование информации	**	В соответствии с политикой информационной безопасности
ОДТ.5	Обеспечение возможности восстановления информации	**	В соответствии с политикой информационной безопасности
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	Обеспечивается архитектурой
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	–	
X. Защита технических средств и систем (ЗТС)			Меры ЗТС.0, ЗТС.2–ЗТС.5 организационные. Меры ЗТС.1 и ЗТС.6 необязательные
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)			Меры ЗИС.0–ЗИС.5, ЗИС.8 организационные. Меры ЗИС.7, ЗИС.9–ЗИС.12, ЗИС14, ЗИС.15, ЗИС.17, ЗИС.18, ЗИС.22–ЗИС.26, ЗИС.28–ЗИС.31, ЗИС.36, ЗИС.37 необязательные
ЗИС.6	Управление сетевыми потоками	+	Обеспечивается ключевой системой
ЗИС.13	Защита неизменяемых данных	+	
ЗИС.16	Защита от спама	+	
ЗИС.19	Защита информации при ее передаче по каналам связи	+	
ЗИС.20	Обеспечение доверенных канала, маршрута	+	
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	
ЗИС.27	Обеспечение подлинности сетевых соединений	+	
ЗИС.32	Защита беспроводных соединений	+	
ЗИС.33	Исключение доступа через общие ресурсы	+	
ЗИС.34	Защита от угроз отказа в обслуживании (DoS, DDoS-атак)	+	
ЗИС.35	Управление сетевыми соединениями	+	
ЗИС.38	Защита информации при использовании мобильных устройств	+	
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	–	

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

Окончание табл. 1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Соответствие требованиям ФСТЭК России	Примечание
XII. Реагирование на компьютерные инциденты (ИНЦ)			Все меры этой группы организационные
XIII. Управление конфигурацией (УКФ)			Все меры этой группы организационные
XIV. Управление обновлениями программного обеспечения (ОПО)			Меры ОПО.0, ОПО.1 и ОПО.3 организационные
ОПО.2	Контроль целостности обновлений программного обеспечения	+	
ОПО.4	Установка обновлений программного обеспечения	+	
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)			Все меры этой группы организационные
XVI. Обеспечение действий в нештатных ситуациях (ДНС)			Все меры этой группы организационные
XVII. Информирование и обучение персонала (ИПО)			Все меры этой группы организационные

* При использовании в ИС без СКЗИ мера осуществляется установкой СПО СЗИ.

** При использовании в ИС при установке СПО СЗИ.

Таблица 2

Применение m-TrusT для защиты значимых объектов КИИ

Обозначение и номер меры	Меры обеспечения безопасности
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.27	Обеспечение подлинности сетевых соединений
ЗИС.32	Защита беспроводных соединений
ЗИС.33	Исключение доступа через общие ресурсы
ЗИС.35	Управление сетевыми соединениями

При этом обеспечиваются:

— работа в автоматическом режиме, что существенно снижает нагрузку на организационно-технические меры при эксплуатации СКЗИ;

— изменение форм-фактора без повторной сертификации изделия, что значительно сокращает сроки работ по защите КИИ;

— работа с любыми каналами связи, используемыми в КИИ;

Светлана КОНЯВСКАЯ

— защита КИИ без глубокой переработки ее структуры, что сильно сокращает затраты на проведение мероприятий.

Устройства на защищенной платформе

На специализированном компьютере с аппаратной защитой данных строятся решения для разных отраслей экономики: транспорта, энергетики, социальной сферы и многих других. Для финансовых организаций применяется, в частности, линейка криптошлюзов:

1) криптошлюз в технологическом корпусе для установки в банкоматы с возможностью поддержки двух и более операторов мобильного интернета;

2) криптошлюз в корпусе одноюнитового сервера для установки в бэк- или фронт-офис до 50 абонентских устройств;

3) сервер VPN для установки в ЦОД или серверную стойку головного отделения.

Наибольший интерес в рамках рассматриваемых в статье вопросов представляет первое из перечисленных решений (рисунок).

Устройство поддерживает одновременную работу нескольких независимых каналов связи. К примеру, могут быть подключены два Ethernet от различных провайдеров и (или) два LTE-модема различных операторов связи. Это позволяет продолжить работу даже при отказе одного из каналов, что повышает отказоустойчивость и является актуальной задачей именно для банкоматов.

Это дает возможность защитить каналы — как от процессингового центра к компьютеру, так и от компьютера к диспенсеру — и обес-

Рисунок

Криптошлюз для установки в банкоматы

Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры

печить целостность программно-аппаратной среды компьютера, причем сделать это в соответствии с Законом о КИИ, нетравматично для функционирования системы и с сохранением инвестиций. При этом СКЗИ стартует в автоматическом режиме без нарушения правил пользования СКЗИ — безопасность не конфликтует с работоспособностью.

Криптошлюз уже прошел апробацию в банкоматах одного из крупных коммерческих банков, и теперь с учетом этого опыта и завершения сертификации ФСБ России начинается опытная эксплуатация решения в банкоматах на предмет удобства его применения с конструктивной точки зрения: насколько удобно расположение портов, крепежных элементов, нет ли затруднений при обслуживании. По результатам опытной эксплуатации банки, которые в ней участвуют, смогут сформулировать свои пожелания к адаптации серийного корпуса с учетом особенностей именно своих банкоматов.

В этой статье рассмотрены далеко не все (и, наверное, даже не большая часть) атаки, актуальные для финансовых организаций. Многие из оставшихся за рамками рассмотрения (такие, как «оплати мой кофе одним своим взглядом») заслуживают отдельных статей, которые будут опубликованы в дальнейшем.