Чтобы разорвать порочный круг, в котором целостность программы проверяется другой программой — и так до бесконечности, нужен инструмент, который не может быть изменен, то есть автономный и аппаратный. В статье приведены характеристики и примеры средств защиты, которые могут обеспечить доверенную среду в вычислительной системе.

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

Светлана КОНЯВСКАЯ,
ОКБ САПР, заместитель директора, к.ф.н.

Меры для защиты безналичных расчетов должны быть направлены:

1) на создание и поддержание вычислительной среды, в которой программы исполняются корректно;

2) точную идентификацию, аутентификацию и авторизацию пользователя;

3) разграничение доступа к ресурсам системы;

4) реализацию тех участков ИТ, которые не могут контролироваться банком, с использованием технических средств, предназначенных для работы вне доверенной среды;

5) надежную фиксацию событий в системе.

В этой статье мы сосредоточимся на первом пункте.

Очевидно, что «правильная» среда должна исключать влияние на корректность выполнения информационных технологий, программ, которые в ней исполняются. Влияние исключено в том случае, если процессы в ней изолированы один от другого. Известно несколько вариантов реализации такой среды:

— функционально замкнутая среда (ФЗС);

— изолированная программная среда (ИПС);

— доверенная вычислительная среда (ДВС);

— феномен на стыке ФЗС и ДВС — доверенный сеанс связи (ДСС).

Для перечисленных сред разработаны и научно обоснованы модели и доказательства их защищенности[1].

[1] Подробнее о первых трех вариантах среды см.: Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». М.: Радио и связь, 1999. С. 26-60; Конявский В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией. Минск: Серия «Библиотека журнала "УЗИ"», 2004. С. 38-75; о четвертом: Конявский В.А. Серебряная пуля для хакера // Защита информации. INSIDE. 2013. № 4. С. 54-56; № 5. С. 69-73.

Светлана КОНЯВСКАЯ

Какой именно должна быть среда в каждом конкретном случае, зависит от того, что представляет собой защищаемая технология; дать единственно правильный ответ тут нельзя. Самым высоким потенциалом защиты обладает ДВС, однако и стоимость ее создания и поддержания в системе самая высокая. ИПС наиболее сложна с точки зрения доказательства корректности изоляции, ФЗС подходит только для однозадачных систем, а ДСС обходится дешевле всего, но создает защищенную среду только для кратковременных сеансов работы.

Доверенная среда поддерживается, если обеспечиваются:

1) контроль запуска задач и процессов;

2) взаимное невлияние задач;

3) защита от перехвата управления;

4) защита информационных технологий как последовательности операций.

Там, где все операции должны выполняться в доверенной среде, создавайте и поддерживайте ДВС. Если доверенность нужна лишь иногда — достаточно (и удобнее) применять ДСС.

Доверенная вычислительная среда или доверенный сеанс связи?

Однажды созданная ДВС должна поддерживаться за счет средств защиты информации (СЗИ) долго, в отдельных случаях — годы (именно в платежных сегментах не редкость серверы и АРМ, которые должны работать в непрерывной сессии постоянно, в отличие от их эксплуатирующего персонала, работающего посменно). За это время суммарное количество атак может стать огромным, и все эти атаки должны быть отражены защитными механизмами СЗИ. Конечно, такие СЗИ стоят дорого.

ДСС создается каждый раз заново, и это в ряде случаев может быть неудобно — загрузка и проверочные мероприятия продолжаются 30–50 секунд. Но средства ДСС стоят гораздо дешевле, так как длительность ДСС не всегда достигает и 20 минут.

В двух словах необходимо прояснить связь между продолжительностью периода непрерывной защиты и ее сложностью (и стоимостью). Изменяемость вычислительной среды определяет универсальность средств вычислительной техники (СВТ), с одной стороны, а с другой — сама определяется архитектурой большинства современных СВТ, являющихся реализацией «машины Тьюринга». Проще говоря, наши компьютеры универсальны потому, что изменяемы, а изменяемы они потому, что такова их архитектура. Именно это свойство используют вирусы и другое вредоносное ПО. И для поддержания доверенной среды нам необходимо эту изменяемость блокировать.

Средства обеспечения ДСС блокируют ее, если сильно упрощать, путем запрета записи в долговременную память, то есть все, что

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

случилось во время сеанса, обнуляется по его завершении. Поэтому сеанс не должен быть продолжительным, иначе теоретически, даже без записи в долговременную память, хакер сможет накопить изменения так, чтобы создать условия для реализации атаки.

СЗИ, способные обеспечить создание и поддержание ДВС, меняют архитектуру компьютера, поэтому они сложны в разработке, настройке и эксплуатации[1].

Как именно это делается — и в случае с ДВС, и в случае с ДСС, разберем ниже.

Пока зафиксируем, что с этим связана и методика выбора: там, где все операции должны выполняться в доверенной среде, создавайте и поддерживайте ДВС. Если доверенность нужна лишь иногда — достаточно (и удобнее) применять ДСС.

При этом СЗИ клиента должны быть ненастраиваемые (тогда он не настроит их неправильно). Бессмысленно все лучше и лучше защищать сервисы, когда приемлемый уровень квалификации клиента в области информационной безопасности недостижим в принципе, а его неквалифицированные действия обязательно создадут «дыру» в защищенности.

Бессмысленно все лучше и лучше защищать сервисы, когда приемлемый уровень квалификации клиента в области информационной безопасности недостижим в принципе. Поэтому СЗИ клиента должны быть ненастраиваемые.

Как определить, действительно ли среда доверенная?

1. Средство, контролирующее среду, должно быть не подвержено влиянию этой среды, то есть быть изолированным, автономным.

2. Защитные процедуры должны проводиться до загрузки ОС[2]. Если существует даже самый краткий момент времени, когда операционная система уже загружена, а защитные механизмы еще не включены, — злоумышленник сумеет установить нужные ему программы.

Из этого следует, что средство защиты должно быть аппаратным (т.к. программные средства работают в ОС, после ее загрузки). Обеспечить надежную защиту без применения специализированных аппаратных средств невозможно.

3. Чтобы исключить запуск на исполнение измененной программы, проводится контроль целостности.

Правильно выполненный контроль целостности позволяет своевременно обнаружить несанкционированные модификации программ и данных и предотвратить использование недоверенных программ и данных.

[1] Конявский В.А. Иммунитет как результат эволюции ЭВМ // Инсайд. Защита информации. 2017. № 4. С. 46-52.

[2] Правильность этого вывода доказана с применением точного математического аппарата. См.: Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». М.: Радио и связь, 1999.

Светлана КОНЯВСКАЯ

Если для того, чтобы контролировать целостность программы А, мы используем программу В, то кто нам даст гарантию, что программа В осталась неизменной? Значит, нужна программа С, которая проконтролирует целостность программы В, и т.д. Вера в то, что с помощью одной программы можно проверить целостность другой, — это тяжелое техническое заболевание, состоящее в имитации мероприятий по защите без повышения уровня защищенности и получившее название «Синдром Мюнхгаузена».

Для того чтобы разорвать порочный круг, нам нужен инструмент снаружи нашего «болота», который не мог быть изменен, поэтому остался точно доверенным. То есть снова — автономный и аппаратный. Автономность обеспечивает независимость решения от потенциально модифицированного окружения, а обеспечивается она в свою очередь аппаратной реализацией.

Защитные процедуры должны проводиться до загрузки ОС. Из этого следует, что средство защиты должно быть аппаратным (т.к. программные средства работают в ОС, после ее загрузки).

Заручившись этими выводами, мы можем перейти к рассмотрению характеристик и примеров средств защиты, которые могут обеспечить доверенную среду в вычислительной системе.

Средства, обеспечивающие защиту

В этом разделе рассмотрим варианты обеспечения доверенной среды исполнения функционального программного обеспечения и криптографии (для систем, реализующих безналичные расчеты, это обязательное требование в соответствии с Положением Банка России № 683-П[1] и ГОСТом, на который оно ссылается[2]) и конкретные средства, позволяющие реализовать эти варианты.

Раз универсальность компьютера, которую нам необходимо ограничить, как мы выяснили выше, обеспечивается архитектурно, самой «конструкцией» машины Тьюринга, а архитектуру нельзя изменить программным путем, то никакие программные средства не помогут нам защититься от хакеров надежно.

Схема атаки хакера наиболее распространенного типа — атака с целью перехвата управления — выглядит так:

s1) внедряется и размещается в оперативной памяти вредоносное ПО (ВрПО);

s2) внедряется и размещается в оперативной памяти вредоносный обработчик прерываний;

[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».

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

s3) записываются в долговременную память ВрПО и обработчик прерываний;

s4) с помощью любого доступного механизма вызывается прерывание (например, с помощью DDoS-атаки, или злоумышленник может просто дождаться перезапуска СВТ);

s5) внедренный ранее обработчик прерываний срабатывает и передает управление ВрПО;

s6) ВрПО выполняет свою функцию (например, реализует разрушающее программное воздействие).

Здесь s1–s3 — это шаги по подготовке атаки, s4 — инициирование атаки, s5 и s6 — собственно использование архитектурной уязвимости.

Если уязвимость в архитектуре — то и совершенствовать нужно архитектуру.

Мы можем делать это одним из двух способов:

1. Усовершенствовать архитектуру уже существующих технических средств — то есть, приобретая новую технику, устанавливать на нее те или иные средства защиты.

2. Использовать новые технические средства на базе новой, более совершенной архитектуры.

В первом случае мы блокируем выполнение шагов s5 и s6 (не даем сработать вредоносному ПО), а во втором — шага s3 (не даем записать в долговременную память изменения среды).

Для этого применяются:

1) средство доверенной загрузки[1], которое реализует изменение архитектуры уже готового уязвимого компьютера фоннеймановской архитектуры так, чтобы обеспечить его правильный старт (блокирование шагов s5 и s6), а также создает предпосылки к блокированию шага s3 (записи вредоносного ПО в долговременную память);

2) специализированные компьютеры с аппаратной защитой данных Новой гарвардской архитектуры[2], сразу обладающие архитектурой, лишенной описанной уязвимости. Они блокируют шаг s3, то есть не дают возможности записывать изменения в долговременную память никогда, кроме как в специальных режимах, перевод в которые программно невозможен (а значит, хакер этого сделать не сможет);

3) средство обеспечения доверенного сеанса связи (СОДС)[3], позволяющее использовать незащищенный компьютер с уязвимой архитектурой в таком режиме, в котором архитектура не может повлиять

Раз универсальность компьютера, которую нам необходимо ограничить, обеспечивается архитектурно, а архитектуру нельзя изменить программным путем, то никакие программные средства не помогут нам защититься от хакеров надежно.

[1] okbsapr.ru/products/accord/accord-amdz/.

[2] okbsapr.ru/products/newharvard/.

[3] okbsapr.ru/products/storage/compute/sods/.

Светлана КОНЯВСКАЯ

на вычислительную среду пользователя в течение непродолжительного периода защищенной работы.

Последнее решение является промежуточным между первым и вторым.

Аппаратный модуль доверенной загрузки

Итак, когда мы используем компьютеры с принципиально уязвимой архитектурой, то у нас должно быть средство управления этой архитектурой.

На практике это означает, что на время загрузки и проведения контрольных процедур компьютер должен утрачивать свойства машины Тьюринга (универсального исполнителя), а затем, после успешного завершения контрольных процедур, — снова приобретать эти свойства.

Выше мы определили, что изменить таким образом архитектуру уже готового компьютера может только аппаратное активное автономное устройство, начинающее контрольные процедуры до загрузки ОС. Таким устройством является аппаратный модуль доверенной загрузки.

Понятие доверенной загрузки входит в понятийный ряд ФСТЭК России как целевая функция отдельного типа средств защиты информации – средства доверенной загрузки.

Доверенная загрузка — это загрузка заранее определенной операционной системы с заранее определенных постоянных носителей после успешного завершения специальных процедур проверки заранее определенных условий: целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

Понятие доверенной загрузки входит в понятийный ряд ФСТЭК России как целевая функция отдельного типа средств защиты информации — средства доверенной загрузки (СДЗ).

Например, средство доверенной загрузки «Аккорд-АМДЗ», которое во всех его вариантах исполнения согласно терминологии ФСТЭК России является СДЗ уровня платы расширения.

«Аккорд-АМДЗ» может быть реализован на различных контроллерах, принципиально различающихся только шинными интерфейсами: PCI или PCI-X; PCI-express; Mini PCI-express; Mini PCI-express half card; m.2 (рис. 1).

Существует также вариант исполнения «Аккорд-АМДЗ» на базе USB-устройства. Этот вариант имеет определенные ограничения, которые должны восполняться оргмерами или применением дополнительных механизмов.

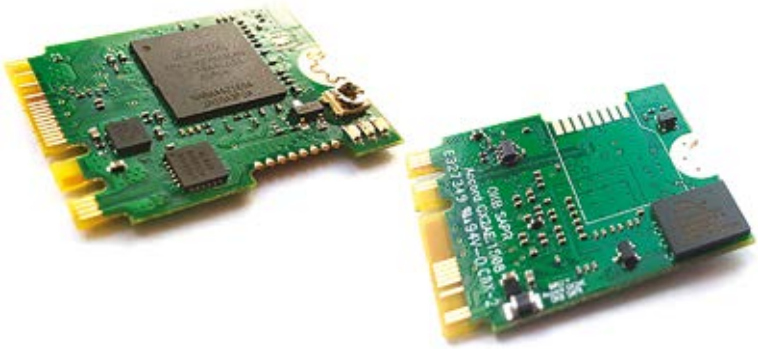
Применение криптографии

Отдельного упоминания в связи с СДЗ требует вопрос применения криптографии.

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

Рисунок 1

СЗИ НСД «Аккорд»



Нормативная методическая база (Положение Банка России № 683-П, ГОСТ Р 57580.1-2017) предписывает большинству финансовых организаций использовать средства криптографической защиты информации (СКЗИ) не ниже класса КС2. Эти требования основаны на требованиях ФСБ России и профильных стандартов[1]. Использование на СВТ СКЗИ класса КС2 возможно исключительно при совместном использовании с СДЗ уровня платы расширения (АПМДЗ), сертифицированным ФСБ России.

Сегодня нет проблем в том, чтобы выбрать АПМДЗ (в терминологии ФСБ России)/СДЗ (в терминологии ФСТЭК России) для создания среды функционирования криптографии (СФК) на большинстве моделей настольных компьютеров и серверов. Хуже, но решаемо — с ноутбуками. Совсем сложно — с планшетами. На то есть технические причины, которые сводятся к двум основным:

1. Мало на каких планшетах есть свободный разъем m.2 с ключами A–E. Это означает m.2 с выходом на интерфейс PCI, который необходим для работы СДЗ уровня платы расширения (АПМДЗ) в формфакторе m.2 (о том, чтобы поместить в планшет какой-то еще вариант, трудно даже вести речь). Обычно имеющийся в планшете разъем m.2 имеет ключи вывода на SSD, то есть предназначен для работы с диском. Если же «нужный» разъем m.2 есть, он, как правило, занят wi-fi модулем, а вынимать из планшета wi-fi, разумеется, неприемлемо в абсолютном большинстве случаев.

Чтобы на планшете можно было использовать криптографию достаточно высокого класса (КС2 и выше), необходимы и особенное средство доверенной загрузки, и особенный планшет.

[1] Конявская С. Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры // Расчеты и операционная работа в коммерческом банке. 2020. № 1. С. 13-25; Применение защищенных микрокомпьютеров МКТ-card lond в системах удаленного доступа смешанного типа // Вопросы защиты информации: Научно-практический журнал / ФГУП «ВИМИ». 2016. Вып. 3. № 114. С. 23-30.

Светлана КОНЯВСКАЯ

2. У планшетов совершенно иначе, чем у стационарных машин, реализовано управление питанием — в частности, режим «сна». И это делает неприменимыми на планшетах существующие в АПМДЗ механизмы реализации «сторожевого таймера» (тем более что в них вообще нет той цепи, разрыв которой осуществляет стандартная схема «сторожевого таймера»), требует изменения механизмов идентификации/аутентификации пользователя и т.д.

Как правило, задача решается тем, что используется СДЗ уровня BIOS. Однако такое СДЗ не подходит для создания СФК. Таким образом, для того чтобы на планшете можно было использовать криптографию достаточно высокого класса (КС2 и выше), необходимы и особенное СДЗ, и особенный планшет. Выходом может стать использование планшета, в котором реализована СФК на класс СКЗИ КС3, как единого решения[1].

За счет совокупности своих функций, включающих аппаратный контроль целостности среды и контроль запуска задач в программной части комплекса, программно-аппаратный комплекс позволяет закрыть уязвимость фоннеймановской архитектуры компьютера.

Программно-аппаратные комплексы

Аппаратный модуль доверенной загрузки контролирует только старт компьютера и не работает в операционной системе. Это означает, что на его ответственности блокирование шагов s5 и s6 описанной выше атаки на перехват управления, но не блокирование шага s3: помешать записи в долговременную память чего-либо, попавшего в оперативную память во время работы ПК, он сам по себе не может. Для того чтобы это сделать, необходимо применять программно-аппаратные комплексы (ПАК)[2].

В ПАК СЗИ НСД «Аккорд» реализованы дискреционный (с использованием 13 атрибутов) и мандатный механизмы разграничения доступа, в том числе контроль запуска задач и контроль печати из любых приложений на принтеры любых типов (сетевые, локальные, виртуальные).

За счет совокупности своих функций, включающих аппаратный контроль целостности среды и контроль запуска задач в программной части комплекса, ПАК позволяет закрыть уязвимость фоннеймановской архитектуры компьютера, блокируя атаку на перехват управления на всех шести ее шагах. При этом архитектура компьютера, как и в случае с Новой гарвардской архитектурой, но значительно бóльшими усилиями, становится динамически изменяемой:

[1] Эта задача решена в планшете «ПК3 2020», на котором установлен «Аккорд-АМДЗ». Аналоги решения на сегодняшний день неизвестны — как целиком, так и АПМДЗ в формате m.2, соответствующего требованиям ФСБ России в части управления питанием для планшетов.

[2] ПАК на базе «Аккорд-АМДЗ» — ПАК «Аккорд-Win32», «Аккорд-Win64» и «Аккорд-X», предназначенные соответственно для разграничения доступа в 32- и 64-разрядных ОС Windows и в ОС Linux.

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

сохраняя необходимые для решения функциональных задач свойства «машины Тьюринга» во время работы, во время старта компьютер ею не является, работая скорее как «конечный автомат».

Когда необходимы альтернативные варианты

Аппаратный модуль доверенной загрузки и решения на его основе не всегда подходят, потому что довольно дороги и сложны в настройке и использовании.

Для защиты центров обработки данных (ЦОД) и компьютеров x86, выполняющих задачи, требующие постоянного поддержания доверенной среды, этот вариант в наибольшей степени отвечает духу и букве требований регуляторов и здравому смыслу.

Однако в других случаях он неудобен или даже неприемлем.

Один из таких случаев — это объекты критических информационных инфраструктур, представляющие собой не офисы или ЦОД, а включающие в себя некоторое специфическое оборудование: в финансовых системах это, например, банкоматы, терминалы оплаты, машины инкассации и многое другое.

Аппаратный модуль доверенной загрузки и решения на его основе нецелесообразно применять для объектов КИИ, включающих в себя специфическое оборудование, типовых рабочих мест фронт- и бэк-офиса, ДБО.

Особенности таких объектов связаны, с одной стороны, со спецификой условий работы средства защиты, а с другой — с необходимостью работы в автоматическом режиме (в т.ч. автоматического старта) с минимальным администрированием и обслуживанием[1].

Другой случай, где целесообразно применение СВТ с Новой гарвардской архитектурой, не имеющей базовой уязвимости традиционных архитектур, а значит, не требующей установки средств защиты, способных менять архитектуру компьютера, — это типовые рабочие места фронт- и бэк-офиса.

На таких участках возможно применять микрокомпьютеры МКТ-card long[2] (рис. 2).

Основная причина их эффективности в этом качестве — «вирусный иммунитет». Он обеспечивается тем, что никакие изменения не записываются в долговременную память компьютера. Работа же во фронт- и бэк-офисах, как правило, производится в рамках удаленного доступа в централизованной информационной системе. А те файлы,

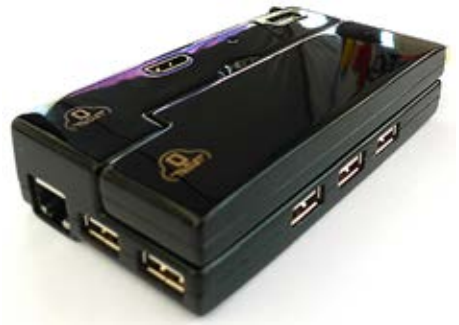
[1] Решение для таких объектов рассмотрено в статье: Конявская С. Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры // Расчеты и операционная работа в коммерческом банке. 2020. № 1. С. 13-25.

[2] См., напр.: Применение защищенных микрокомпьютеров МКТ-card long в системах удаленного доступа смешанного типа // Вопросы защиты информации: Научно-практический журнал / ФГУП «ВИМИ». 2016. Вып. 3. № 114. С. 23-30.

Светлана КОНЯВСКАЯ

Рисунок 2

Микрокомпьютер MKT-card long



что все-таки необходимо сохранять или обрабатывать локально, могут храниться на защищенных служебных носителях[1].

Наконец, случай, когда требования к простоте настройки усиливаются до «не должно быть никакой настройки», а низкая стоимость становится обязательным условием применимости, — это ДБО, особенно тогда, когда клиентом является физическое лицо.

Использование клиентом защищенной технологии взаимодействия с банком может быть условием его обслуживания.

Способы защиты в рамках ДБО

Не находя возможности повлиять на то, чтобы компьютеры клиентов были защищены, банки решают задачу минимизации своих потерь, перекладывая ответственность на клиента. Но существует и альтернативный подход: использование клиентом защищенной технологии взаимодействия с банком может быть условием его обслуживания. Для этого нужно в клиентском договоре предоставить обоснованный выбор: управление счетом с использованием защищенного компьютера — и тогда все риски покрывает банк (или ЦОД, или страховая компания), или любые другие механизмы — тогда все риски на клиенте. Так банк и обезопасит себя, и обеспечит высокий уровень защищенности клиента.

Какие технические предпосылки должны быть созданы для реализации этих возможностей?

Необходимо, чтобы серверная часть информационной системы, реализующей функциональность ДБО, была способна различать, из какой среды — доверенной или нет — подключается в данный момент клиент. Отчасти это обеспечивается подключением, защищенным каким-либо VPN. Однако если ключи VPN у клиента нахо-

[1] См., напр.: okbsapr.ru/products/storage/flash/secret/.

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

дятся на отчуждаемом носителе (что является условием эксплуатации большинства VPN), гарантировать, что пользователь подключается с защищенного компьютера, наличие VPN не может. Об этом нужно помнить при проектировании системы идентификации/аутентификации.

Однако и тогда, когда такая функциональность системой поддержана, установка на компьютеры клиентов комплекса средств защиты за 35–60 тыс. руб., да еще и ограничение возможности связи с банком единственным компьютером — условия, неприемлемые для частных лиц. Зато работа в доверенном сеансе связи здесь видится идеальным выходом.

Средство обеспечения доверенного сеанса связи

В качестве примера опишем работу СОДС «МАРШ!» (рис. 3). Клиент подключает устройство в USB-порт компьютера, например в гостинице (это предельный случай неконтролируемости среды). С устройства загружается эталонная вычислительная среда, в которой автоматически запускается браузер (помимо этого там может быть, например, MS Office, набор драйверов для принтеров и др.).

Рисунок 3

Средство обеспечения доверенного сеанса связи «МАРШ!»

В строке браузера можно вводить что угодно, но встроенный межсетевой экран не даст открыть никакой сайт, кроме онлайн-банка. После завершения работы с банком клиент отключает «МАРШ!» и перезагружает компьютер, чтобы использовать все возможности интернет-серфинга без ограничений.

Таким образом, мы изолируем от возможного негативного влияния только среду взаимодействия с банком, но изолируем надежно.

Как обеспечивается защита?

Конструктивно СОДС представляет собой USB-устройство и выглядит точно так же, как обычная флешка. Однако на самом деле это активное микропроцессорное устройство с многоконтурной крип-

Светлана КОНЯВСКАЯ

тографической подсистемой, проверенной защищенной операционной системой Linux, браузером, специальной подсистемой управления к памяти и многим другим.

Основная задача СОДС — создание доверенной среды функционирования криптографии. Для этого в специальном разделе его памяти размещается все необходимое программное обеспечение.

При начале ДСС пользователь загружается с СОДС, обеспечивая тем самым доверенную среду. Далее стартуют браузер и все сопутствующее программное обеспечение, необходимое для работы. В браузере в доверенном сеансе обеспечивается защищенный обмен информацией с соблюдением всех требований Федерального закона № 63-ФЗ.

Загрузка производится из защищенной от записи памяти, жесткий диск компьютера не используется. Конфигурация загруженной операционной системы максимально ограничивает свободу пользователя: ему недоступны органы управления операционной системой, рабочая среда полностью изолирована от посторонних сетевых соединений, открытый трафик отсутствует, после завершения работы в браузере сеанс связи завершается, не давая пользователю делать лишнего.

СОДС устраняет «привязанность» пользователя и средств обеспечения информационной безопасности к конкретной рабочей станции, но обеспечивает уверенность в том, что если пользователь вообще подключился, то точно из доверенной среды.

После загрузки ОС на компьютер клиента и старта браузера устанавливается ДСС с сервером (VPN-шлюзом) центральной ИС, то есть защищенное соединение на основе криптографических алгоритмов. Закрытые ключи и сертификаты хранятся в защищенной памяти СОДС, и доступ к ним возможен только из операционной системы СОДС. Таким образом, исчезает «привязанность» пользователя и средств обеспечения информационной безопасности к конкретной рабочей станции, но появляется уверенность в том, что если пользователь вообще подключился, то точно из доверенной среды.

С точки зрения управления доступом СОДС представляет собой память, состоящую из нескольких разделов. В СОДС «МАРШ!» это, как правило, не менее одного раздела ReadOnly (RO), не менее одного раздела ReadWriteHidden (RWH), используются также разделы AddOnly (AO) и разделы с общим доступом RW. Разделение осуществляется при производстве и пользователем изменено быть не может.

Обычно в разделе RO размещаются операционная система и другое ПО, которое является неизменяемым достаточно длительное время. Обновления и дополнения ФПО размещаются в одном из разделов RWH, в другом размещается ключевая информация VPN, а раздел AO используется для ведения аппаратных журналов событий безопасности.

Безопасность безналичных расчетов: средства создания и поддержания доверенной среды

Взаимодействие клиента с банком в случае применения обыкновенного СОДС «МАРШ!» осуществляется через сетевые подключения компьютера.

Это совершенно нормально для компаний, но у обычного пользователя может вызвать трудности в настройках, так как на территории страны услуги предоставляют сотни провайдеров, зачастую с проприетарными механизмами.

Пользователю, не владеющему навыками работы с сетевыми подключениями, лучше предоставить ненастраиваемое устройство, избавив его от множества проблем. В этом случае взаимодействие может осуществляться не через компьютер, а непосредственно через СОДС.

В этом случае обеспечиваются и простота эксплуатации, и высокий уровень защищенности. Достигается такой режим путем встраивания в СОДС беспроводного модема. Настройка на провайдера обеспечивается только SIM-картой[1].

Такой подход позволяет использовать одно устройство как идентификатор, как носитель неизвлекаемых ключей, как модем и как устройство обеспечения ДСС. Остается только одно — освободить пользователя от необходимости иметь под рукой какой-либо компьютер, к которому можно было бы подключить СОДС. Такое решение тоже существует — в линейке микрокомпьютеров Новой гарвардской архитектуры.

Пользователю, не владеющему навыками работы с сетевыми подключениями, лучше предоставить ненастраиваемое устройство. Взаимодействие может осуществляться не через компьютер, а непосредственно через СОДС.

Микрокомпьютеры

Микрокомпьютер Новой гарвардской архитектуры (рис. 4) может быть подключен к любому монитору или телевизору, имеющему интерфейс HDMI[2]. В остальном все принципиально так же, как и в случае с СОДС.

Если средство обеспечения ДСС (будь то СОДС или микрокомпьютер) будет позиционироваться аналогично карточке — как собственность банка, предоставляемая клиенту на тех или иных условиях для получения услуги, ситуация будет выглядеть крайне привлекательно как для клиента, так и для банка. Клиент банка получает ненастраиваемое устройство, которое обеспечивает загрузку неизменяемой проверенной операционной системы, устанавливает защищенное с использованием криптографических алгоритмов

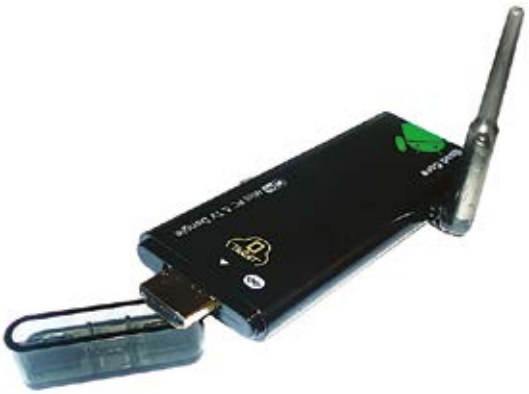
[1] См., напр.: okbsapr.ru/products/storage/compute/sods/m-m/.

[2] Конявский В.А. Защищенный микрокомпьютер МК-TRUST — новое решение для ДБО // Национальный банковский журнал. 2014. № 3.

Светлана КОНЯВСКАЯ

Рисунок 4

Микрокомпьютер МКТ



соединение с защищенным ЦОД, в котором установлено программное обеспечение (клиент ДБО) для доступа к АБС банка. Риски клиентов и банка сведены к минимуму.

Клиент ДБО (программное обеспечение) размещается в ЦОД, отвечающем всем требованиям по защите информации. Соответственно, доступ к АБС выполняется из одной достоверно известной точки — из ЦОД, по защищенному каналу.

В заключение напомним об одной существенной детали. Доверенная вычислительная среда обеспечивает корректность выполнения программ в том смысле, что они исполняются так, как написаны, как эталонная версия, без искажений. Однако она не защищает от ошибок программного обеспечения, ошибок проектирования системы, неверного выбора или неверного применения технологий.