УДК 004

Практика совмещения функций в защите информации: за и против

С. В. Конявская, канд. филол. наук
Закрытое акционерное общество "ОКБ САПР", Москва, Россия
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская обл., Россия

Рассматриваются и сравниваются между собой предлагаемые интеграторами и разработчиками решения задач в сфере защиты информации, включающие в себя совмещения разного рода (функций, областей применения, функциональных обязанностей).

Ключевые слова: два-в-одном, организационно-ролевая структура, Интернет, контуры защищенности, ключевые носители.

Концепция "два-в-одном" имманентна природе человека. Имеет смысл проанализировать тенденцию к проникновению подхода "два-в-одном" в защиту информации на самых разных уровнях.

При развитии любой идеи возникают добросовестные и недобросовестные ее воплощения, и недобросовестные способны скомпрометировать саму идею. Поэтому очень важно разграничить одно и другое как можно раньше.

Попробуем это сделать.

Как показала практика, идея совместить "два в одном" чаще всего возникает при выработке решения следующих задач.

- Оптимизация организационно-ролевой структуры. Под этим можно понимать любые мероприятия по перераспределению обязанностей, но в контексте защиты информации имеет смысл ограничиться случаями, касающимися функций управления и контроля.
- Организация возможности доступа в Интернет для сотрудников, компьютеры которых должны быть изолированы от сети Интернет по требованиям безопасности.
- Организация возможности выполнения отдельных критичных операций в среде более высокого уровня защищенности, изолированной от основной рабочей вычислительной среды. Эта задача обратна предыдущей: там выделена задача, которая не должна повлиять на рабочую среду, а тут выделена задача, на которую не должна повлиять рабочая среда.
- Обеспечение возможности доступа одного сотрудника в сегменты информационной системы с разными уровнями защищенности с одного рабочего места. Эта задача отличается от двух предыдущих тем, что в обоих – разных по требованиям к защищенности – контурах у пользователя должно быть полноценное рабочее место с некоторой относительно универсальной функциональностью.
- Организация мобильного рабочего места руководителя. Мобильное рабочее место руководителя отличается от мобильного рабочего места любого другого сотрудника в первую очередь тем, что руководителю необходимо обеспечить доступ к широкому спектру функций, а ограничения свести к минимуму, что в известной мере противоречит задаче обеспечения защищенности.
- Контроль среды применения криптографических ключей. Эту задачу нужно отличать от задачи создания и поддержания среды функционирования средства криптографической защиты информации (СКЗИ). СКЗИ может функционировать в корректной среде, а ключи будут скомпрометированы при подключении их носителя к совершенно другому компьютеру с совершенно другой средой.

Очевидно, что все задачи, кроме первой и последней, типологически близки, однако представляется уместным рассматривать их раздельно потому, что решения для них удобно применять (и они фактически применяются) разные.

Начнем по порядку.

Оптимизация организационно-ролевой структуры. Системной ошибкой в этом смысле является убежденность, что человек более управляем, чем техническое или программное средство, потому что с ним можно договориться. Очевидно, что именно поэтому он как раз менее управляем, потому что заметно менее предсказуем. Однако несмотря на многочисленные предупреждения в

Конявская Светлана Валерьевна, заместитель генерального директора, доцент, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru

Статья поступила в редакцию 5 июня 2017 г.

специальной и околоспециальной литературе, часто встречаются ситуации, когда один сотрудник является одновременно администратором системы и администратором безопасности этой же системы или администратором и пользователем какого-либо устройства, или — по сути это то же самое — являясь "функциональным пользователем" (то есть таким, который на данном ПК решает какие-то конкретные прикладные задачи), работает под учетной записью администратора.

Это примеры того, как делать не надо, не нуждающиеся в аргументировании в профессиональной аудитории.

Однако есть и положительные примеры, когда принцип "два-в-одном" в организационно-ролевой структуре усиливает защищенность системы. Это обратные примеры, когда два человека связаны различными способами с одной ролью.

Например, это схема доступа "четыре глаза", когда для работы приложения (или запуска системы, или входа в помещение) требуется аутентификация одновременно двух сотрудников — того, который зарегистрирован как Пользователь, и того, который зарегистрирован как Контролер.

В основу такой схемы работы обязательно должен быть положен хорошо продуманный сценарий, препятствующий тому, чтобы Контролер делегировал свои обязанности Пользователю, например передав ему свой идентификатор, или, в случае, если присутствие Контролера требуется не только в момент начала работы, а на протяжении всего сеанса, сценарий не должен быть ограничен контролем его присутствия в момент авторизации.

В продуктах ОКБ САПР для этого применяется следующий подход. Аппаратный идентификатор средств защиты информации (СЗИ) объединяется с пропуском СКУД. Это может быть как регистрация карточки СКУД в СЗИ НСД, так и физическое совмещение двух разных идентификаторов в зависимости от особенностей применяемой на объекте СКУД. Система управления СЗИ НСД интегрируется со СКУД в части передачи событий от одного сервера другому. Желательно (но не обязательно) при этом дополнить систему аутентификации считывателем биометрических данных. В описываемом далее примере используется комбинированный считыватель сосудистого русла ладони и бесконтактных карт rfid.

Сценарий работы выглядит следующим образом.

Пользователь и Контролер заходят в помещение, предъявив на считыватель СКУД свои карты. Событие о наличии сотрудников в помещении передается на сервер СЗИ НСД. При включении рабочего места Пользователь предъявляет карту и ладонь на считыватель из состава СЗИ НСД, затем снимает свою карту, и карту предъявляет Контролер. В случае, если регламентом предусмотрена работа при постоянно находящейся на считывателе карте, после снятия карты Контролера Пользователь снова кладет карту на считыватель и начинает работать. Если Контролер захочет покинуть помещение, он должен предъявить карту на считыватель СКУД, который передаст эти данные на сервер СЗИ НСД, и работа Пользователя будет заблокирована до повторной аутентификации Контролера. Естественно, попытка Пользователя покинуть помещение приведет к аналогичному поведению системы.

Сценарий может быть и совсем другим, он задается настройками. Главное, чтобы СЗИ принципиально предусматривало возможность создания учетной записи типа "Контролер" и выбора режима работы "с Контролером".

Важным может быть, например, с одним ли конкретным Контролером должен работать данный Пользователь или с любым, как именно должна система реагировать на попытку выхода Контролера, на снятие карты Пользователя, на попытку выхода Пользователя, на разблокировку не тем Контролером, который изначально авторизовался при старте, и так далее.

Другой случай "два-в-одном" в части организации работы сотрудников — так называемая "Коллективная учетная запись".

Это корректный способ организации контроля доступа для таких случаев, когда работа в прикладном программном обеспечении должна вестись без перерыва и, соответственно, необходимо продолжать сеанс Пользователя ОС дольше, чем может продолжаться смена работы одного сотрудника.

К сожалению, как правило, эта проблема решается таким образом, что под одной учетной записью с одним идентификатором и одним паролем работает несколько человек. В случае возникновение инцидента невозможно установить, кто же работал в это время на этом автоматизированном рабочем месте (АРМ).

Подход ОКБ САПР в этом случае следующий. Одной учетной записи ОС сопоставляется "Коллективная учетная запись" СЗИ НСД "Аккорд", в которой существует несколько разных пользователей. В журнале Аккорда они отображаются как разные, можно ясно понять, в какой момент фактический пользователь, т. е. человек, сотрудник, сменился. Смена Пользователя производится следующим образом. Пользователь, заканчивающий работу, снимает карту со считывателя, и АРМ блокируется. Пользователь, заступающий на сме-

ну, разблокирует АРМ своей картой. При этом сеанс операционной системы и, соответственно, технологический процесс не прерываются.

Доступ в Интернет для сотрудника, компьютер которого должен быть изолирован от сети Интернет. Эту задачу общество решает так давно, что решения уже кажутся очевидными. В отделах выделяется "рабочее место с Интернетом" или, для сотрудников более высокого иерархического статуса, собственный второй компьютер с Интернетом. Отсутствие влияния этого компьютера на остальные через подключаемые носители (ведь, как правило, сотрудник хочет не только что-то прочесть в Интернете, но и что-то оттуда скачать или скопировать) обеспечивается организационными мерами, но не технически. Очевидно, что это довольно плохое, хоть и широко применяемое решение.

Примерно 10 лет назад ОКБ САПР для одного проекта было реализовано другое решение, ставшее прототипом последующей технологии доверенного сеанса связи [1].

Решение построено на специально разработанном для этого переключателе дисков и выглядит следующим образом: ПК с двумя жесткими дисками, в который установлен "Аккорд-АМДЗ" на базе контроллера с USB-хостом, к которому подключен SATA-блокиратор. В зависимости от того, подключена ли к USB-хосту контроллера ШИПКА в момент подачи питания, коммутируется один или другой жесткий диск и после контрольных процедур АМДЗ загружается одна из соответствующих ОС, в каждой из которых установлено СПО "Аккорд".

Если подключен жесткий диск, предназначенный для обработки информации ограниченного доступа, второй жесткий диск, предназначенный для обработки общедоступной информации, будет недоступен физически: он просто не будет подключен к материнской плате. Значит, никакие ресурсы этого диска не смогут оказать влияния на доверенную среду. В случае же работы на втором жестком диске, имеющем недоверенные ресурсы, будет полностью исключен доступ к первому [2].

При этом поскольку на разных жестких дисках одного ПК в описываемой модели работа ведется под управлением разных ОС, с помощью настроек сети или специального ПО либо аппаратных решений несколько таких компьютеров можно объединить в локальную сеть на уровне ресурсов одного контура (уровня доступа), и для этой сети ресурсов другого уровня доступа вообще не будет существовать. Или они могут быть объединены параллельно в две изолированные друг от друга локальные сети.

Естественно, для того чтобы сменить контур, Пользователю необходимо перезагрузить компьютер.

По этой причине другой Заказчик ОКБ САПР в свое время не признал описанное решение в полной мере реализующим идеологию "два-в-одном" и поставил задачу разработать решение, не требующее даже перезагрузки, но тем не менее тоже надежно защищенное от всех прецедентов, связанных с использованием Интернета.

В качестве решения была предложена технология одновременной изолированной работы Пользователя с корпоративной сетью и сетью Интернет на одном рабочем месте в рамках двух независимых терминальных сессий с их одновременным отображением на экране одного монитора в разных "окнах" [3].

На основном терминальном сервере (будем называть его функциональным терминальным сервером — ФТС) нет ни браузера, ни других средств и инструментов работы с сетью Интернет.

К той же локальной сети, через которую взаимодействуют терминальные клиенты с ФТС, подключен другой терминальный сервер, но не напрямую, а через специальный фильтр, как показано на рис. 1.

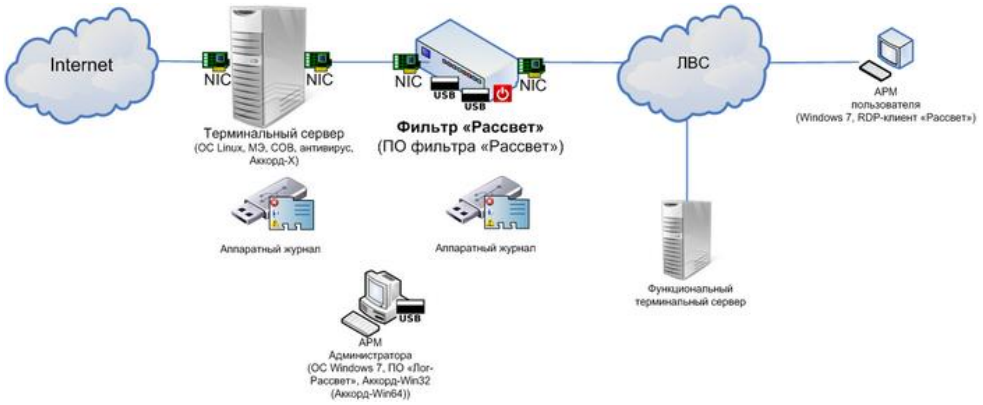

Рис. 1. Структурная схема комплекса технических средств решения

Это терминальный сервер (ТС) под управлением ОС Linux, имеющий соединение с сетью Интернет. На терминальном сервере опубликован браузер (рис. 1).

Обмен данными между ТС и сетью Интернет производится в штатном порядке, без ограничений. Для соединения с Интернетом у ТС предусмотрена отдельная сетевая карта, установлен полный комплект средств защиты информации: средства защиты от воздействия вредоносных кодов (СЗ ВВК), средство обнаружения вторжений (СОВ), межсетевой экран (МЭ), ПАК СЗИ НСД "Аккорд-X".

Через отдельный сетевой интерфейс (вторую сетевую карту) ТС взаимодействует с аппаратным комплексом с функциональностью фильтра (фильтр "Рассвет"). У фильтра тоже две сетевые карты. Через одну из них фильтр взаимодействует с ТС (получает все команды и данные, которые не были заблокированы МЭ, СОВ, СЗ ВВК или ПАК СЗИ НСД "Аккорд-X").

От фильтра на ТС передаются только нажатия клавиш клавиатуры и движение мыши. Через другой сетевой интерфейс (вторую сетевую карту) фильтр взаимодействует с ЛВС предприятия. От фильтра в ЛВС передаются только изображения рабочего стола. От ЛВС в фильтр передаются все данные и команды без ограничений.

Взаимодействие Пользователя с ЛВС производится через установленный на АРМ Пользователя модифицированный RDP-клиент (далее RDP-клиент "Рассвет"). Для Пользователя взаимодействие происходит обычным порядком, без изменений, все изменения взаимодействия от него скрыты. Он работает параллельно в окне браузера и в окне сессии с ФТС — "два-в-одном".

Схематично взаимодействие компонентов системы показано на рис. 2.

Изоляция вычислительной среды, предназначенной для выполнения отдельных критичных операций (например, клиент—банк, или подписание документов электронной подписью — ЭП), *от основной рабочей вычислительной среды*. Как уже было сказано, это задача идеологически обратная. Мы изолируем не опасную среду, а наоборот, самую чувствительную к защищенности. Это классическая задача для доверенного сеанса связи, понимаемого как *кратковременный* период работы с удаленным защищенным ресурсом с компьютера, на который загружена доверенная среда организации этого сеанса.

Рассмотрим особенности этого сценария. В подавляющем большинстве случаев человек не нуждается в доверенной среде, он не работает с чувствительными к безопасности ресурсами и не выполняет критичных с точки зрения безопасности операций. Таких действий большинство людей производят не более чем несколько за день: перевести деньги online, получить госуслугу, подписать документ (предположим, что вне задач получения госуслуг или перевода денег). Все остальное время доверенная среда будет человеку только мешать, потому что она ограничивает далеко не один Интернет.

Часто из-за этого люди просто идут на риск. Такой вариант рассматривать не будем.

Другой вариант, средний, до сих пор применяется в заметном числе очень уважаемых организаций. Это те же два компьютера на одном рабочем месте. За одним сотрудник работает весь день, а за другой садится по мере необходимости поработать в доверенной среде. Часто дополнительным доводом в пользу такого очевидно неэкономичного решения является то, что основное рабочее место, типовое для всех (или большинства) сотрудников, отличается вовсе не тем, что оно незащищенное,

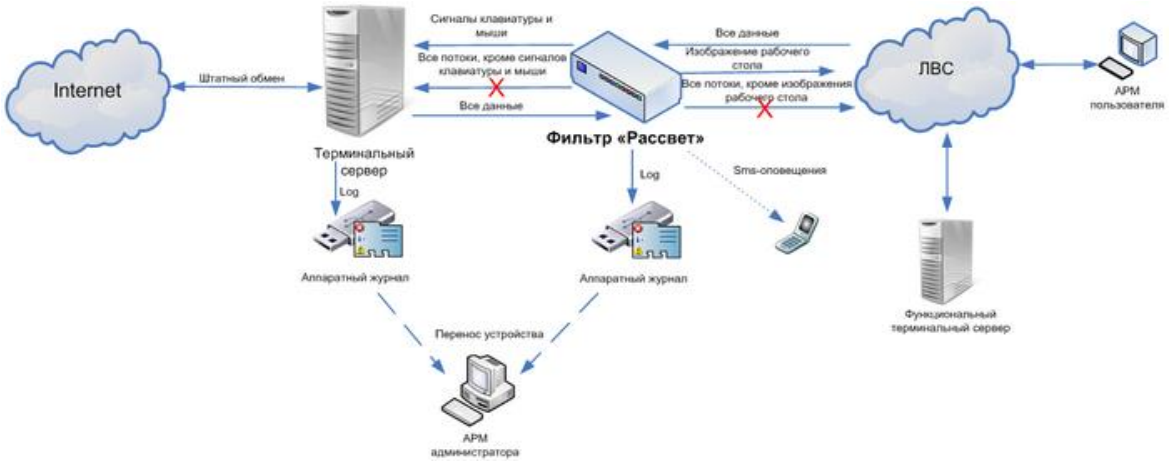

Рис. 2. Функциональная схема решения

а тем, что оно не обладает достаточными вычислительными ресурсами или иными специфическими характеристиками, требующимися для выполнения этих отдельных операций, а вместо перепроектирования системы якобы проще и дешевле поставить отдельным сотрудникам по второму компьютеру (снова принцип "два-в-одном").

Здесь предлагаются другие варианты.

Для случая, когда основное рабочее место стационарное и имеет сетевой интерфейс, оптимально СОДС МАРШ!. МАРШ! обеспечивает загрузку доверенной неизменяемой среды, хранящейся в его защищенной памяти с управляемым доступом, и, с использованием сетевых ресурсов ПК, подключение к нужному информационному ресурсу, защищенное VPN.

В тех случаях, когда основные компьютеры не имеют сетевого интерфейса либо его нельзя или неудобно использовать (например, это ноутбук с WiFi-модулем сетевые настройки которого всякий раз могут оказаться разными), целесообразно применение специфической версии МАРШ!а — М!&М, что расшифровывается как "МАРШ! и Модем" [1, 4]. Как очевидно из названия, это устройство, имеющее собственный модуль подключения к беспроводной сети. Во всем остальном схема работы получается точно такой же, просто для установления доверенного сеанса связи не используются сетевые ресурсы основного ПК.

Отметим, что, строго говоря, ничто не мешает при использовании этих подходов основное рабочее место тоже делать защищенным так, как это требуется политикой предприятия. Но если задача осознана уже на стадии проектирования, то можно выбрать решение "под ключ" — двухконтурный моноблок.

Двухконтурный моноблок — это моноблок, позволяющий Пользователю работать в одной из двух защищенных ОС (в общем случае одна из них — Windows, а другая — Linux). ОС Windows загружается с жесткого диска моноблока. При работе в этом режиме Пользователь может устанавливать любое ПО и инициировать любые подключения в рамках заданных для него правил разграничения доступа: в ОС установлен ПАК "Аккорд-Win64".

При запуске двухконтурного моноблока во втором режиме ОС загружается из защищенного от записи раздела памяти микрокомпьютера «MKT-card long». При работе в этом режиме Пользователю доступно только то ПО, которое изначально установлено в образ ОС; этот состав определяется при заказе и затем может изменяться только в рамках обновления ОС в установленном порядке по специальной защищенной процедуре.

Переключение между режимами выполняется посредством KVM-переключателя для передачи сигналов клавиатуры и мыши к текущей системе и нажатия кнопки переключения для смены экрана, расположенной на корпусе моноблока.

Таким образом, один моноблок сочетает в себе две на физическом уровне изолированные одна от другой ОС разных семейств, обе они защищены, но каждая по специфичным для своих задач требованиям.

Еще одно решение – это целая ветка семейства защищенных компьютеров на базе Новой гарвардской архитектура МКТ — компьютеры MKTrusT [5, 6]. Это микрокомпьютеры, позволяющие работать в одном из двух режимов — защищенном и незащищенном. Работа в разных режимах производится в разных ОС, загружающихся из разных, физически разделенных разделов памяти (т. е. взаимовлияние ОС исключено технологически). Переключение режимов работы производится с помощью физического переключателя, расположенного на корпусе устройства, т. е. необходимый режим выбирает Пользователь и не может выбрать хакер (невозможно программное воздействие на выбор режима). К этой ветке относяться собственно модель MKTrusT, а также защищенный планшет TrusTPad.

Незащищенная ОС в обоих случаях Android, а защищенная — обычно Linux в MKTrusT, Android в TrusTPad, но может быть и наоборот в зависимости от задач той системы, под которую адаптируется решение.

Доступ одного сотрудника в сегменты информационной системы с разными уровнями защищенности с одного рабочего места. Эта задача принципиально близка предыдущим, разница состоит только в потенциальной широте функциональности "второй" рабочей среды. В предыдущих случаях это отдельные задачи (заметно более опасные, или заметно более чувствительные к защищенности, чем основная среда), а в этом случае обе среды "полнофункциональные" — с некоторым множеством приложений, но разными ограничениями.

Вместе с тем сложилось так, что как раз такая задача крайне редко решается путем настройки для одного сотрудника двух компьютеров. Заметно чаще настраивают два разных профиля пользователя. Вообще говоря, это можно сделать действительно защищенно, если изолировать среду полностью, от старта компьютера. Однако зачастую этого не происходит. Как правило, задача касается работы в режиме удаленного доступа, а не локальной, а компьютер, с которого осуществляется доступ, воспринимается как терминал, ко-

торому можно уделять крайне мало внимания с точки зрения защиты информации. Профили создаются, предположим, на разных терминальных серверах, оборудованных комплектами всех необходимых защитных средств, сервера работают в разных сетях, возможно разделенных физически, а не только логически. Все сделано крайне добросовестно, кроме одного: компьютер, с которого осуществляется доступ, — один и тот же. Более того, как правило, он загружен под профилем одного и того же Пользователя ОС и, в случае, если на нем вообще установлено СЗИ НСД, — под профилем одного и того же Пользователя СЗИ НСД, а значит, последний обладает с одними и теми же правами, ему доступны одни и те же ресурсы компьютера при работе в разных контурах системы. Такая ситуация создает опасную иллюзию изолированности контуров друг от друга, оставляя очень удобную для потенциального нарушителя уязвимость.

Избежать данной проблемы можно с помощью целого ряда решений, различными способами реализующих принцип "два-в-одном". Это уже упоминавшиеся МАРШ!, МКTrusT и двухконтурный моноблок. В данном случае особенность решений состоит в том, "куда ведет" ОС, загружаемая с МАРШ! и с МКТ-card long. Если в предыдущем случае эти ОС содержали средства выполнения той конкретной задачи, для которой нужна особая среда исполнения, то в данном случае они будут, например, содержать терминальный клиент для доступа к нужному серверу или VPN-клиент к нужному шлюзу и межсетевой экран, настроенный так, чтобы позволить доступ к строго определенному веб-ресурсу, и т. п. При этом ОС, загруженной с МАРШ!а, будут недоступны сетевые ресурсы, доступные из "основной" ОС компьютера. Разумеется, возможность доступа в тот или иной контур только из той или иной среды должна быть поддержана системой защиты информации самого централизованного ресурса (терминального или веб-сервера, виртуальной системы или иного, к которому идет подключение), иначе в один и тот же контур можно будет попасть и с МАРШ!ем, и без него.

Решением, очень близким по "внешним" признакам, также нацеленным на доступ с одного СВТ в два разных контура, является ПАК "Центр-Т" [7]. С применением этого комплекса можно реализовать даже две разные стратегии. Если в качестве рабочих мест используются машины, изначально пригодные для применения в одном из контуров, то доступ в один из контуров осуществляется из их собственной ОС, а во второй — из ОС, загружаемой с помощью "Центр-Т". Если же зоопарк терминалов таков, что управлять ими слишком сложно, то целесообразно сопоставить клиентским устройствам по 2 загружаемых образа и при старте выбирать, какой получить в данный момент. Один образ будет инициировать сессию в одном контуре системы, а другой — в другом.

Мобильное рабочее место руководителя. Руководитель — это категория людей, которым необходимо обеспечить режим работы со сведенными к минимуму ограничениями. Именно поэтому даже в организациях с очень серьезным подходом к обеспечению защиты информации для них всегда стараются найти возможность сделать разнообразные исключения: разрешить Интернет, флешки, планшеты и т. д.

К сожалению, обычно это выливается не в действительно защищенное решение, а в имитацию защиты по принципу «раз есть какой-то защитный механизм, значит, все в порядке». Например, на планшет устанавливается VPN-клиент, но не устанавливаются средства доверенной загрузки; в ноутбук устанавливается две ОС, одна из которых контролируется первым и единственным в мире аппаратным модулем доверенной загрузки, не имеющим в своем составе аппаратного модуля.

Мы предлагаем не ограничивать руководителя в праве работать в защищенной среде. В случае с планшетом это уже упоминавшийся TrusTPad с двумя режимами работы в одном. В случае с ноутбуком — это ПАК "Ноутбук руководителя" [8]. Это действительно ноутбук, в котором за счет предустановленных средств защиты реализована возможность выбора того, какую среду загружать: основную ОС ноутбука или защищенную ОС из контроллера "Аккорд", предназначенную для соединения с защищенной информационной системой.

Обычный режим характеризуется тем, что безопасность сетевых соединений не контролируется, действия Пользователя не ограничены, а ОС загружается из памяти ноутбука.

При выборе защищенного режима ОС загружается из защищенной от записи памяти комплекса СЗИ НСД "Аккорд-АМДЗ", входящего в состав ПАК "Ноутбук руководителя"; жёсткий диск ноутбука не используется. Кроме того, пользователю предоставляется изолированная среда, в которой единственным доступным соединением является соединение, разрешенное администратором.

Режим выбирается Пользователем при включении ноутбука, когда загружается сервисная ОС из состава ПАК "Ноутбук руководителя", проверяющая наличие привязанной к ноутбуку смарт-карты Пользователя в считывателе.

Работа с ключами в доверенной среде. Постепенно, в основном, к сожалению, усилиями регуляторов необходимость работы с ключами исключительно в доверенной среде становится осознанной. На смену заявлениям о том, что для безопасной работы с ДБО, например, достаточно использовать токены, приходят решения "два-в-одном", имитирующие СОДС МАРШ!, — "токены с памятью". Это устройства, помимо токена включающие в себя флеш-память, на которой в виде live-CD записан образ ОС, загружающейся на компьютер и создающей ощущение доверенной среды.

Рассмотрим "МАРШ!" в сравнении с получившими некоторое распространение устройствами, совмещающими в едином конструктиве токен и флешку (рис. 3) [1, 2].

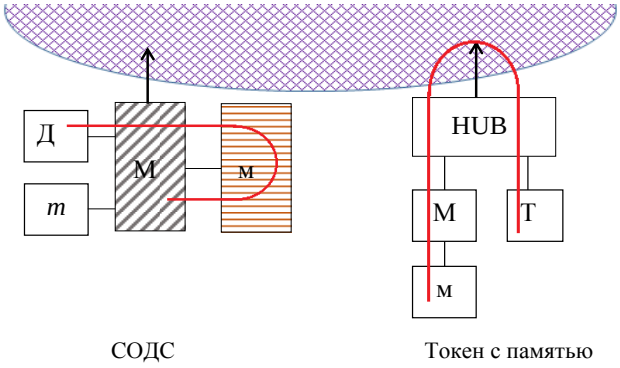

Рис. 3. Архитектура аппаратных средств
(СОДС: Д — датчик случайных чисел, *m* — память кода, М — универсальный микроконтроллер, м — память;
Токен с памятью: HUB — USB-хаб, М — специализированный микроконтроллер, м — память, Т — токен)

На рис. 3 затенена зона компьютера, а изогнутой линией показано движение критичных для безопасности данных. Видно, что во втором случае критичные данные проходят через память компьютера. Это не опасно, если среда доверенная, но доверенной ее можно считать в том случае, когда контрольные процедуры выполнены **до загрузки.** Последнее возможно для архитектуры, показанной в левой части рисунка, и невозможно для альтернативной архитектуры.

"Токен с флешкой" — это два разных устройства, объединенных хабом в единый конструктив. В этом, казалось бы, нет ничего плохого. Действительно, с флешки, входящей в состав устройства, загружается фиксированная среда, которую признаем доверенной. Следовательно, совершенно допустимо получить ключи из токена через посредство этой самой доверенной среды.

Однако компоненты "токена с памятью" не взаимодействуют. Токен ничего не знает о том, загружена ли среда, которая его вызывает, из памяти того же USB-stick'а или откуда-то еще. Это обыкновенный токен, который не различает "свою" и "чужую" среду.

Компоненты "МАРШ!" управляются централизованно собственным микроконтроллером устройства, и до того, как они отработают все процедуры (и/а, загрузка ОС, загрузка СЗИ и т. д. в зависимости от состава образа ОС данного конкретного "МАРШ!а"), о доступе к ключам просто невозможно поставить вопрос. Все взаимодействие между компонентами "МАРШ!" осуществляется внутренними ресурсами микроконтроллера, что дает возможность на стадии контрольных процедур быть полностью независимым от внешней среды и загружать гарантированно доверенную среду.

Однако очевидно, что не во всех без исключения случаях работать с ключами целесообразно в рамках доверенного сеанса связи. Работать же с ними в доверенной среде требуется во всех без исключения случаях.

Значит, необходимо еще какое-то решение, позволяющее контролировать, куда подключили токен с ключами — туда, куда можно, или туда, куда нельзя.

Такое решение — "два-в-одном" — токен и "Секрет" [9] или "Идеальный токен".

"Идеальный токен" монтируется к компьютеру только в том случае, если этот компьютер указан в "Идеальном токене" его администратором как разрешенный для работы [10]. В любом другом случае ключи недоступны как Пользователю, даже знающему PIN-код, так и вредоносному программному обеспечению, потенциально установленному на том компьютере, на котором Пользователь решает зачем-то поработать с ключами.

Очевидно, что любая идея имеет и хорошие, и плохие отражения. Имея достаточную для анализа информацию о предлагаемых на рынке защиты информации технических решениях, вполне можно не попадать под влияние идей в ущерб здравому смыслу и в то же время не отказываться от них из-за отдельных не совсем удачных их реализаций. В заключение для наглядности представим получившуюся картину в виде таблицы.

Сравнение решений задач в сфере защиты информации, включающих совмещения разного рода

Задача	Неудачный вариант	Удачный вариант
Оптимизация организационно-ролевой структуры	Совмещение двух ролей одним сотрудником	Режим "четыре глаза"; "коллективная учетная запись"
Доступ в Интернет для сотрудника, компьютер которого должен быть изолирован от сети Интернет	Два СВТ на одном рабочем месте, один из которых предназначен только для Интернета	Два диска через sata-коммутатор; соединение с Интернетом через фильтр "Рассвет" во второй терминальной сессии
Изоляция вычислительной среды, предназначенной для выполнения отдельных критичных операций, от основной рабочей вычислительной среды	Два СВТ на одном рабочем месте, один из которых предназначен только для выполнения критичной функции	Двухконтурный моноблок; M!&M; МАРШ!; защищенные микрокомпьютеры линейки МКTrusT
Доступ одного сотрудника в сегменты информационной системы с разными уровнями защищенности с одного рабочего места	Вход в два контура с одного СВТ (по разным идентификаторам)	МАРШ!; двухконтурный моноблок; доступ в два контура с применением ПАК Центр-Т
Мобильное рабочее место руководителя	Ноутбук с двумя ОС, одна из которых защищена программно; планшет без доверенной среды, но с VPN, который должен обеспечить работу в защищенном режиме	Ноутбук руководителя; TrusTPad
Работа с ключами в доверенной среде	Токен с памятью	МАРШ!; Идеальный токен

Литература

1. *Конявский В. А.* Серебряная пуля для хакера (Окончание) // Защита информации. 2013. № 5. С. 69—73.
2. *Конявская С. В., Счастный Д. Ю., Кубеев Е. О., Ясиновская Е. Д.* Технология доверенного сеанса связи (ДСС) и средство обеспечения доверенного сеанса связи (СОДС) "МАРШ!": методическое пособие / Под общей ред. Конявского В. А. —М.: НИЯУ МИФИ, 2015. — 128 с.
3. *Конявская С. В., Кравец В. В., Батраков А. Ю.* Безопасный Интернет: видимость как необходимое и достаточное // Вопросы защиты информации.2014. № 4. С. 41—45.
4. Модем для безопасных коммуникаций в компьютерных сетях. Патент на полезную модель № 128055. Опубл. 10.05.2013. Бюл. № 13.
5. *Конявский В. А.* Компьютер с "вирусным иммунитетом" // Информационные ресурсы России. 2015. № 6. С. 31—34.
6. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. Опубл. 20.03.2014. Бюл. № 8.
7. Способ защиты от несанкционированного доступа к информации, хранимой в компьютерных системах. Патент на изобретение № 2470349. Опубл. 20.12.2012. Бюл. № 35.
8. *Счастный Д. Ю.* Ноутбук руководителя: мат. XX научно-практической конф. "Комплексная защита информации". Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015. С. 12—113.
9. *Бирюков К. А.* Средства безопасного хранения ключей // Безопасность информационных технологий. 2013. № 3. С. 50—53.
10. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. Опубл. 10.11.2014. Бюл. № 31.

The practice of combining functions in the protection of information: the pros and cons

S. V. Konyavskaya

Closed Joint Stock Company "OKB SAPR", Moscow, Russia

Moscow Institute of Physics and Technology (state university), Dolgoprudny, Moscow region, Russia

The article suggests the comparison of solutions being offering by developers and integrators in field of information security, that include different kinds of combination (function, sphere of use, functional duties joining).

Keywords: all-in-one, role structure, Internet, safety counters, token.

Bibliography — 10 references. *Received June 5, 2017*