Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ИДЕОЛОГИЯ «ДВА-В-ОДНОМ» КАК СПОСОБ ПОВЫШЕНИЯ И СНИЖЕНИЯ ЗАЩИЩЕННОСТИ

С.В. КОНЯВСКАЯ

Закрытое акционерное общество «ОКБ САПР»

Концепция «два-в-одном» имманентна природе человека. С этим согласны и приверженцы версии о его (человека) дуалистической природе (тело и душа), и те, кто считает, что человек – как и все остальное в Мире – триада (тело-душа-дух), ведь два (душа и дух) – таки в одном (теле).

Не углубляясь в вопрос, сколько же это всего – «два-в-одном» – два или все же три, имеет смысл проанализировать тенденцию к проникновению этого подхода в защиту информации на самых разных уровнях.

Как происходит всегда, когда идея овладевает массами, возникают добросовестные и недобросовестные ее воплощения, и недобросовестные способны скомпрометировать на корню саму идею. Поэтому очень важно разграничить одно и другое как можно раньше. Попробуем это сделать.

Как показала практика, идея совместить два чего-то в одном чаще всего возникает при выработке решения следующих задач:

1) 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.

2) Организация возможности доступа в Интернет для сотрудников, компьютеры которых должны быть изолированы от сети Интернет по требованиям безопасности.

3) 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.

4) 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.

5) 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.

6) Контроль среды применения криптографических ключей. Эту задачу нужно отличать от задачи создания и поддержания среды функционирования 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 фактически применяются) разные.

Но начнем по порядку.

1. 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 нотации в специальной и околоспециальной литературе, в порядке вещей 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 все примеры того, как делать не надо, и это, конечно, не нуждается в аргументировании в профессиональной аудитории.

Однако есть и положительные примеры, когда «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 основе 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 Контроллера требуется не только в момент начала работы, а на протяжение всего сеанса, то 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 объединяется с пропуском СКУД. Это может быть, как регистрация карточки СКУД в СЗИ НСД, так и физическое совмещение двух разных идентификаторов – это зависит 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 примере используется комбинированный считыватель сосудистого русла ладони и бесконтактных карт rfid.

Сценарий работы выглядит так.

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, он 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 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 – это 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, возможности сменить сеанс пользователя ОС, дольше, чем может продолжаться смена работы одного сотрудника.

К сожалению, как правило, эта коллизия решается таким образом, что в одной учетной записи с одним идентификатором и одним паролем работает несколько человек. Такое вот «два-в-одном», при котором в последствии невозможно установить, если, не дай Бог, произошел инцидент, кто же работал в это время на этом 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, то есть человек, сотрудник – сменился. Смена пользователя производится так – пользователь, заканчивающий работу, снимает карту со считывателя, и АРМ блокируется. Пользователь, заступающий на смену, разблокирует АРМ своей картой. При этом сеанс операционной системы и, соответственно, технологический процесс – не прерываются.

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

Довольно давно, примерно 10 лет назад ОКБ САПР для одного проекта было реализовано другое решение, ставшее прототипом технологии доверенного сеанса связи в тогда еще далеком будущем [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 соответствующая 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 подключен к материнской плате, значит, никакие ресурсы этого диска не смогут оказать влияния на доверенную среду. А в случае же работы на втором жестком диске, имеющем недоверенные ресурсы, будет полностью исключен доступ к первому [2].

Причем поскольку на разных жестких дисках одного ПК в описываемой модели работа ведется под управлением разных ОС, то 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 наш Заказчик в свое время не признал это 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 Интернет-неприятностей.

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 «функциональный терминальный сервер» (ФТС) — нет ни браузера, ни каких 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 рисунке.

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

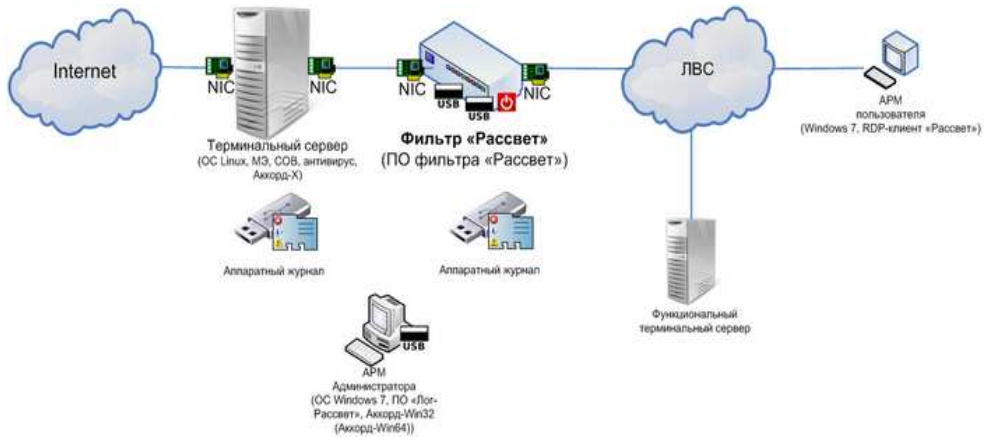


Рис. 1 – Структурная схема комплекса технических средств решения

Обмен данными между ТС и сетью Интернет производится в штатном порядке, без ограничений. Для соединения с Интернет у ТС предусмотрена отдельная сетевая карта, установлен полный комплект средств защиты информации: средства защиты от воздействия вредоносных кодов, средство обнаружения вторжений, межсетевой экран, ПАК СЗИ НСД «Аккорд-Х».

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-Х»).

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 рисунке 2.

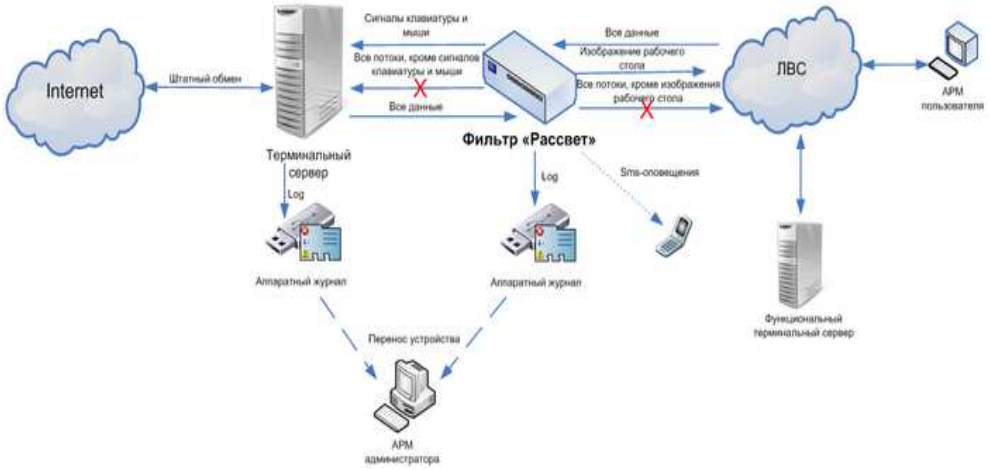


Рис. 2 – Функциональная схема решения

3. Изоляция вычислительной среды, предназначенной для выполнения отдельных критичных операций (например, клиент-банк, или подписание документов 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.

В чем особенности этого сценария. В подавляющем числе 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 у большинства людей случается не более, чем несколько за день. Перевести деньги online, получить гос.услугу, подписать документ (предположим, что вне задач получения гос.услуг или перевода денег, а для чего-то еще). Все остальное время доверенная среда ему будет только мешать, потому что она ограничивает далеко не только Интернет.

Часто из-за этого люди просто идут на риск. Это вариант настолько скверный, что рассматривать его не будем совсем.

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, а тем, что оно не обладает достаточными вычислительными ресурсами или какими-то еще специфическими характеристиками, требующимися для выполнения этих отдельных операций, и вместо того, чтобы перепроектировать систему так, чтобы все увязать, будто бы проще и дешевле поставить отдельным сотрудникам по второму компьютеру. Чем не «два-в-одном».

Мы предлагаем 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, или его нельзя использовать, или это неудобно (например, это ноутбук с WiFi-модулем, и значит, сетевые настройки всякий раз могут оказаться разными) – целесообразно применение специфической версии МАРШ!а – «М!&М», что расшифровывается как «МАРШ! и Модем» [1, 4]. Это устройство, как очевидно из названия, имеющее собственный модуль подключения к беспроводной сети. Во всем остальном схема работа получается точно такой же, просто для установления доверенного сеанса связи не используются сетевые ресурсы основного ПК.

Обратим внимание, что, строго говоря, ничто не мешает при использовании этих подходов основной 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, собственно, моноблок, позволяющий пользователю работать в одной из двух защищенных ОС (в общем случае одна из них Windows, а вторая – Linux). В 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 «МКТ-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 изолированных одна от другой ОС разных семейств, обе из которых 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 МКТrusT [5, 6]. Это микрокомпьютер, позволяющий работать в одном из двух режимов – защищенном или незащищенном. Работа в разных режимах производится в разных ОС, загружающихся из разных, физически разделенных, разделов памяти (то есть взаимовлияние ОС исключено технологически). Переключение режимов работы производится с помощью физического переключателя, расположенного на корпусе устройства, то есть необходимый режим

выбирает пользователь, и не может выбрать хакер (невозможно программное воздействие на выбор режима). В этой ветке есть собственно модель МКTrusT, а также защищенный планшет TrusTPad.

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

4. Доступ одного сотрудника в сегменты информационной системы с разными уровнями защищенности с одного рабочего места.

Эта задача принципиально близка предыдущим, разница 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 практика сложилась так, что как раз такая задача крайне редко решается путем настройки для одного сотрудника двух компьютеров. Заметно чаще для этого настраивают два разные профиля пользователя. Вообще говоря, это можно сделать действительно защищенно, если изолировать среду полностью, от старта компьютера. Однако зачастую этого не происходит, потому что, как правило, задача касается работы в режиме удаленного доступа, а не локальной, а при этом компьютер, с которого осуществляется доступ, воспринимается как терминал, которому 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, 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 один от другого, оставляя очень удобную для потенциального нарушителя уязвимость.

Избегнуть ее можно с помощью целого ряда наших решений, различными способами реализующих «два-в-одном». Это уже упоминавшиеся МАРШ!, МКTrusT и двухконтурный моноблок. В данном случае особенность решений будет в том, «куда ведет» ОС, загружаемая с МАРШ! и с МКТ-card long соответственно. Если в предыдущем случае эти ОС содержали средства выполнения той конкретной задачи, для которой нужна особая среда исполнения, но 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 тому подобное. При этом ОС, загруженной с МАРШ!а будут не доступны сетевые ресурсы, доступные из «основной» ОС компьютера. Разумеется, возможность доступа в тот или иной контур только из той или иной среды должны быть поддержана системой защиты информации самого централизованного ресурса (терминального или веб-сервера, виртуальной системы, или того иного, к чему, собственно, подключаемся), иначе в один и тот же контур можно будет попасть и с МАРШ!ем и без. А такое «два-в-одном» никому не нужно.

Решением, очень близким по «внешним» признакам, также нацеленным на доступ с одного СВТ в два разные контура, является ПАК «Центр-Т» [7]. С применением этого комплекса можно реализовать даже сразу две разные стратегии. Если в качестве

рабочих мест используются машины, пригодные для применения в одном из контуров как они есть, 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.

5. Мобильное рабочее место руководителя. Руководитель – эта такая 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 всяческие исключения – и разрешить Интернет, флешки, планшеты – в общем, все, что нельзя, но очень хочется.

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. Или 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, а в случае с ноутбуком – это ПАК «Ноутбук руководителя» [8]. Это действительно ноутбук, в котором за счет предустановленных средств защиты реализована возможность выбора, какую среду загружать — основную ОС ноубтука, 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 защищённой 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.

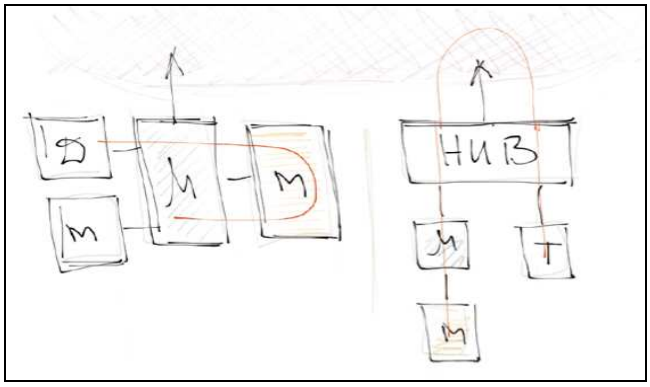
Режим выбирается пользователем при включении ноутбука, когда загружается сервисная ОС из состава ПАК «Ноутбук руководителя», проверяющая наличие привязанной к ноутбуку смарт-карты пользователя в считывателе.

6. Работа с ключами в доверенной среде. Постепенно, в основном, к сожалению усилиями регуляторов, необходимость работы с ключами исключительно в доверенной среде становится осознанной. И 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 такие устройства, которые помимо токена включают в себя флеш-память, на которой в виде live-CD записан образ ОС, которая загружается на компьютер и создает ощущение доверенной среды.

Рассмотрим «МАРШ!» в сравнении с получившими сегодня некоторое распространение устройствами, совмещающими в едином конструктиве токен и флешку [1, 2].

На рисунке затенена зона компьютера, а красной 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 доверен-

ной ее можно считать в том случае, если контрольные процедуры выполнены ДО ЗАГРУЗКИ, и это возможно для архитектуры, показанной в левой части рисунка, и невозможно для альтернативной архитектуры.



СОДС (слева) и «токен с памятью» (справа).
Архитектура аппаратных средств (Д – датчик случайных чисел, т – память кода, М – универсальный микроконтроллер, м – память; HUB – USB-хаб, М – специализированный микроконтроллер, м – память, Т – токен)

«Токен с флешкой» – это два разных устройства, объединенных hub'ом в единый конструктив. В этом, казалось бы, нет ничего плохого, потому что с флешки, входящей в состав устройства, загружается фиксированная среда, которую признаем доверенной, стало быть, совершенно допустимо и нормально получить ключи из токена через посредство этой самой доверенной среды.

Это не совсем так. Принципиальная ущербность описанной архитектуры в том, что для передачи данных между двумя совмещенными устройствами (токеном и памятью) необходима их передача наружу, во внешнюю среду. Это означает, что контрольные процедуры не могут быть выполнены независимо от внешней недоверенной среды. Как бы ни была логически построена процедура доступа, физически устройство построено так, что взаимодействие между его компонентами требует «участия» в этом процессе внешней ОС. Данные для управления доступом к каждому «защищенному» хранилищу поступают снаружи, значит, не могут считаться доверенными.

Именно эта особенность привела к необходимости использовать универсальный микроконтроллер, а не смарт-карточный кристалл, как в токене. 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. А работать с ними в доверенной среде нужно во всех без исключения случаях.

Значит, нужно 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] – это «Идеальный токен», еще одно наше решение.

«Идеальный токен» – это токен, который монтируется к компьютеру только в том случае, если этот компьютер указан в «Идеально 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 решил зачем-то поработать с ключами.

Очевидно, что любая идея (в платоновском смысле) имеет и хорошие, и плохие отражения (в платоновском же смысле). Но имея достаточную для анализа информацию о предлагаемых на рынке защиты информации технических решениях мы вполне можем не попадать под обаяние идей в ущерб здравому смыслу, и в то же время не отказываться от них из-за отдельных не совсем удачных их реализаций. В одном популярном телесериале Шерлок Холмс говорит: «нельзя же судить идею только по результату!». Высказывание экстравагантное, но по сути верное.

И в заключение для наглядности представим получившуюся картину в виде таблицы.

Задача	Плохо:	Хорошо:
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 только для Интернет	два диска через sata-коммутатор; соединение с Интернет 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 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 которой 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

Список литературы

1. *Конявский В. А.* Серебряная пуля для хакера (Окончание) // Защита информации. INSIDE. СПб., 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 редакцией В. А. Конявского. 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: Научно-практический журнал/ФГУП «ВИМИ», 2014. Вып. 4 (107). С. 41-45.

4. Модем для безопасных коммуникаций в компьютерных сетях. Патент на полезную модель № 128055. 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. 20.03.2014, бюл. № 8.

7. Способ защиты от несанкционированного доступа к информации, хранимой в компьютерных системах. Патент на изобретение № 2470349. 20.12.2012, бюл. №35.

8. *Счастный Д. Ю.* Ноутбук руководителя // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. – Минск: РИВШ, 2015. С. 112–113.

9. *Бирюков К. А.* Средства безопасного хранения ключей // Безопасность информационных технологий. М., 2013. № 3. С. 50–53.

10. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014, бюл. №31.

О ПРОБЛЕМЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНФРАСТРУКТУРЫ ВИРТУАЛИЗАЦИИ

С.С. ЛЫДИН

Закрытое акционерное общество «ОКБ САПР»

Проектирование системы защиты информации для информационной системы (ИС), как правило, подразумевает выполнение следующих мероприятий:

определение состава организационных и технических мер защиты информации, подлежащих реализации;

определение видов и типов средств защиты информации (СЗИ), обеспечивающих реализацию технических мер защиты информации в соответствии с результатами выполнения этапа 1;

выбор моделей средств защиты информации в соответствии с результатами выполнения этапа 2, сертифицированных на соответствие требованиям по безопасности информации.

На почве многочисленных дискуссий, ведущихся в профессиональных кругах, у владельца ИС при выполнении этапа 2 довольно часто возникают трудности, связанные с принятием решения, какие СЗИ предпочтительнее использовать: *встроенные* в системное и прикладное программное обеспечение или *наложенные*.

При этом следует отметить, что в отношении систем, реализующих технологии виртуализации и облачных вычислений, указанная проблема выбора, как правило, не актуальна. Дело в том, что наиболее востребованные на сегодняшний день программные среды виртуализации не содержат *встроенных* СЗИ, сертифицированных для использования в ИС достаточно высоких классов. Таким образом, область поиска подходящего решения для владельца подобной системы, как правило, ограничивается только множеством *наложенных* СЗИ.

В то же время получил достаточно широкое распространение тезис, согласно которому соотношение сил могло бы оказаться иным – в случае наличия у программных комплексов со *встроенными* функциями защиты среды виртуализации необходимых сертификатов безопасности. Зачастую принято считать, что по большинству других показателей превосходство *встроенных* СЗИ над *наложенными* не вызывает сомнений.