УДК 004.3

Бытие определяет сознание или влияние аналогового мира на цифровой

[1,2]*В. В. Кравец*; [2,3]*С. В. Конявская*, канд. филос. наук
[1] Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации», Москва, Россия
[2] ЗАО «ОКБ САПР», Москва, Россия
[3] Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Описано решение, возникшее на базе существующего продукта под влиянием особенностей области применения: новая модификация СОДС "МАРШ!" с ОС Windows и поддержкой локальных хранилищ.

Ключевые слова: доверенный сеанс связи (ДСС), средство обеспечения доверенного сеанса связи (СОДС), защищенный служебный носитель.

Для разработчика СЗИ НСД очень важно не подпадать под обаяние своих разработок настолько, чтобы это мешало их гибкому изменению и сочетанию между собой. Приведем пример модификации и интеграции между собой разработок.

После того, как ОКБ САПР предложило рынку решение для защищенного ДБО с использованием семейства продуктов "МАРШ!", в среде специалистов (как по защите информации, так и по ДБО) начались обсуждения этого решения с точки зрения его "жизненности" в реальных условиях.

"МАРШ!" — это устройство, которое хранит эталонный образ операционной системы в специальном разделе. Доступ к такому разделу возможен только для чтения данных, и запрещена любая модификация эталонного образа.

Таким образом, пользователь каждый раз при загрузке получает эталонную (доверенную) среду. Загрузить ОС с устройства "МАРШ!" можно на любом компьютере — фактически не требуется выделение дополнительного защищенного рабочего места. Подход к созданию доверенной вычислительной среды на короткий период времени для решения конкретной задачи называется концепцией "Доверенного сеанса связи" (ДСС).

Кравец Василий Васильевич, аспирант, программист.
E-mail: vkravec@okbsapr.ru
Конявская Светлана Валерьевна, заместитель генерального директора, доцент, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

Одно из основных замечаний к устройству "МАРШ!" заключалось в том, что корпоративный рынок использует 1С, и вообще бухгалтеры работают в ОС Windows, а в "МАРШ!" — Linux, и нет возможности использовать программы и данные с жесткого диска компьютера.

В первую очередь, нельзя не согласиться, что есть случаи, когда "МАРШ!" для Клиент-банка, действительно, не требуется. Это те случаи, когда для взаимодействия с банками используются отдельные, специально только для этого отведенные и полностью защищенные компьютеры.

Однако обычно так бывает только в относительно крупных компаниях. Не каждая компания, даже из тех, что может позволить себе отдельного бухгалтера, может выделить отдельный компьютер, поставить на него все, перечисленное выше, и обучить человека со всем этим работать. Последнее особенно сложно, если человек, который будет работать за компьютером, не будет являться специалистом в области IT. С бухгалтерами такая ситуация встречается довольно часто (в конце концов, ему достаточно быть специалистом в своей области).

Очевидно, что "МАРШ!" тут был бы совершенно уместен, но, напомним, "бухгалтер работает в ОС Windows", а "1С чаще всего использует локальные базы". Строго говоря, существует клиент 1С для Linux. Но, действительно, в подавляющем большинстве случаев используется все-таки не он.

Стало быть, необходимо специальное решение на базе особой версии продукта "МАРШ!" с установленной ОС Windows и поддержкой защищенной работы с локальными данными.

Опишем использование этого решения на примере работы с "1С:Предприятие".

Для обеспечения нормального функционирования "1С:Предприятие" необходимо использовать ОС Windows, поэтому в качестве эталонной операционной системы на устройстве "МАРШ!" мы выбрали Windows Embedded Standard 7. Это модульная операционная система бинарно совместимая с Windows 7. Данное решение представляется нам крайне удачным в силу следующих причин:

- интерфейс Windows Embedded Standard 7 повторяет интерфейс Windows 7, а значит, пользователь получит привычное рабочее окружение;
- модульность позволяет собирать такой образ ОС, который занимает небольшой объем и содержит только те компоненты, которые необходимы для работы;
- бинарная совместимость с традиционными программами позволит, при необходимости, установить дополнительные инструменты для работы, не задумываясь о поиске аналогов — можно использовать ровно все те программы, что используются в десктопных версиях Windows.

Перечисленные обстоятельства позволяют полностью повторить для ОС Windows классическую версию работы в режиме ДСС — загрузить из защищенной памяти устройства эталонную рабочую среду на непродолжительное время, обеспечив тем самым доверенную среду исполнения критически важной задачи.

Однако вспомним, что для работы программы "1С:Предприятие" требуется рабочая база данных.

Доступ к этой базе данных может осуществляться по сети или локально — в зависимости от логики построения информационной инфраструктуры в конкретной организации.

Если доступ к базе осуществляется по сети, то в строгом соответствии с классической реализацией ДСС в эталонный образ включается программное обеспечение для защиты канала связи, например VPN-клиент. Но в небольших организациях, не выделяющих для Клиент-банка отдельного защищенного компьютера, такая инфраструктура встречается редко. Как же быть, если работа с базой происходит локально?

Первое решение, которое нам настоятельно предлагали реализовать — расположение базы на устройстве "МАРШ!" не выдерживает никакой критики: к эталонному образу ОС и защищаемым данным нельзя подходить с одной меркой. При такой реализации база оставалась бы доступной для чтения при подключении устройства к любому компьютеру.

Делать доступным какой-то раздел жесткого диска ПК недопустимо, потому что теряется главное достижение — изолированность среды. В этом случае защищенность ПК должна быть не ниже защищенности среды, загружаемой с "МАРШ!".

Необходимо некое защищенное хранилище, которое будет доступно только из ОС, загруженной с "МАРШ!", и не будет доступно ни при каких других обстоятельствах.

Служебный носитель

Служебный носитель — это такой носитель, который позволяет оперативно и просто переносить информацию внутри системы согласно ее внутренним правилам, но не позволяет ни выносить хранимую на нем информацию из системы, ни приносить в систему информацию, записанную на него вне системы. Никому, в том числе и легальному, пользователю. Только в этом случае носитель не будет снижать общего уровня защищенности системы даже при его физическом выносе за ее периметр. Концепция защищенного служебного носителя полностью реализована в настоящее время только в линейке продуктов "Секрет".

Очевидно, что напрашивается использование уже существующего и хорошо себя зарекомендовавшего решения: защищенного служебного носителя "Секрет". "Секрет" — это флешка, которая монтируется и запрашивает PIN-код только на тех компьютерах, которые в ней зарегистрированы как разрешенные, а на остальных — не монтируется и не опознается как устройство типа mass-storage.

Из существующих на сегодняшний день продуктов линейки "Секрет" оптимально подходит для применения в описываемой системе "Секрет Особого Назначения", поскольку для регистрации компьютера как разрешенного он использует следующий набор параметров:

- номер материнской платы;
- UID операционной системы;
- имя компьютера;
- имя домена/рабочей группы (если есть);
- номер аппаратного модуля доверенной загрузки (если есть).

Это дает возможность "привязать" "Секрет" сразу к связке ПК и "МАРШ!". То есть сотрудник сможет работать с защищаемой базой не только исключительно в доверенной среде, но и исключительно на своем рабочем месте.

Единственным разрешенным компьютером для такого "Секрета" должен быть задан компьютер с программой "1С:Предприятие", загруженный с устройства "МАРШ!". В этом случае характеристики "имя компьютера" и "UID ОС" будут взяты

из ОС "МАРШ!", а номер материнской платы — от ПК.

"Секрет" имеет множество преимуществ перед обычными носителями, перечислим самые важные:

- можно не беспокоиться о потере или краже такого устройства — если его подключить к любому компьютеру, даже к тому же самому, на котором он ранее использовался при подключенном "МАРШ! ", флешка не примонтируется, и доступа к данным не будет;
- не имея возможности использовать «Секрет» на различных компьютерах, пользователь не заразит его вирусами;
- устройство ведет внутренний журнал подключений — администратор всегда сможет узнать, когда, к какому ПК и с каким результатом подключали «Секрет», даже если подключение было бессмысленным, и открыть его не удалось.

Таким образом, защищенная работа с программой "1С:Предприятие" будет выглядеть так.

Пользователь работает на компьютере в обычном режиме, используя электронную почту, ICQ, Интернет и другие вредные для защищенности ресурсы. Затем у него возникает необходимость поработать с программой "1С:Предприятие". Он перезагружает ПК и загружается с "МАРШ!". После загрузки ОС, он подключает «Секрет Особого Назначения» и вводит PIN-код.

Теперь пользователь может работать с программой "1С:Предприятие" в привычном режиме без каких-либо изменений.

Единственное отличие — после завершения работы с программой, прежде чем перейти к переписке по электронной почте или другим делам, необходимо снова перезагрузиться, отключив "МАРШ!".

Работа по такой схеме с использованием ПО "1С:Предприятие" на "МАРШ!" с "Секретом Особого Назначения" была подробно протестирована и является полноценно работающим решением, одновременно недорогим, не требующим от пользователя специальных знаний и навыков и в то же время обеспечивающим достаточный уровень безопасности.

Принципиальное преимущество разработчика перед интегратором состоит именно в том, что он легче видит и более прямо и оперативно может влиять на свойства продуктов под влиянием изменения внешних обстоятельств. Для эффективного использования этого преимущества разработчики должны обязательно иметь возможность и желание видеть и учитывать обратную связь с потенциальными и реальными эксплуататорами их разработок.

Objective reality determines realization or analogue world impact on the digital one

[1,2] *V. V. Kravec*, [2,3] *S. V. Konyavskaya*
[1] All-Russia Scientific Research Institute of Computer Technology and Informatization Problems (VNIIPVTI), Moscow, Russia
[2] OKB SAPR JSC, Moscow, Russia
[3] National Research Nuclear University "MEPhI", Moscow, Russia

The article is devoted to the solution, that appeared determined by the particularity of the sphere of usage on base of the existing one: the new modification of TST MARCH! with OS Windows and Local Storage Support.

Keywords: trusted session (TS), trusted session tool (TST), protected official carrier.

Received June 14, 2014