УДК 004.45

Защищенные тонкие клиенты для виртуальной инфраструктуры или терминальной системы

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

Предложено направление унификации технических средств системы терминального доступа за счет использования в качестве клиентского рабочего места отчуждаемого микрокомпьютера с док-станцией. Решение позволит без снижения защищенности снизить стоимость комплекта «терминальный клиент + средства его защиты», а также повысить эффективность организационных мер защиты.

Ключевые слова: система терминального доступа, клиентское рабочее место, микрокомпьютер

На определенном этапе эксплуатации системы терминального доступа и/или виртуальной инфраструктуры владелец системы неизбежно сталкивается с тем, что экономический эффект от возможности применения «зоопарка» средств вычислительной техники (СВТ) в качестве терминальных клиентов начинает снижаться. Это связано с тем, что у разнородных СВТ, возможность использования которых изначально позволяла сохранить инвестиции, постепенно заканчивается срок полезного использования, и инвестиции в новое оборудование все равно требуются, а вот негативные особенности, такие как необходимость, обеспечивать совместимость с различной периферией, нюансы совместимости с подсистемой защиты информации и просто необходимость для управляющего персонала разбираться в «зоопарке», остаются.

В этом случае на смену этапу сбора системы из того, что есть в наличии, должен прийти этап унификации.

Очевидный способ унификации – остановить свой выбор на одной модели тонкого клиента (или близких моделях одного вендора). Однако есть другой вариант, позволяющий одновременно с унификацией рабочих мест решить еще ряд задач — это реорганизация клиентских рабочих мест таким образом, чтобы стационарным устройством осталась своего рода «док-станция», к которой на время работы подключается мобильное отчуждаемое персональное устройство, выполняющее собственно функции тонкого клиента.

В случае корректной реализации предлагаемого подхода в конкретных устройствах такая реорганизация позволит достичь:

- повышения скорости загрузки клиентских рабочих мест;
- снижения влияния на состояние системы фактора поддержки периферийного оборудования операционной системой терминального клиента;
- повышения защищенности информации в системе за счет изоляции функциональной и интерфейсной частей терминального клиента одной от другой;
- повышения защищенности информации в системе за счет схемотехнической защиты от несанкционированной (в том числе, случайной) перезаписи и/или повреждения образа начальной загрузки терминальной станции;
- повышения эффективности организационных мер обеспечения защиты информации за счет возможностей новой аппаратной архитектуры;
- ощутимого снижения стоимости комплекта «аппаратный терминал + средства обеспечения его загрузки».

Измененное рабочее место пользователя будет выглядеть следующим образом.

На столе или на стене около стола (в случае дефицита свободного рабочего пространства)

Конявская Светлана Валерьевна, зам. генерального директора, доцент, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru
Кравец Василий Васильевич, аспирант, программист.
E-mail: vkravec@okbsapr.ru
Батраков Антон Юрьевич, начальник отдела программирования.
E-mail: abatrakov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

будет установлено стационарное устройство небольшого размера (примерно $10\times10\times7$ см), подключенное к электрической сети и сети Ethernet.

Возможно исполнение с модулем Wi-Fi, но не всегда применение Wi-Fi допускается политикой безопасности предприятия.

В это устройство подключены: монитор, клавиатура, мышь, в общем, все периферийное оборудование, которое требуется на данном конкретном рабочем месте.

Устройство не имеет никаких собственных ресурсов, поэтому использовать рабочее место пока невозможно – ни локально, ни в качестве терминального клиента.

Для того чтобы начать работу, пользователь подключает к устройству свой персональный отчуждаемый микрокомпьютер (будем называть его ТУЗИК – типовое устройство защиты информационной коммуникации), который он приносит с собой в начале рабочего дня.

В нерабочее время, в зависимости от регламента предприятия, устройство может сдаваться под охрану или оставляться под ответственность пользователя.

После того как пользователь включает свой «собранный из двух частей» терминал, производится загрузка клиентской ОС и старт сессии работы с терминальным сервером или удаленным рабочим столом, и пользователь работает в обычном режиме, как с любым другим терминалом.

Принципиально важным является тот факт, что всю персонифицированную информацию должен содержать только ТУЗИК, стационарное же устройство не должно содержать никаких данных, кроме необходимых для поддержки интерфейсов взаимодействия с периферийными устройствами (мониторы, клавиатуры, мыши, принтеры (МФУ), носители ключей СКЗИ).

Это дает возможность свободно перемещать пользователя, в случае необходимости, между единообразно оборудованными рабочими местами, всю персональную информационную среду он будет приносить с собой, и такая мобильность пользователей не скажется на усложнении администрирования системы.

Загрузка клиентской ОС с использованием отчуждаемого носителя (что мы, по сути, и имеем в этом случае) может строиться двумя способами: локальная загрузка ОС, расположенной на носителе, и сетевая загрузка ОС с некоего корпоративного ресурса (при этом стартовая ОС начальной загрузки все равно загружается, конечно, с носителя).

Эти два случая реализованы, в частности, в СОДС «МАРШ!» (локальная загрузка) и ПАК «Центр-Т» (сетевая загрузка).

Оба эти способа загрузки имеют свои плюсы и в разных случаях предпочтительны для эксплуатирующей организации.

Поэтому представляется правильным создавать ТУЗИК в двух вариантах исполнения — с поддержкой технологии «МАРШ!а» и с поддержкой технологии «Центра-Т». Очевидно, что в обоих случаях та часть ОС, которая загружается непосредственно из памяти устройства, должна располагаться в защищенной от перезаписи памяти.

С точки зрения безопасности важной стороной этого решения является также то, что после отключения отчуждаемой части терминала на стационарной не остается никаких следов персональной информационной среды пользователя, а также то, что после отключения отчуждаемой части от стационарной локально загружаемая с устройства ОС не сохраняет никаких изменений, произведенных в течение сессии работы, возвращается к эталонному состоянию. Это важно, потому, что делает бессмысленными атаки типа «получение доступа к информации, основанное на восстановлении (в том числе фрагментарном) остаточной информации в компьютерной системе» и «инъекция (внедрение) исполняемого кода».

Особой статьей практически в любой организации является применение ключевых носителей. В зависимости от того, какие ограничения накладываются на этот тип устройств, в качестве защищенного ключевого носителя (с извлекаемым или неизвлекаемым ключом) может использоваться сама отчуждаемая часть терминала, так как она обладает всеми необходимыми для этого аппаратными ресурсами. Однако естественно, что в силу особенностей внутренних нормативных документов или просто сложившейся на предприятии практики может быть необходимо применять вполне определенные ключевые носители.

В этом случае ключевые носители будут одним из устройств, подключаемых к стационарной части терминала. Регламент организации при этом может предусматривать раздельное хранение в нерабочее время ключевых носителей и персональных микрокомпьютеров – например, пользователь будет сдавать их в разные подразделения, или запирать в сейфе.

Естественным требованием, вытекающим из логики комплексной защиты, является совместимость со средствами защиты, устанавливаемыми на терминальный сервер или защищающими виртуальную инфраструктуру. Причем эта совместимость не должна исчерпываться тем, что средства защиты клиентской и серверной частей системы не должны мешать работе друг друга. Это необходимое, но не достаточное условие защищенности

системы. Компоненты защиты должны взаимодействовать между собой.

Предлагаемое решение, являясь разработкой ОКБ САПР, конечно, совместимо с ПАК СЗИ НСД «Аккорд TSE», устанавливаемым на терминальные сервера и фермы, а также с ПАК СЗИ НСД «Аккорд-В», обеспечивающим защиту инфраструктуры виртуализации на базе VMware, и ПАК «ГиперАккорд», обеспечивающим защиту инфраструктуры виртуализации на базе Hyper-V.

Дополнительно при адаптации решения для каждой конкретной эксплуатирующей организации должны учитываться особенности и требования данной конкретной системы. Например, могут предъявляться такие требования:

- решение должно обеспечивать возможность применения токенов, поддерживающих технологию привязки к разрешенной рабочей среде (технология «Идеальный токен»);
- должна поддерживаться возможность применения технологии биометрической аутентификации пользователя (при этом считыватель биометрических данных пользователя должен подключаться к стационарной части терминала, а эталон биометрических данных пользователя должен храниться на его персональном идентификаторе);
- в качестве персонального идентификатора пользователя должны использоваться имеющиеся в системе аппаратные идентификаторы;
- должна предоставляться возможность опционально использовать ТУЗИК в качестве аппаратного идентификатора пользователя (рисунок).

Концептуальной основой технологии является разделение двух составляющих классического тонкого клиента (аппаратный терминал):

– ОС терминального клиента;

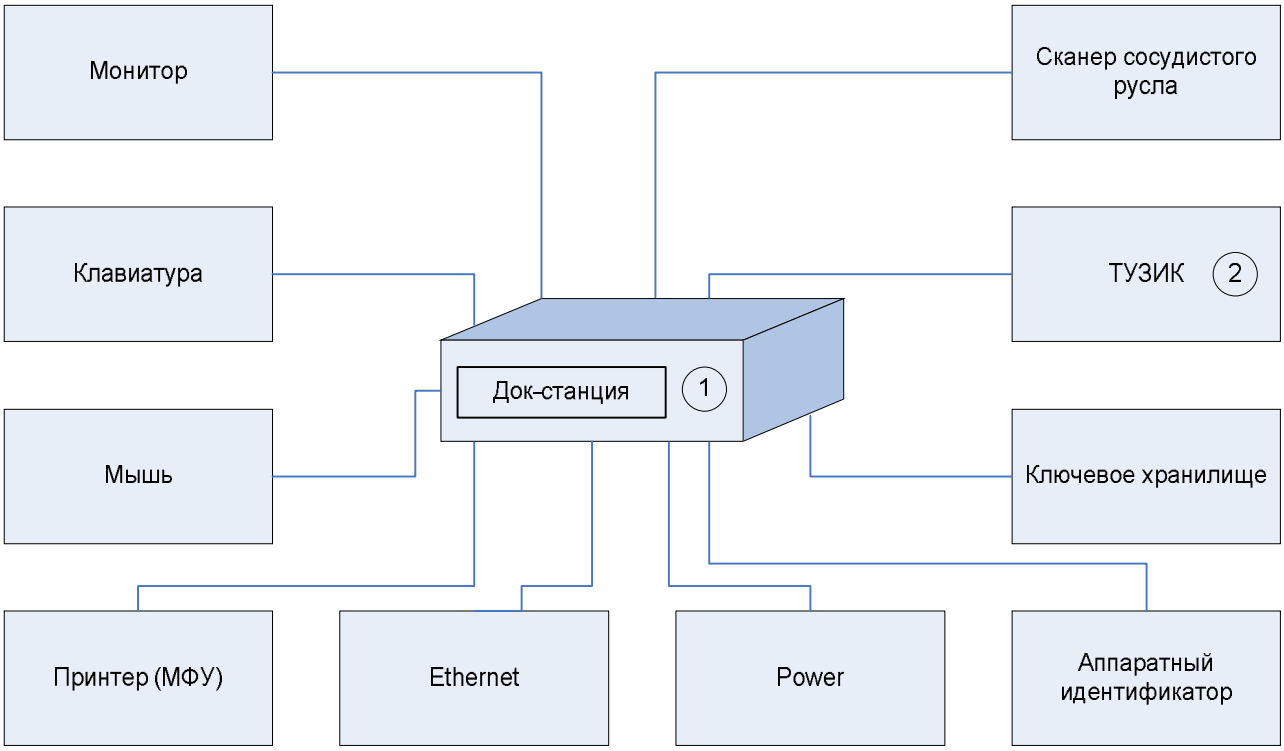
– интерфейсы подключения устройств и сетевой интерфейс на два отдельных устройства, более простые и за счет этого более экономичные, более защищенные и обеспечивающие более комфортную рабочую среду пользователя:

1) отчуждаемый персональный микрокомпьютер;

2) стационарная станция с интерфейсами подключения устройств и сетевым интерфейсом.

Экономичность

Фактически в системах, где обеспечивается защищенность клиентского рабочего места, а не только серверной части системы, аппаратные терминалы используются только как хаб — средство подключения элементов управления (клавиатура, мышь, монитор) и периферийных устройств (локальные принтеры, USB-устройства), ЛВС. Исключением являются системы, в которых внутрь тонких клиентов устанавливается полноценный аппаратный модуль доверенной загрузки



Структурная схема клиентского рабочего места с применением описанной технологии

и в защищенном режиме загружается штатная ОС терминала. Это решение защищенное, но крайне нелогичное с экономической точки зрения, так как «дешевизна» терминала полностью нивелируется дороговизной комплекса защиты. В любом другом случае контролируемость клиентской операционной среды обеспечивается за счет загрузки ОС из внешнего доверенного источника, т. е. значимым для пользователя параметром терминала является, по сути, только объем его оперативной памяти, так как от этого зависит комфортность загрузки (особенно) и (в меньшей степени) дальнейшей работы.

Все остальное определяется уже не свойствами терминала, а загружаемым образом, собранным в рамках «Центра-Т» или «МАРШ!а», или, возможно, какого-то еще решения по защищенной загрузке терминала.

При таких обстоятельствах значительные расходы на приобретение аппаратных терминалов с высокими характеристиками неоправданны, а приобретение более дешевых моделей с низкими характеристиками чревато очень низкой скоростью загрузки и некомфортной работой пользователей.

Кроме того, поддержка каждой конкретной модели аппаратного терминала должна быть обеспечена в «Центре-Т» или «МАРШ!е».

Это неизбежно влечет за собой отставание поддержки аппаратных терминалов в решениях, обеспечивающих защищенную сетевую загрузку, так как разработчикам решений сообщают о необходимости поддержки *уже приобретенных* эксплуатирующими организациями моделей. В этом, в принципе, нет ничего страшного, кроме того, что возникает постоянный фон недовольства разработчиками со стороны эксплуатирующих организаций.

Использование отдельного устройства, реализующего интерфейсы подключения устройств и сетевое подключение, и отдельного устройства, реализующего только вычислительные ресурсы без периферии, позволяет избежать всех перечисленных недостатков применения классических аппаратных терминалов.

Защищенность

Отчуждаемость персонифицированной части программной среды, которая обеспечивается за счет разделения вычислительных ресурсов и интерфейсов подключения (как устройств, так и сетевого подключения), а также их размещения в разных устройствах, позволяет усилить защищенность системы:

– технологически — за счет размещения ОС (локально загружаемого образа ОС или ОС начальной загрузки) в защищенной от перезаписи памяти;

– организационно — устройство после окончания работы может запираться пользователем в сейфе, сдаваться под охрану или сохраняться под персональную ответственность иным способом.

Комфортность работы

За счет архитектуры микрокомпьютера выполнение проверки подписи или кодов аутентификации под загружаемым образом ОС при использовании технологии защищенной сетевой загрузки может без снижения защищенности быть перенесено в ОС терминального клиента и выполняться с использованием вычислительных ресурсов микрокомпьютера. Это важно, так как именно проверка подписи является тем узким местом, из-за которого защищенная загрузка по сети производится медленнее, чем привычно пользователю, что снижает положительный эффект от ее применения.

Вынесение наиболее объемной части клиентской ОС и наиболее ресурсоемких вычислений в устройство с высокими вычислительными характеристиками и высоким уровнем защищенности одновременно позволит заметно повысить скорость загрузки аппаратных терминалов, а стало быть, и удовлетворенность пользователей условиями труда.

Поддержка различных технологий защищенной загрузки и различных вариантов порядка работы с аппаратными идентификаторами и ключевыми носителями призвана сделать переход на применение тонкого клиента на базе предлагаемой технологии необременительным для пользователей и управляющего персонала системы.

Для соответствия требованиям к решению микрокомпьютер должен подключаться к стационарной части терминала напрямую, без переходников и кабелей, причем способ подключения должен быть таким, чтобы не требовать специальных знаний и навыков от пользователя, но вместе с тем чтобы возможность неверного подключения была минимизирована или исключена. В варианте исполнения, предназначенном для работы в режиме защищенной сетевой загрузки, должна быть предусмотрена возможность подключения к ПЭВМ для записи образа ОС начальной загрузки через стандартный интерфейс.

Стационарная часть терминала должна предусматривать возможность подключения как минимум:

– монитора;
– клавиатуры;
– мыши;
– ключевого носителя (токена).

Могут подключаться также:

– принтер;
– USB-накопители;
– сканер сосудистого русла;
– считыватель аппаратных идентификаторов / аппаратный идентификатор.

При этом перечень подключаемых устройств может регулироваться на уровне ОС микрокомпьютера, а не только на уровне СЗИ НСД на серверной части системы.

Для этого устройство должно иметь:

– 2-х HDMI;
– Ethernet;
– 6–8-х USB;
– внешнее питание.

Внедрение описанной технологии применения тонкого клиента на базе отчуждаемого персонального микрокомпьютера с «док-станцией» не требует внесения значительных изменений в архитектуру системы, а значит, не увеличит нагрузку на управляющий персонал и не окажет негативного влияния на бесперебойность работы.

Время появления решения на рынке — конец 2014 г.

Protected "thin clients" for virtual or terminal access system

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

The approach to the unification of client workstations, offered in the article, is based on the using special alienable microcomputer with dock-station. This solution allows to reduce the complex "thin client + its protection tools" cost without reducing the level of system security and also to increase the efficiency of the organization steps.

Keywords: terminal access system, client workstation, microcomputer.

Received June 14, 2014