Угрозы недоверенного рабочего места пользователя и методы защиты от них

Рябко С.Д.,
президент группы компаний "С-Терра", к.ф.-м.н.

Мировая тенденция

Сегодня большое внимание уделяется тематике облачных вычислений. И что бы люди не понимали под этим термином, следует признать, что вынос информационного ресурса (услуги) в некий центр обслуживания и снижение функциональной нагрузки на клиентском рабочем месте — это объективная тенденция. Это — позитивно. Однако этой тенденции сопутствует и другая, негативная — снижение внимания к безопасности клиентского рабочего места. В том числе в области безопасности. А напрасно.

Основания для беспокойства

Во-первых, "облака" — это шаг к системам массового обслуживания. Следует предполагать, что число парк рабочих мест, выполняющих преимущественно функции представления информации (вне зависимости от конфигурации будем для краткости называть их пользовательскими терминалами) будет расти. В большой же массе пользователей всегда найдется человек неквалифицированный, нерадивый, а то и злоумышленный.

Во-вторых, "облако" — это шаг к предоставлению услуги, т.е. к ослаблению организационных связей между участниками процесса. Если в корпоративной системе терминалом владеет организация, полностью контролирующая технический регламент его безопасности, то к потребителю услуги часто просто невозможно подойти с требованиями исполнения строгого регламента. Пользователь потребляет услугу по своей потребности. И если во время потребления слуги оператор "облака", еще может, пусть малоэффективно, но контролировать его деятельность, то вне потребления сервиса пользователь принципиально неподконтролен. И какую информационную "грязь" он приобретет в неконтролируемом цикле — никому неведомо.

Из этих двух предположений вытекает следствие: в модель угроз облачного сервиса непременно должно быть заложено положение, что статистически весомая доля пользовательских терминалов поражена вирусами, закладками, руткитами.

Тяжесть этой угрозы никак нельзя переоценивать. Компрометированный терминал — прямой шаг к компрометации процесса, в котором участвует пользователь и, вполне вероятно, — промежуточный этап компрометации облака в целом.

Эти угрозы давно осознаны информационным сообществом. И оно давно пытается на них реагировать. В последние годы по перечисленным выше причинам эти усилия многократно активизировались. И в России, и за рубежом.

Что предлагает индустрия

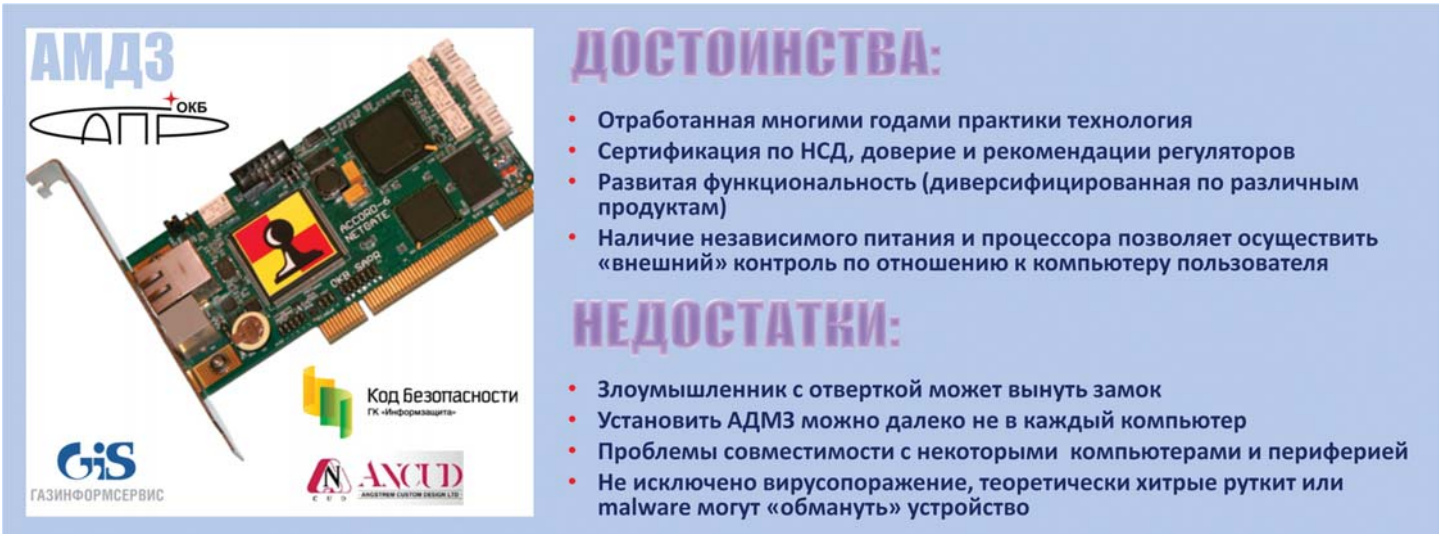
Парадоксально, но проблема доверенной загрузки — это область технологий, в которой Россия имеет опережающие заделы.

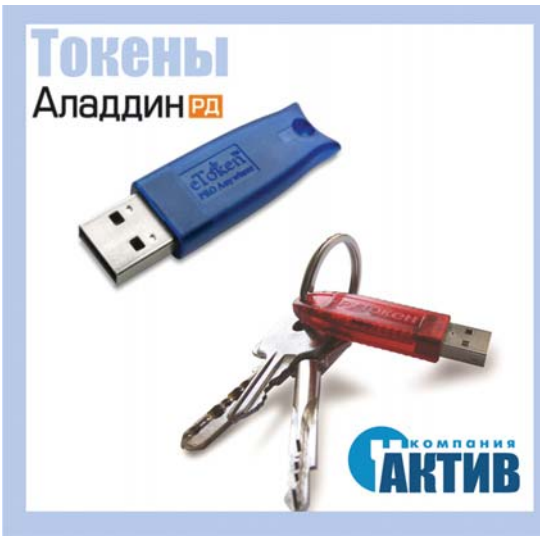
Мировое сообщество породило устройства для генерации одноразовых паролей, токен PKCS#11 и этим надолго ограничилось. Российский же климат характеризуется одновременно отсутствием собственной (доверенной) элементной и технологической базы и наличием более требовательного технического регулирования. Отсюда и возник более широкий ассортимент устройств, призванных ограничить потенциально злонамеренные возможности недоверенного компьютера.

АМДЗ

К пионерам направления относится компания ОКБ САПР, еще в 1994 г. выпустившая продукт АМДЗ (аппаратный модуль доверенной загрузки) "Аккорд". Классический АМДЗ перехватывает управление перед загрузкой операционной системы, обеспечивает аутентификацию пользователя, контролирует целостность ряда программных компонентов (набора файлов операционной системы, настроек BIOS и т.п.) и обеспечивает контроль доступа при работе компьютера.

Сегодня компания ОКБ САПР выпускает широкую линейку такой продукции, но на рынке уже не одинока - помимо нее аналогичные продукты предлагают компании "Код Безопасности" (замок "Соболь"), "Анкад" ("Анкад-Замок"), "Газинформсервис" ("Блокхост-МДЗ").





ДОСТОИНСТВА:

- Двухфакторная аутентификация, инструмент контроля доступа и Single Sign On
- Аппаратный носитель ключей, криптопровайдер малой мощности с неизвлекаемым ключом, электронная подпись с неотказуемостью
- Распространенная технология, возможность встраивания в готовые инфраструктуры аутентификации, ключевого управления, приложения

НЕДОСТАТКИ:

- Несамостоятельность (компонентность) решения: нужна внешняя криптобиблиотека и совместимое ПО
- Нестойкость по отношению к атакам на перехват управления компьютером пользователя (главный способ взлома ДБО на сегодня)

Токен

Первые изделия этого класса были представлены на российском рынке в 1999 г. компанией "Аладдин". В 2002 г. начитает работать другой крупный игрок — компания "Актив" (продукт ruToken).

Токен сам по себе не является полнофункциональным средством для обеспечения доверия к терминалу пользователя. Более того, современные закладки для систем дистанционного банковского обслуживания успешно обворовывают пользователей, использующих токен, причем без компрометации данных самого токена. Токен — это просто аппаратный криптопровайдер малой мощности, носитель ключевого материала и аутентификатор. Но исторически от технологии токенов начитаются четыре родовые ветви продуктов доверенной среды. Это — Java-токены, BIOS-замки, средства обеспечения электронной подписи в доверенной среде и среды построения доверенного сеанса.

Поскольку эти продукты относительно новы, о них следует рассказать подробнее.

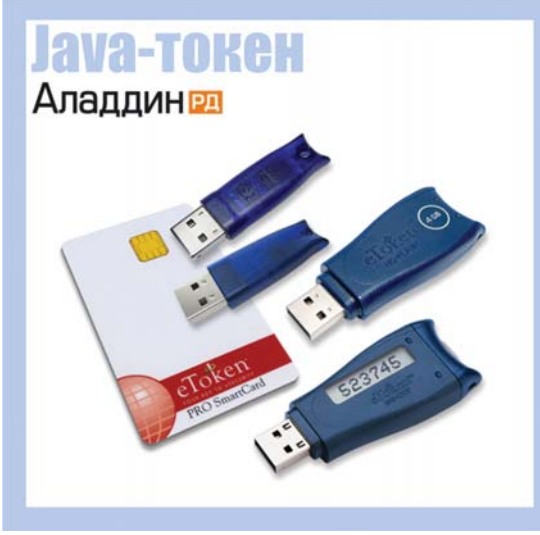
Java-токен

Java-токен, в сравнении с обычным токеном, содержит одно, казалось бы, небольшое функциональное дополнение — встроенную Java-машину. Но возможности она дает очень интересные. Во-первых, сама машина является доверенной (не подверженной искажению) исполнительной средой. Во-вторых, она способна обеспечить расширение функциональности рабочего места пользователя без инсталляции дополнительного программного обеспечения путем приема и исполнения поступающих от удаленного сервера мобильных прикладных модулей (апплетов). Эта возможность чрезвычайно ценна, поскольку позволяет очень недорого и очень оперативно решить задачи, например, модернизации функциональности системы, обновления программного обеспечения, предоставления услуг по запросу. При этом обновленная функциональность поставляется также в виде компонентов доверенной среды, поскольку для Java-апплетов, поступающих с удаленного сервера, проверяется электронная подпись.

Однако степень устойчивость такой системы к работе в условиях компрометированного рабочего места пользователя требует дополнительного исследования. Можно предполагать, что при внедрении руткитов или целенаправленно подготовленных закладок рабочее место, даже при целостности ключевого материала и полной аутентичности Java-среды, может быть очень опасно, например, способствовать уже упомянутой краже денег в системе дистанционного банковского обслуживания. Сказанное, впрочем, совершенно не означает что токен или Java-токен — негодное средство защиты. Просто при его использовании нужно применять дополнительные меры контроля целостности рабочей среды пользователя.

BIOS-замок

Большинство функций контроля, выполняемых АМДЗ, может выполняться и на уровне BIOS. Однако импортные BIOS в своем оригинальном виде не содержат полного набора функций контроля, требуемых национальными органами технического регулирования. Поэто-

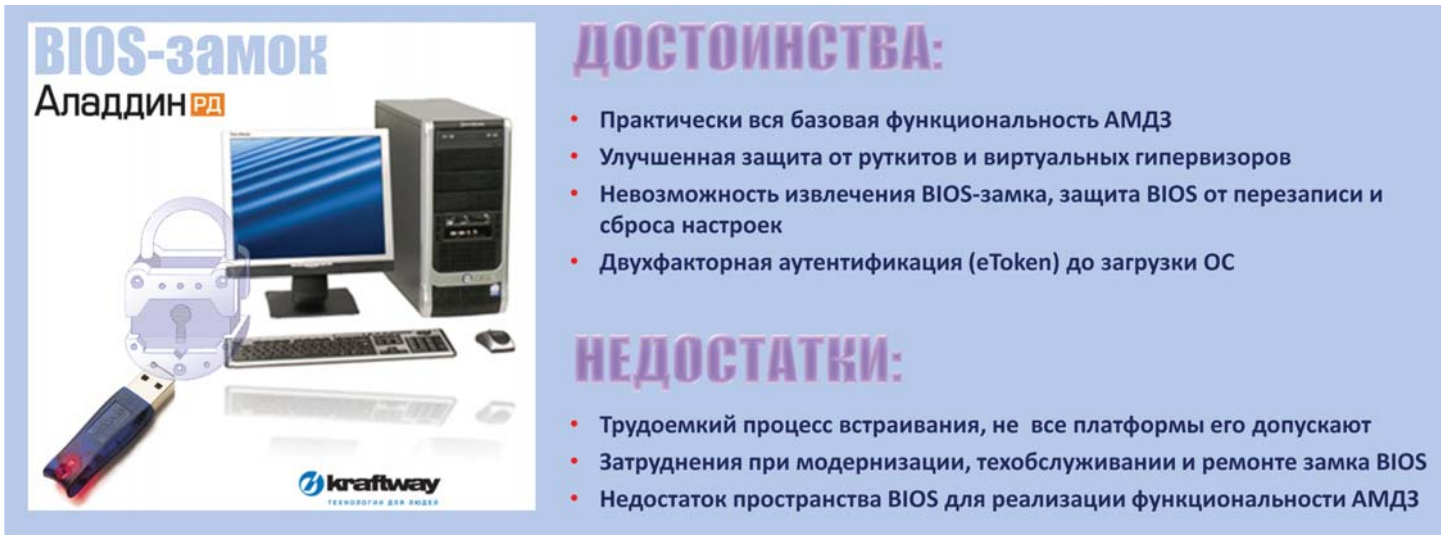


ДОСТОИНСТВА:

- Расширяемость функциональности за счет Java-апплетов
- Гибкость (свободная замена апплетов и их централизованное распространение)
- Отсутствие целевого ПО на рабочем месте оператора
- Доверие к мобильным компонентам ПО: проверка подписей апплетов

НЕДОСТАТКИ:

- Ограниченные возможности встроенной Java-машины, некоторые ограничения функциональности
- Смарт-карта зарубежного производства
- Нестойкость по отношению к «загрязнению» рабочей среды оператора (вирусы, руткиты, виртуализация BIOS)



му для реализации этих функций требуется модернизация BIOS. Дополнительно на этапе начальных проверок можно провести и аутентификацию пользователя до загрузки операционной системы. Так делает, например, компания "Аладдин", сочетая функциональность BIOS-замка с аутентификацией пользователя по PIN-коду продукта eToken. Этот продукт впервые был предложен рынку в 2010 г.

ruToken PINpad

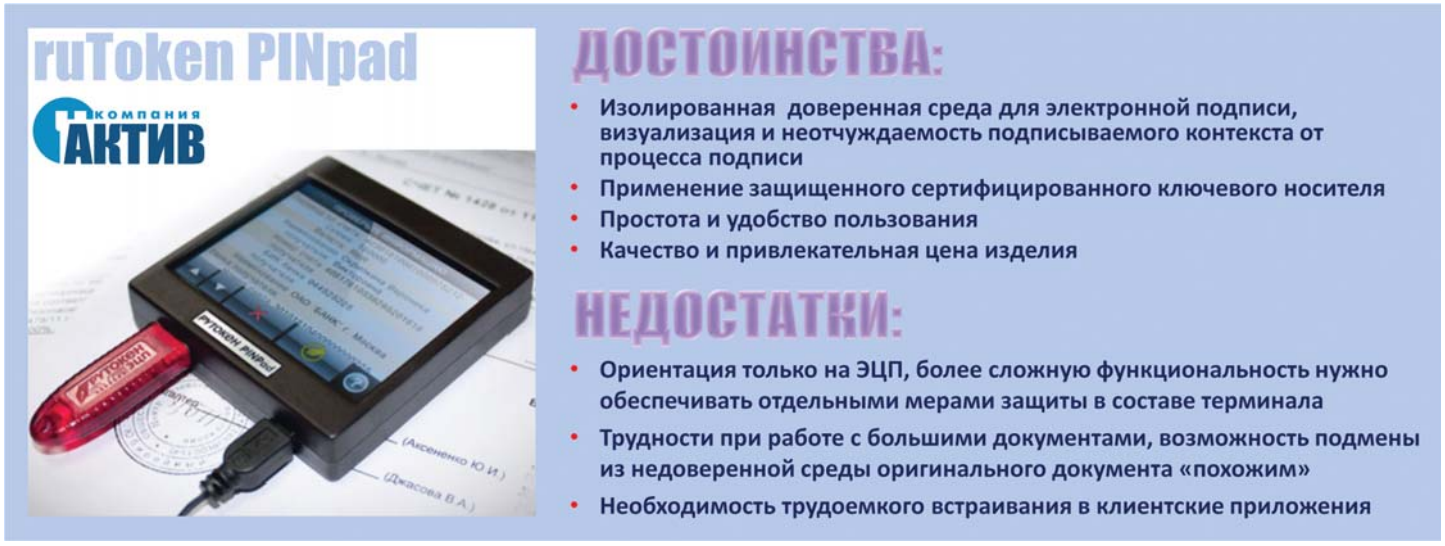
С вводом в действие ФЗ 63 об электронной подписи у российских производителей средств защиты появилось еще одно затруднившее их жизнь требование. Именно: при производстве электронной подписи пользователь должен непременно видеть документ, который он подписывает.

По поводу этого требования производители и нормотворцы предъявили законодательству ряд претензий: требование не конкретизировано, неясно как его трактовать и т.д. Между тем требование это не содержит методических проблем. Визуализация может осуществляться любым устраивающим пользователя способом, достаточным для того, чтобы он мог убедиться в подлинности подписываемого им документа. Важно только, чтобы визуализация производилась в доверенной среде, где невозможна подмена (разделение) визуализируемого и подписываемого контекстов.

Требование визуализации, а также возросший уровень краж в системах дистанционного банковского обслуживания, где злоумышленники научились "обходить" токен, искажая платежный документ на пути между визуализацией и подписью, побудили компанию "Актив" к созданию специализированного доверенного устройства, объединяющего функции визуализации и электронной подписи в доверенной среде. Это - портативный прибор, подсоединяемый к недоверенному терминалу пользователя через USB-порт и содержащий экран для визуализации подписываемого контекста. Пользователь загружает в прибор документ, визуально проверяет его содержание (сенсорный экран позволяет пролистать текст) и, если оно соответствует его заданию - производит электронную подпись. При этом в качестве носителя ключа используется ruToken.

Идея доверенного сеанса

Наряду с перечисленными устройствами в последние годы внимание специалистов привлекает идея загрузки в недоверенный терминал пользователя "чистой" рабочей среды с внешнего носителя. Такая загрузка производится для каждого рабочего сеанса доступа к доверенному ресурсу из потенциально недоверенной среды с защищенного носителя, содержащего целостный эталон рабочей среды пользователя. Первые опыты по созданию такой технологии еще в 2008 г. предприняли компании "Аладдин", "Алмитек" и "С-Терра" на базе носителя eToken NG Flash, однако эта работа не завершилась сертифицированным продуктовым результатом. Затем последовал ряд продуктов на носителе "Марш!" ("ОКБ САПР") и продукт "ПОСТ", самостоятельная разработка компании "С-Терра". Актуальность идеи доверенного сеанса подчеркивает тот факт, что два подобных продукта появились и на западном



рынке. Это — продукт "Abra" компании "Check Point" и "Trusted Access" компании "Iron Key". Поскольку все эти продукты обладают определенными функциональными различиями, поясним концепцию доверенного сеанса на основе продукта "ПОСТ".

Продукт "ПОСТ"

Загрузка среды построения доверенного сеанса (СПДС) в терминал пользователя производится со специального защищенного носителя "СПДС-USB-01", память которого разделена на несколько зон различного назначения. Критичные данные (исполняемый код) защищены от доступа пользователя и несанкционированной модернизации. Ключевой материал и атрибуты доступа хранятся на встроенном токене. Дело в том, что хранение этих сверхкритичных данных просто на флэш-носителе представляется рискованным. На рынке распространена услуга восстановления данных с флэш-носителей. Цена чтения данных из флэш-памяти составляет несколько тысяч рублей. Цена их изъятия из специальной микросхемы - в тысячу раз выше, да и выполнить эту работу сможет только специализированная организация, а не техник с феном для отпаивания микросхем.

На специальном носителе находится целостный эталон среды функционирования (СФ), включающей доверенную операционную систему, комплект средств криптографической защиты информации (СКЗИ) и целевые приложения.

После аутентификации пользователя при помощи PIN-кода с ограниченным числом попыток ввода со специального загрузочного носителя загружаются эталонный образец среды функционирования и целевое приложение.

Между рабочим местом пользователя и точкой доступа в корпоративную сеть устанавливается защищенное VPN-соединение, причем передача открытого трафика при этом запрещена, чем достигается полная изоляция сетевой среды, в которой реализуется доверенный сеанс.

Пользователь получает доступ строго к целевому приложению. Доступ к операционной системе или посторонним приложениям для него исключен, командная консоль операционной системы и посторонние приложения просто изъяты из среды функционирования.

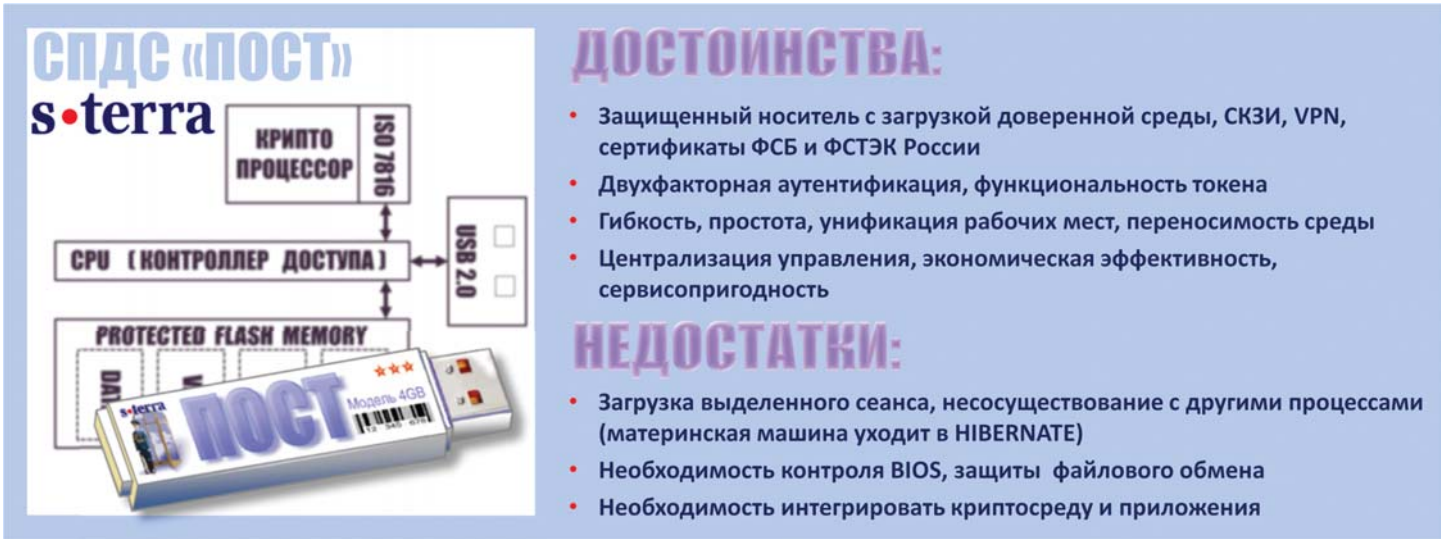
Прикладное программное обеспечение может иметь узко ограниченную функциональность. По завершении работы с приложением доверенный сеанс прекращается и питание компьютера выключается.

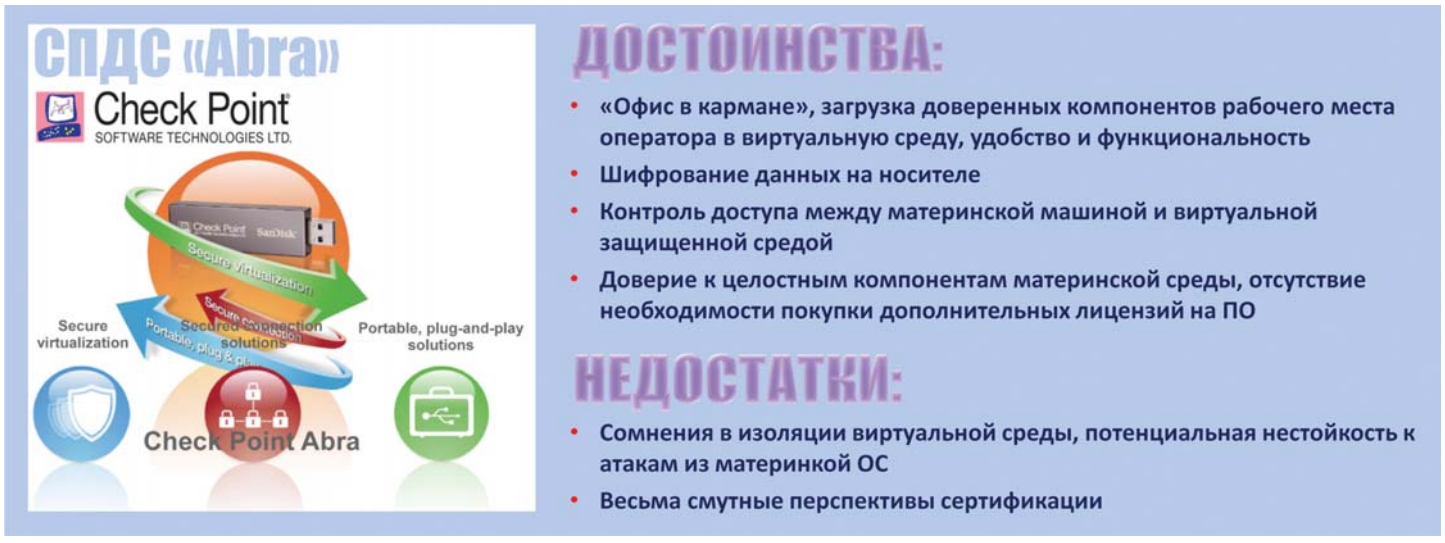
Таким образом, в области защиты информации технология СПДС имеет ряд преимуществ:

- Обеспечивается целостность программной среды терминала удаленного доступа. При всякой инициализации доверенного сеанса производится загрузка эталонного образца СФ. Эталонный образец среды функционирования хранится на носителе, исключающем ее модификацию. Никакие данные по результатам работы пользователя в течение предыдущих сеансов в СФ не вносятся. Это позволяет отказаться от применения средств защиты от вирусов, опасного ПО, закладок, что не только составляет экономию средств на антивирусном программном обеспечении, но и существенно облегчает процесс эксплуатации массового парка терминалов пользователей, поскольку в этом случае нет необходимости контролировать их конфигурацию обновлять на них антивирусные базы данных.
- Обеспечивается изоляция вычислительного процесса клиента удаленного доступа в ходе доверенного сеанса: модуль загрузки среды функционирования исключает взаимодействие с "грязной "периферией" и загрузку недоверенного программного обеспечения.
- Строгая аутентификация пользователя при доступе к доверенному сеансу работает по традиционной двухфакторной схеме: пользователь аутентифицируется перед загрузкой СФ при помощи стойкого установленного администратором безопасности пароля (число попыток ввода пароля ограничено). Затем доступ в корпоративную сеть и к серверным ресурсам осуществляется при помощи цифрового сертификата X.509, хранящегося на защищенном носителе. При необходимости эти средства аутентификации могут быть усилены средствами аутентификации в составе целевых приложений.
- Сетевая среда доверенного сеанса полностью изолирована от посторонних воздействий: трафик шифрован на основе криптоалгоритма ГОСТ 28147, обеспечивается целостность передаваемых данных и целостность потока пакетов. Поскольку в защищенную сеть может войти только владелец секретного ключа -контроль доступа в защищенный сегмент сети приобретает криптографическую стойкость, недоступную для некриптографических методов контроля сетевого доступа.

Комплект доверенного сеанса

Перенос рабочей среды пользователя на съемный носитель позволяет предложить интересное усиление идеи BIOS-замка: комплект доверенного сеанса. В комплект входят: бездисковая рабочая станция и специальный защищенный носитель. От обычного защищенного терминала комплект доверенного сеанса отличается двумя чертами. Во-первых, на бездисковой станции в отсутствие пользователя вообще отсутствует какой-либо исполняемый код. Злоумышленнику там просто нечего атаковать. Во-вторых, BIOS бездисковой станции в составе комплекта модернизируется таким образом, что для ее загрузки требуется выполнение определенного криптографического протокола





между станцией и специальным защищенным носителем СПДС. В результате терминал пользователя не грузится вообще ни с какого устройства, кроме легитимного спецносителя.

Такое решение находят весьма привлекательным заказчики, у которых реализуется посменная работа операторов на одних и тех же рабочих местах. Каждый сотрудник "носит" свою информационную среду в кармане, может воспроизвести ее в различных кабинетах и не оставляет следов после своей работы. А в отсутствие сотрудника терминал представляет собой пустое и мертвое, незагружаемое железо.

Кроме того, в силу высокой защищенности этой системы, как и в случае с ruToken PINpad, при использовании комплекта доверенного сеанса не возникают вопросы относительно доверия к визуализированному документу и корректности реализации электронной подписи в этой среде.

Доверенные среды на Западе

Продукт компании "Check Point" "Abra" анонсирован в 2010 году и позиционируется в точности как и продукты доверенного сеанса — для работы в недоверенной среде. Однако не связанные жесткими требованиями технического регулирования западные товарищи позволили себе более причудливую и, надо признать, более функциональную, архитектуру. Продукт "Abra" не производит загрузку своей операционной системы в недоверенный терминал. Вместо этого продукт загружает виртуальную машину, которая сосуществует с недоверенной средой. Способ сосуществования представляется весьма занимательным. Виртуальная машина "Abra" может использовать отдельные ресурсы недоверенной материнской системы, например, подгружать из нее отдельные приложения. Безусловно, для подгружаемых приложений реализуется ряд мер безопасности. Проверяется их целостность, обмены между виртуальной машиной и недоверенной материнской средой тщательно фильтруются. Безопасность такого решения — вопрос спорный. Можно предположить, что нашим органам технического регулирования разработчик никогда не сможет доказать отсутствие вредных влияний на доверенную среду в такой архитектуре. Однако, если предположить, что эта архитектура таки безопасна, то у нее мы найдем два несомненных удобства: доверенный сеанс не требует перезагрузки терминала пользователя, а использование приложений из материнской среды позволяет сэкономить на стоимости лицензий на ПО.

Другой производитель доверенной среды - компания "Iron Key" — анонсировала свой продукт "Trusted Access" также в 2010 г. По функциональному описанию продукт выглядит в точности также, как и СПДС, но детали реализации своего решения компания "Iron Key" тщательно скрывает. Преодолевая интеграционные сложности, компания в 2011 году пошла по пути предложения на базе технологии "Trusted Access" целостного облачного сервиса для платежных систем. И, что интересно, довольно быстро нашла несколько банков, перенесших системы дистанционного обслуживания на облачную платформу "Iron Key". Очевидно, это тот случай, когда безопасность архитектуры СПДС выступила сильным аргументом даже для консервативной отрасли ДБО, где базовые технологии давно сформировались.

Заключение

На сегодня задача обеспечения безопасности корпоративных и сервисных (облачных) систем при работе с парком недоверенных терминалов пользователей обеспечена рядом продуктовых предложений. Провести исчерпывающий анализ перечисленного многообразия попыток построить доверенную среду довольно трудно по ряду причин. Первая — в том, что каждая из технологий ветвится во множество реализационных сценариев и утверждение, верное для одного сценария, окажется неверным для другого. Вторая - в том, что доверенное решение не атомарно. Отсутствие определенной функциональности в одном из продуктов нельзя трактовать, как функциональную недостаточность отдельного продукта. Зачастую такой функциональный недостаток — просто ниша, в которую в интегрированном решении устанавливается другой продукт.

Общие плюсы и минусы решений кратко представлены в продуктовых врезках. На более глубокий анализ сегодня, ввиду новизны технологий и малой внедренческой практики замахиваться пока рано. Но что можно утверждать вполне определенно — так это то, что мы подошли к черте, когда старые продукты перестали удовлетворять потребностям быстро изменяющегося индустриального ландшафта. Появление кросс-ведомственных (некорпоративных*) систем, облачные системы, сервис которых направлен не к своему сотруднику — требуют новых подходов к защите. Тенденция, однако.

---

* *Термин принадлежит И.А.Трифаленкову, характеризующему таким образом облачные сервис-ориентированные системы компании "Ростелеком".*