Семинар Конявской С. В. на InfoSecurity-2016

Применение защищенных компьютеров MKT-card long в системах удаленного доступа смешанного типа

Честно говоря, практически каждая система через пару лет функционирования становится системой смешанного типа. Начинает совмещать в себе терминальный доступ, VDI и web, рабочие места пользователей соседствуют с участками автоматической обработки данных, к одним и тем же файловым серверам обращаются компоненты разных (в том числе по уровню защищенности) систем, а клиентские СВТ применяются одновременно в двух и более контурах, которые должны, по-хорошему, быть строго изолированными один от другого.

Истоки такой ситуации нам всем хорошо понятны, поскольку мы работаем в одних и тех же реалиях: информационные системы складываются исторически.

Сначала они проектируются. Затем начинаются локальные улучшения. Потом появляются деньги на модернизацию, покупается и внедряется что-то новое и полезное, потом вносятся улучшения, призванные совместить это новое на скорую руку с тем, что уже работало, а теперь перестало.

Например, в системе внутреннего электронного документооборота должна появиться электронная подпись. Для применения выбранного СЭП необходимо добавить в систему какую-нибудь деталь, допустим, средство защиты канала.

Оно, в свою очередь, требует работы с другим протоколом обмена данными. Тоже не беда, протоколы-то стандартные, будем работать по тому, который устраивает СЭП.

Вырастает нагрузка на канал – ну, в общем, тоже дело житейское – можно расширить каналы.

Требуется определенная версия ОС – на такую мелочь и вовсе не надо обращать внимания. Но с этой версией как раз перестает работать функциональное ПО, выполняющее целевую функцию системы.

Как правило именно в этот момент эксплуатирующая организация задумывается о том, что что-то пошло не так, а подрядчик, выполняющий модернизацию, должен разрешить клубок проблем, возникших из-за исторически сложившейся цепочки логичных решений, часто совершенно не связанных между собою.

Что нужно, чтобы так не получалось – всем хорошо известно. Но жизнь складывается тем не менее именно так, а не иначе.

Поэтому просто разберем возможное направление облегчения ситуации на примере условной системы удаленного доступа смешанного типа.

Пускай наша система совмещает в себе следующие инфраструктурные решения и технические средства:

1) физические серверы, часть из которых является ESXi-серверами, часть – терминальными серверами, часть – серверами приложений, часть – файловыми серверами, часть – серверами обработки данных, возможно еще есть какие-нибудь серверы безопасности и/или обновлений.
2) виртуальные серверы, среди которых те же терминальные серверы, серверы приложений, файловые серверы и серверы обработки данных (как правило так бывает тогда, когда систему начали «виртуализировать», но процесс растянулся по различным причинам на годы), и еще – серверы управления виртуальной инфраструктурой.
3) инфраструктура виртуализации – VMware.
4) отдельные функции управления системой реализованы в виде web-сервисов.
5) пользователи в основном работают в терминальном режиме в среде Windows (на терминальных серверах – Windows).

6) терминальное ПО – Microsoft и Citrix.
7) два контура с разными уровнями защищенности (общедоступно и информация ограниченного доступа).
8) основным способом загрузки ОС терминальных клиентов является сетевой, но отдельные клиенты загружаются локально по причине плохих каналов в территориально удаленных подразделениях.
9) система ЭДО включает в себя механизмы ЭП, реализованные каким-то определенным СКЗИ.
10) используются аппаратные идентификаторы пользователей и ключевые носители на базе USB-устройств и таблеток Touch Memory.
11) контролируется применение флешек (то есть флешки применяются, но с определенными ограничениями).

и так далее, каждый интегратор и большинство эксплуатирующих организаций способны продолжить этот список новыми и новыми деталями без ущерба для правдоподобности общей картины.

Очевидно, что причин для тревог за работоспособность и защищенность такой системы – более чем достаточно, и утверждение, что снизить накал напряженности можно за счет использования определенного клиентского устройства в качестве основного – звучит малоубедительно.

Попробуем все же рискнуть.

Проблема такой «естественной» системы в том, что она развивается из специализированной в универсальную, а это процесс довольно противоестественный.

Изначально корректно спроектированная система «заточена» на оптимальное решение конкретных, описанных в проекте задач.

Для решения ясно описанного круга задач во всех без исключения случаях лучше использовать специальные, а не универсальные средства.

Затем «жизнь вносит коррективы» **в систему, но не в проект**, и от специальных средств требуются все новые несвойственные им функции. Рассмотрим на примере средств защищенной сетевой загрузки ПО терминальных станций.

Идея применения таких средств состоит в том, что от тонкого клиента не требуется ничего, кроме поддержки периферии, и/а пользователя, контролируемой целостности и аутентичности, журналирования и управляемости. При этом защищенность становится, по сути, основной характеристикой технологии, потому что пользователь практически не имеет никаких дел ПО терминальной станции, он работает *с терминальным сервером* уже после того, как средство защищенной сетевой загрузки закончило свою работу.

Однако увеличим постепенно число поддерживаемых чипсетов до нескольких десятков, расширим парк периферии (ведь каждый год начинает выпускаться много новых мониторов все лучшего качества), усложним подсистему печати (любой сотрудник скажет, что ему удобнее иметь принтер на своем столе, а не ходить к сетевому), добавим клиент VPN, поддержку

разнообразных идентификаторов и ключевых носителей, а затем еще встроим клиента СЭП, и загружаемый по сети образ станет полноценной операционной системой. Это неплохо, но он будет, скажем, довольно объемным – особенно для загрузки по каналам связи низкой пропускной способности.

Чем более размывается контур круга задач системы, тем менее эффективными становятся специализированные технические средства и решения.

Казалось бы, выход очевиден – необходимо ставить универсальные ПЭВМ, защищать их универсальными СЗИ НСД (разумеется, семейства «Аккорд»), а также антивирусами, средствами межсетевого экранирования, шифрования трафика и всем остальным. Тем самым создадим среду функционирования криптографии (СФК) и решим все задачи. Пострадают, правда, управляемость, стоимость владения, удобство обновления и обслуживания… В общем, необходимо признать, что это решение плохое, хотя нам, как производителям «Аккордов», довольно выгодное.

Видимо, необходимо найти ту грань универсальности и специализированности, которая позволит удовлетворить разросшимся требованиям системы, не разрушая ее полностью.

Мы ее нашли.

Защищенные терминалы, о которых пойдет речь, – это МКТ-card long, отечественные инновационные микрокомпьютеры с динамически изменяемой архитектурой, запатентованной под названием «Новая Гарвардская».

Именно модель МКТ-card long потому, что ее форм-фактор (док-станция с отчуждаемым компьютером) оптимален для оседлого использования.

В кабинетах на столах сотрудников будут оставаться док-станции с подключенными мониторами, клавиатурами, мышами и всем остальным, и на включение такого рабочего места будет уходить не больше времени, чем на запуск обыкновенного компьютера.

В образ операционной системы МКТ-card long интегрирована клиентская часть ПАК «Аккорд», общая для комплексов защиты физических и виртуальных инфраструктур, так что один и тот же терминал сможет работать с физическими и виртуальными терминальными серверами без

внесения изменений в систему защиты или конфигурацию ОС. Таким образом исключаются сложности *по пунктам 1 и 2*.

Для корректной работы с виртуальными рабочими столами в образ ОС терминала встроен VMware View Client, тем самым сняты возможные конфликты *по пункту 3*.

Для защищенной работы с web-сервисами в ОС MKT-card long встраивается браузер и межсетевой экран, который не позволит пользователю отвлечься на посторонние задачи, пользуясь наличием Интернет на рабочем месте. Таким образом, *пункт 4* также не вызовет проблем.

Наличие клиентов ICA и RDP исключают сложности, потенциально связанные *с пунктами 5 и 6*.

Задачу работы в двух контурах защиты (*пункт 7*) с использованием микрокомпьютеров семейства МКТ можно решить без использования дополнительных инфраструктурных решений типа «брокеров» несколькими разными способами.

Работа в разных контурах будет изолирована в том случае, если соединение с серверной частью производится из разных ОС.

Соответственно, мы можем:

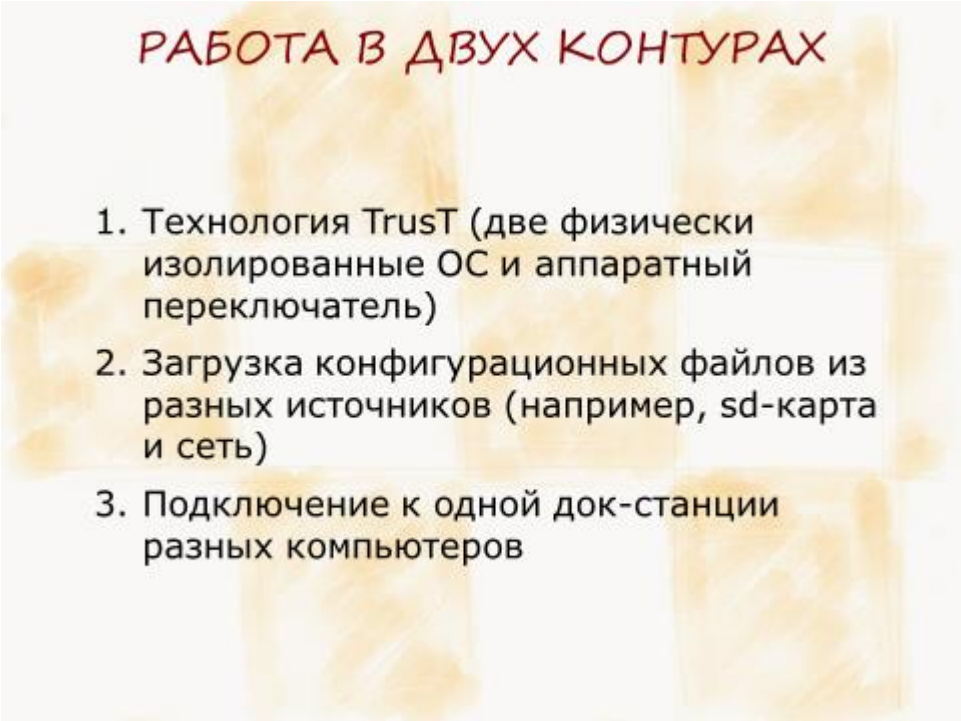
1) использовать модификацию TrusT (компьютер в этом случае будет содержать физический переключатель и называться MKTrusT-card long). У этой модификации в разных физических банках памяти находятся две разные ОС. Запуск одной или второй ОС определяется положением физического переключателя. Этот механизм абсолютно надежен, поскольку перевести переключатель в другое положение может только пользователь, загружающий компьютер, а никак не вирус или хакер. Итак, **при одном положении переключателя запускается ОС, например, с ICA клиентом, который инициирует сессию с терминальным серверов в общедоступном контуре, а при втором положении переключателя – загружается ОС с,**

допустим, VMware View Client, соединяющимся с защищенным виртуальным рабочим столом. Или как-угодно иначе. Главное, что из одной ОС можно попасть только в один контур, а из второй – только в другой.

2) в стандартной комплектации МКТ-card long, поскольку ОС в компьютерах МКТ неизменяемая, параметры доступа хранятся на внутренней SD-карте. Однако помимо получения этих параметров с SD-карты, можно получать их (и какое-либо дополнительное ПО в случае необходимости) с сервера по сети. В модификации «МКТ-card long для двойного применения» реализованы оба эти варианта одновременно, и **в процессе загрузки пользователь может выбрать, откуда получить конфигурационную информацию, и в зависимости от этого выбора попасть в один или в другой контур**.

Таким образом, помимо потенциально проблемного *пункта 7*, выполняется и условие *пункта 8*.

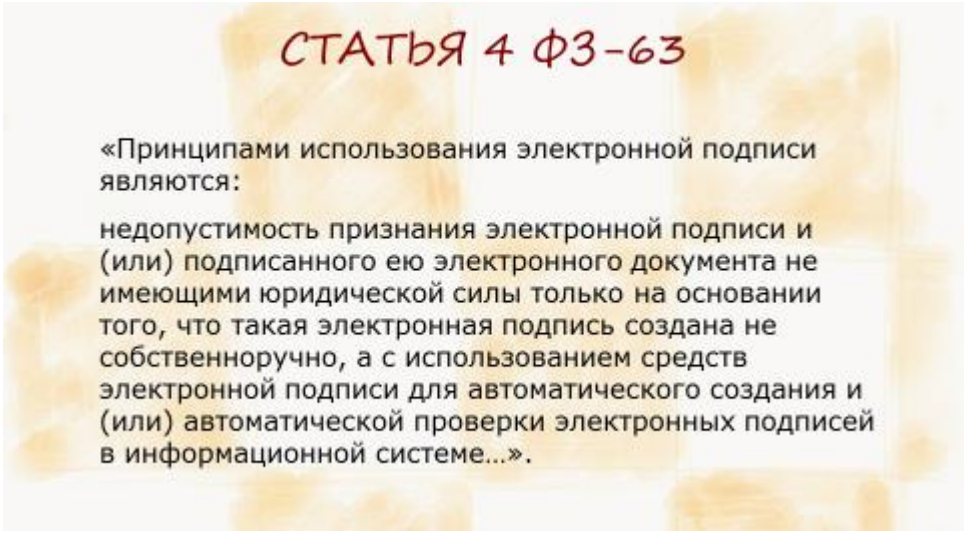
Ну и, конечно, неверно было бы списывать со счетов естественный способ, порождаемый самой архитектурой решения – док-станция и отчуждаемый ПК. Док-станции и ПК в общем случае инварианты один к другому, то есть любой ПК можно подключить к любой док-станции той же модели. А значит, доступ в разные контуры можно получать, просто подключая к своей док-станции разные компьютеры.



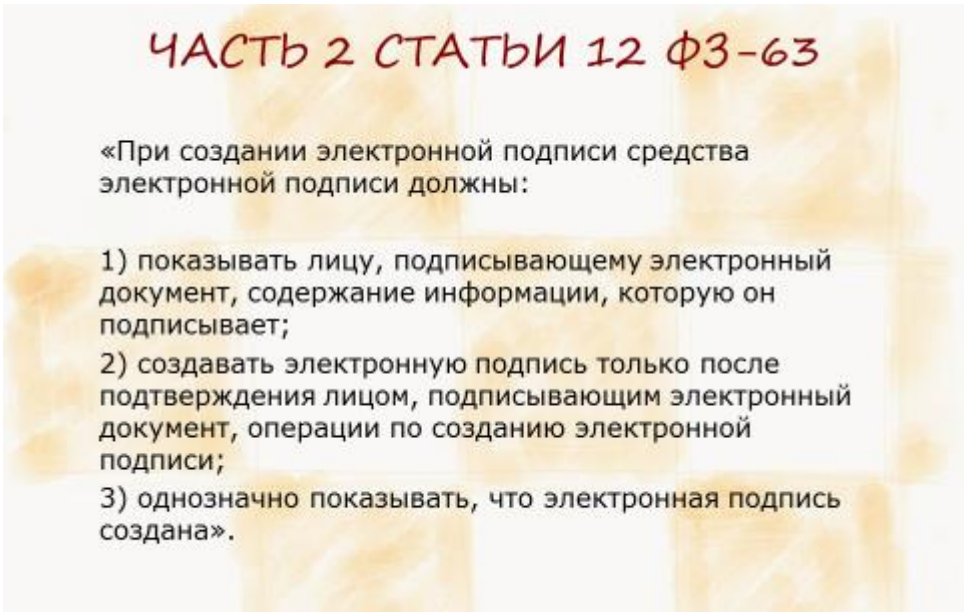
Пункт 9 – выработка и проверка ЭП – имеет огромное количество нюансов, связанных с особенностями деятельности организации, особенности документов, которые должны таким образом обрабатываться, и очень многого еще. Если нарисовать предельно обезличенную схему, то она может выглядеть примерно так: документы формируются на терминальных серверах и должны быть подписаны операторами терминалов, при этом работа должна производиться с учетом требований Федерального закона «Об электронной подписи» и Требований к средствам электронной подписи (Приложение №1 к приказу ФСБ России от 27 декабря 2011 г. № 796).

С применением защищенного терминала МКТ-card long это может быть реализовано, например, так:

1. Документ формируется на терминальном сервере.
2. Для подписания документ передается на терминальный клиент.
3. Для контроля целостности документа при передаче по каналу, перед отправкой на терминал он подписывается СКЗИ на ключе сервера в автоматическом режиме (статья 4 63-ФЗ).



4. На терминале подпись проверяется резидентным СКЗИ терминала.
5. В случае подтверждения целостности, документ визуализируется (часть 2 статьи 12 63-ФЗ).



6. Оператор должен сознательным действием подтвердить корректность отображенного документа.
7. Подтверждение оператора является сигналом для вычисления хеш-функции от документа резидентным СКЗИ терминала. Далее тем же резидентным СКЗИ, или отчуждаемым персональным СКЗИ вычисляется ЭП (п. 15 Требований).

8. После подписания документ снова визуализируется на терминале (часть 2 статьи 12 63-ФЗ).

Подтверждение оператора является сигналом для отправки подписанного документа на сервер.

Идентификаторам и ключевым носителям в нашем описании условной системы посвящен отдельный пункт, однако именно в контексте ЭП имеет смысл заметить, что в случае актуальности угрозы использования подложного СВТ в качестве терминального клиента необходимо чтобы применяемый токен имел механизмы различения разрешенных и неразрешенных для работы с ключами СВТ (пункт 31 Требований).

Такое устройство – «Идеальный токен» – поддерживается МКТ-card long.

Факторами, определяющими реализуемость данной схемы, являются с одной стороны, доверенная среда, обеспечиваемая технологически, и с другой, – вычислительные характеристики, достаточные для вычисления и проверки ЭП резидентным СКЗИ и корректной визуализации документа.

На данный момент есть опыт встраивания всех наиболее распространенных отечественных СКЗИ.

В части идентификаторов и ключевых носителей (*пункт 10*) первоочередное значение имеет сложившаяся в системе практика применения. Этой мелочи в системе настолько много, что необходимость замены шила на мыло, особенно единовременной, может стать решающим противопоказанием для приобретения новых СВТ или системы защиты.

Если использование даже очень удачного во всех отношениях оборудования потребует перерегистрации всех пользователей во всех подсистемах, требующих предъявления идентификатора, его привлекательность резко снижается. Что уж говорить о ключевых носителях – во многих организациях выпуск ключей является абсолютно сакральной процедурой.

Имея в виду эту особенность, мы предусмотрели в МКТ-card long целый ряд возможностей.

Во-первых, сам отчуждаемый компьютер из состава МКТ-card long удовлетворяет всем признакам персонального аппаратного идентификатора и ключевого носителя. Он отчуждаемый, персональный, безусловно

аппаратный и защищенный. Он может выполнять функции идентификатора пользователя в СЗИ НСД семейства «Аккорд» и защищенного ключевого носителя.

Такое хранение и аутентифицирующей, и ключевой информации является заметно более правильным с точки зрения защиты информации по следующим причинам. При идентификации с помощью компьютера, пользователь подтверждает не только то, что подключается к системе именно он, но и то, что он это делает именно со своего законного рабочего места, а не со специально подготовленного шпионского ноутбука, просто используя свой легальный идентификатор.

В плане работы с ключами при этом выполняется уже упомянутое требование обеспечения применения ключей только на легальных компьютерах.

Заметим, что пропорции отчуждаемого компьютера позволяют убирать его в стандартный пенал для ключей сдавать под охрану.

При этом перерегистрацию идентификаторов и перезапись ключей можно производить постепенно, в плановом порядке, а в переходном периоде продолжать использовать старые– за эту возможность отвечает пункт «во-вторых» (ниже).

Во-вторых, в МКТ-card long реализована поддержка наиболее распространенных типов идентификаторов (список расширяемый, поскольку образ ОС формируется для каждой конкретной системы отдельно) и ключевых носителей, работающих по стандартному протоколу CCID.

Наконец, остался последний из выделенных в начале пунктов – *11-й пункт*: флешки.

Для решения задачи защищенной работы с флешками необходимо использовать флешки на базе защищенных служебных носителей. Работа с такими флешками – «Секрет Особого Назначения» – в режиме терминальной сессии в МКТ-card long поддержана.

Подведем итоги.

Мы рассмотрели систему, представляющую собой практически эталон предбарочной российской церковной архитектуры XVII века, когда за многочисленными пристроечками и новыми полезными элементами малореально рассмотреть изначальный замысел архитектора. Несомненно, так же, как и в архитектуре, в строительстве автоматизированных систем этот период тоже будет преодолен. Но преодолеть его можно минимально травматично и постараться при этом максимально сохранить инвестиции.