УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.33

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

С. В. Конявская, канд. филол. наук
Закрытое акционерное общество "ОКБ САПР", Москва, Россия
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская область, Россия

На примере гипотетической системы смешанного типа показаны направления оптимизации стоимости и трудоемкости ее содержания за счет модернизации парка клиентских рабочих мест.

Ключевые слова: клиентское рабочее место, система удаленного доступа, многообразие инфраструктурных решений.

Неоднократно поднимался вопрос о защите систем удаленного доступа, в которых применяется "зоопарк" разнообразных клиентских устройств. Так, семинар, посвященный одному из аспектов этого вопроса — аттестации такой разнородной системы [1], оказался самым востребованным на ТБ-Форуме-2016.

Однако жизнь все чаще сталкивает нас с обратной проблемой — необходимостью обеспечить работоспособность и защищенность системы, построенной на большом разнообразии не технических средств, а инфраструктурных решений. Системы все чаще совмещают в себе терминальный доступ, VDI и web, причем 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 в идеале быть строго изолированными друг от друга.

Причины такой ситуации хорошо понятны. Обобщить их можно так: информационные системы складываются исторически.

Зачастую изначально они проектируются и какое-то время соответствуют современному уровню развития науки и техники. Затем осуществляется модернизация. Часто она проходит незаметно, например на уровне локальных улучшений системы управления. Так, если в той или иной специализированной подсистеме удобно осуществлять функции мониторинга через web-интерфейс, то почему бы не ввести в нее такой модуль?

Потом наступает время более глобальной модернизации: технологии унеслись далеко вперед. Но имеющихся на модернизацию денег бывает недостаточно на коренное перепроектирование, а достаточно (опять же в хорошем случае) только на приобретение новых инфраструктурных элементов и технических средств, например на внедрение виртуальной инфраструктуры в целях централизации вычислений за счет виртуализации терминальных серверов и серверов обработки данных. Приобретенное (скорее всего, ПО и серверы, но возможно, и средства защиты) встраивается в систему настолько успешно, насколько хватает квалификации и энтузиазма у управляющего персонала системы и подрядчика. Системы продолжают работать и даже иногда начинают работать более эффективно.

Предположим, однажды появляется необходимость включить в состав технологического процесса новую операцию, например работу с электронной подписью (ЭП) в системе внутреннего электронного документооборота. Выбранное по тем или иным причинам средство электронной подписи (СЭП) принципиально удовлетворяет проектным характеристикам системы (поддерживает работу в терминальном режиме, имеет сертификат, поддерживает нужную систему управления ключами), для его применения необходимо только добавить в систему какой-то инфраструктурный элемент, например средство защиты канала. Это несложно, но, в свою очередь, требует работы с другим протоколом обмена данными (это тоже несложно, так как протоколы стандартные). Вырастает нагрузка на канал, но в этом случае можно расширить каналы. Хуже, если начинает требо-

Конявская Светлана Валерьевна, зам. генерального директора, доцент, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

ваться изменение версии ОС. Совсем незначительное: не замена на ОС другого семейства, а всего лишь другая версия. И вот с этой версией как раз и перестает работать функциональное ПО, выполняющее целевую функцию системы. Не говоря уже о том, что система электронного документооборота (СЭДО) оказывается готова к встраиванию СКЗИ, но не готова к выполнению требований к СЭП, и начинается выяснение границ ответственности (на чьей стороне, например, визуализация, СЭП или СЭДО; за счет свойств ключевого носителя или системы управления ключами лучше снижать нагрузку на персонал; имеется еще очень много аналогичных вопросов).

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 собой.

Абсолютно очевидно, что не имеет смысла рассказывать, как сделать, чтобы так не получалось. Это всем хорошо известно: нужно все время проектировать. Но жизнь тем не менее складывается именно так, а не иначе.

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

Пусть 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, есть еще 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, когда систему начали "виртуализировать", но процесс по различным причинам растянулся на годы), а также серверы управления виртуальной инфраструктурой;

3) инфраструктура виртуализации — VMware;

4) отдельные функции управления системой реализованы в виде web-сервисов;

5) целевое функциональное ПО пользовательского сегмента информационной системы работает 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) в системе используются аппаратные идентификаторы пользователей и ключевые носители на базе USB-устройств и таблеток Touch Memory;

11) в системе контролируется применение флеш-носителей (есть определенные правила и ограничения, однако в целом они применяются);

12) и т. д.; каждый интегратор и большинство эксплуатирующих организаций способны пополнить 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 о том, что снизить накал напряженности можно за счет использования определенного клиентского устройства в качестве основного, звучит малоубедительно.

Попробуем все же рискнуть.

Если обобщать до схематичности, то проблема такой "естественной" системы состоит в том, что она развивается из специализированной в универсальную, а это процесс довольно противоестественный.

Изначально корректно спроектированная система "заточена" на оптимальное (т. е. с максимальной эффективностью при минимальных затратах и сложностях управления) решение конкретных, ясно описанных в проекте задач.

Для решения ясно описанного круга задач во всех без исключения случаях лучше использовать специальные, а не универсальные средства. Этот тезис подробно раскрыт в [2—5].

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 (т. е. возможности контролируемой модификации в соответствии с изменениями ситуации со стороны удаленного аутентифицированного администратора). При этом защищенность становится, по сути, основной характеристикой технологии, так как с точки зрения состава и тем более "удобства" такого загружаемого образа требования минимальны: пользователь практически

не имеет с ним никаких дел, он работает с терминальным сервером уже после того, как средство защищенной сетевой загрузки закончило свою работу.

Однако, если постепенно увеличить число поддерживаемых чипсетов до нескольких десятков, расширить парк периферии (ведь каждый год начинает выпускаться много новых мониторов все лучшего качества), сделать смешанной подсистему печати (ввести и сетевые, и локальные принтеры; любой сотрудник скажет, что ему удобнее иметь принтер на своем столе, а не ходить к сетевому), добавить клиент VPN, поддержку разнообразных идентификаторов и ключевых носителей, а затем еще встроить клиент СЭП, чтобы выработка ЭП производилась корректно на стороне клиента, то 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.

То же касается всех технологий, нацеленных на специализацию системы, но развиваемых в сторону ее универсализации.

Протокол передачи данных, оптимизирующий передаваемые данные для минимизации нагрузки на канал, теряет все свои преимущества при попытке шифрования трафика. Также в этом случае теряют эффективность и специальные "компрессоры". Шифртекст не сжимается.

Примеров можно привести множество.

Очевидно главное: чем более размывается круг задач системы, тем менее эффективными становятся специализированные технические средства и решения.

Казалось бы, выход очевиден: необходимо ставить универсальные ПЭВМ, защищать их универсальными ПАК 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. Кроме, разве что, управляемости системы, стоимости владения, удобства обновления, потери всех выгод от виртуализации и от терминального доступа и … многого другого. В общем, необходимо признать, что это плохое решение, хотя производителям "Аккордов" довольно выгодное.

Видимо, необходимо найти ту грань универсальности и специализированности, которая позволит удовлетворить разросшимся требованиям системы, не вставая на экстенсивный путь бессмысленного наращивания ресурсов (использование техники все большей мощности со все более избыточной функциональностью, требующей обслуживания все большим штатом высококвалифицированного персонала).

Именно подсистема защиты информации, вопреки ожиданиям, может стать элементом, который позволит скрепить элементы разросшейся системы и снова сделать ее единым целым. И получится это в том случае, если клиентские СВТ станут частью данной подсистемы, тем самым делая ее фузионной [6], а не агглютинативной*.

Защищенные терминалы, о которых пойдет речь, — это МКТ-card long, отечественные инновационные микрокомпьютеры с динамически изменяемой архитектурой, запатентованной под названием "Новая гарвардская" [7].

Указанная архитектура описана в [8—13], а линейка микрокомпьютеров на ее основе — в [14].

Для разрешения описанной ситуации мы предлагаем выбрать именно модель МКТ-card long потому, что ее форм-фактор (док-станция с отчуждаемым компьютером) оптимален для использования на стационарно расположенных рабочих местах (рис. 1).

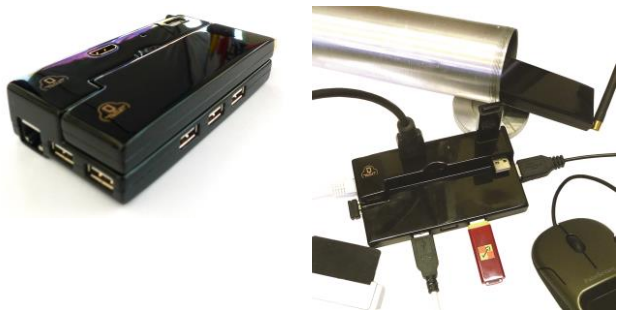

Рис. 1. Модель МКТ-card long

* Агглютинация и фузия — два способа построения слов в разных языках. Агглютинация — это механическое присоединение нового члена (форманта) с одним-единственным значением (например, только множественность или только мужской род, или только притяжательность) при каждом наращении смысла. Пример агглютинации в татарском: "в его письмах" — "хатларында" ("хат" — "письмо", "лар" — формант множественного числа, "ын" — притяжательный формант 3-го лица, "да" — формант местного падежа). Фузия же — это способ построения слов и форм, при котором один суффикс, например, может выражать сразу целую совокупность значений, а соединение частей в слово происходит так, что не всегда легко провести точную границу. Например, слово "плачет": корень "плак" в месте присоединения суффикса (означающего *одновременно* и ед. ч., и 3-е лицо, и настоящее время) изменился (претерпел чередование к\ч из-за влияния гласного переднего ряда на заднеязычный согласный). Как правило, в языках наблюдаются оба способа, но какой-нибудь один преобладает. Искусственные языки всегда агглютинативные. К естественным чисто агглютинативным языкам относятся: тюркские, некоторые финно-угорские, монгольские, тунгусо-маньчжурские, корейский, японский, грузинский, баскский, абхазо-адыгские, дравидийские, часть индейских и некоторые африканские.

В отличие от микрокомпьютеров в форм-факторе донглов, к которым необходимо каждый раз подключать всю периферию, в кабинетах на столах сотрудников будут оставаться док-станции с подключенными мониторами, клавиатурами, мышами, считывателями ключевой информации и т. д. 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 (ПАК СЗИ НСД Аккорд-Win32 TSE / Аккорд-Win64 TSE и ПАК СЗИ НСД Аккорд-В), 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 пп. 1 и 2*.

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

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

Наличие клиентов ICA и RDP исключает сложности, потенциально связанные *с пп. 5 и 6*.

Задачу работы в двух контурах защиты (*п. 7*) с использованием микрокомпьютеров семейства МКТ можно решить несколькими разными способами. Опишем те из них, которые не требуют использования никаких дополнительных инфраструктурных решений типа "брокеров" или аналогичных им.

Основа у этих способов общая: работа в разных контурах будет изолирована в том случае, если соединение с серверной частью производится из разных ОС. Соответственно можем:

1) использовать модификацию TrusT (компьютер в этом случае будет содержать физический переключатель и называться МКTrusT-card long). У этой модификации в разных физических банках памяти находятся две разные ОС. Запуск одной из 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, например, ОС с ICA-клиентом, который инициирует сессию с терминальным сервером в общедоступном контуре, а при другом — 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 другой — только в другой;

2) при использовании стандартной комплектации МКТ-card long обеспечить две различные среды для доступа в разные контуры можно следующим образом. В общем случае, поскольку ОС в компьютерах МКТ неизменяема (она находится в банке памяти, физически переведенном в режим Read Only), 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.

В решении совмещены функции комплекса защищенной сетевой загрузки ПО терминальных станций "Центр-Т" и стандартные функции МКТ-card long. Такое совмещение удобно еще и тем, что микрокомпьютеры в этом случае можно использовать внутри уже имеющейся в организации инфраструктуры "Центр-Т", т. е. используя серверы хранения и сетевой загрузки этого комплекса без разворачивания новых.

Наиболее логичной видится организация доступа в контур ограниченного доступа с помощью загружаемых по сети конфигураций и в общедоступный контур с конфигурациями на SD-карточке (это позволит более гибко и оперативно управлять настройками доступа именно в более тщательно защищаемый контур). Хотя можно поступить и наоборот — зависит это, скорее, от желательного порядка администрирования конфигураций, а не от соображений безопасности.

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

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 друг другу, т. е. 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 — включение в технологию обработки электронных документов выработки и проверки

ЭП — имеет огромное количество нюансов, связанных с особенностями деятельности организации, особенностями документов, которые должны таким образом обрабатываться, и очень многим еще. Если нарисовать предельно обезличенную схему, то она с учетом обрисованных условий может выглядеть, например, приблизительно так: документы формируются на терминальных серверах и должны быть подписаны операторами терминалов; при этом работа должна производиться с учетом требований Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ "Об электронной подписи" (далее 63-ФЗ) [15] и Требований к средствам электронной подписи (Приложение № 1 к приказу ФСБ России от 27 декабря 2011 г. № 796; далее Требования) [16].

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

1. Документ формируется на терминальном сервере.

2. Когда его должен подписать оператор терминала, документ передается с терминального сервера на терминальный клиент.

3. В целях 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 (ч. 2 ст. 12 63-ФЗ[**]).

6. Оператор должен сознательным действием подтвердить корректность отображенного документа (ч. 2 ст. 12 63-ФЗ).

7. Подтверждение оператора является сигналом для вычисления хеш-функции от документа резидентным СКЗИ терминала. Далее тем же резидентным СКЗИ или отчуждаемым персональным СКЗИ (токеном) вычисляется ЭП (п. 15 Требований[*]).

8. После подписания документ снова визуализируется на терминале (ч. 2 ст. 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 (п. 31 Требований[**]). Такое устройство — "Идеальный токен" [17—20] — поддерживается МКТ-card long.

Очевидно, что факторами, определяющими реализуемость данной схемы (как и любой другой разумной схемы встраивания в технологию ЭДО механизмов ЭП) на микрокомпьютерах семейства МКТ, являются, с одной стороны, доверенная среда, обеспечиваемая технологически, и с другой, — их вычислительные характеристики, достаточные для вычисления и проверки ЭП резидентным СКЗИ и корректной визуализации документа[***].

Опыт встраивания всех наиболее распространенных отечественных СКЗИ имеется.

В части идентификаторов и ключевых носителей (*п. 10*) первоочередное значение имеет сложившаяся в системе практика применения, поскольку это как раз та мелочь, которой в системе настолько много и замена которой настолько трудоемка, что необходимость такой замены, особенно единовременной, может стать решающим противопоказанием для приобретения новых СВТ или системы защиты. Если использование даже очень

---

[*] Статья 4 ФЗ-63: "Принципами использования электронной подписи являются: недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе".

[**] Часть 2 статьи 12 ФЗ-63: "При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана".

[*] Пункт 15 Требований: "Средства ЭП класса КС3 противостоят атакам, при создании способов, подготовке и проведении которых используются возможности...: ...доступ к СВТ, на которых реализованы средство ЭП и СФ".

[**] Пункт 31 Требований: "В состав средств ЭП классов КС3 должны входить компоненты, обеспечивающие: ...управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭП и СФ на основе параметров, заданных администратором или производителем средства ЭП...".

[***] *Параметры компьютера*: процессор 4-ядерный, 1,6 ГГц, Cortex A9; графический процессор Mali400, 2D/3D OpenGL ES2.0/OpenVG1.1; ОЗУ 2GB DRR3; WiFi IEEE 802.11 b/g/n; Bluetooth V4.2; считыватель карт MICRO SD (TF card) до 32 ГБ; размер защищенного диска 8 ГБ. *Параметры докстанции*: порт HDMI: 2, порт USB: 8 (host) + 1 (slave), порт Ethernet, порт питания 1 DC 4.0 мм, питание DC 5 В, 2 А.

удачного во всех отношениях пользовательского терминала потребует перерегистрации всех пользователей во всех подсистемах, требующих предъявления идентификатора, или даже просто дополнительной регистрации еще N идентификаторов (особенно если N — трехзначное и выше число), то любой владелец системы взвесит трудозатраты на эту процедуру. Это в еще большей степени касается ключевых носителей, так как 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 ноутбука, например просто используя свой легальный идентификатор. Это позволит блокировать значительное число уязвимостей, связанных с так называемым BYOD, что на самом деле зачастую является неконтролируемым размыванием защищенного контура.

В плане работы с ключами все еще более очевидно, ведь даже храня ключи на так называемом токене, можно скомпрометировать их, подключив токен не к защищенному рабочему месту, а к какому-либо незащищенному компьютеру, на котором уже есть какой-нибудь ворующий ключи троян. Так же как и в предыдущем случае, пользователь может действовать из лучших побуждений, например желая поработать сверхурочно на домашнем компьютере, но при этом он сведет на нет усилия по защите информации в целой системе.

Заметим, что для укрепления метафорического смысла термина "ключ" пропорции отчуждаемого компьютера таковы, что он помещается в стандартный пенал для ключей (рис. 2) и может сдаваться под охрану в конце рабочего дня.

Рис. 2. Фотография отчуждаемого компьютера

В случае, если такое применение для эксплуатирующей организации привлекательно, перерегистрацию идентификаторов и перезапись ключей можно производить постепенно, в плановом порядке, а в переходном периоде продолжать использовать уже введенные в эксплуатацию устройства.

Для этого 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.

Особенностью политики работы с идентификаторами и ключевыми носителями в отдельных организациях бывает запрет на использование одного и того же устройства одновременно в обоих качествах. Даже если и в качестве носителя ключа, и в качестве идентификаторов используются, допустим, ТМ-идентификаторы, USB-ключи или смарт-карты, использовать *одно и то же* устройство для того, чтобы хранить данные для и/а и ключи с сертификатами, нельзя. В таких случаях, как бы ни было удобно идентифицироваться с помощью своего же рабочего места и на нем же носить свои ключи, придется как минимум использовать отдельный ключевой носитель.

Учитывая описанные выше опасности, связанные с применениями ключевых носителей на несанкционированных компьютерах, рекомендуется использовать "Идеальный токен", который подключается только к заранее разрешенным администратором рабочим местам.

Остался последний из выделенных в начале пунктов – *11-й пункт*: флешки.

До сих пор все средства защиты информации, нацеленные на контроль использования подключаемых устройств, представляли собой некоторое ПО, устанавливаемое на сервер (или в ОС автономного ПК). Это были или модули в составе монитора разграничения доступа (такой модуль есть

и в СПО "Аккорд"), или специальное ПО, предназначенное для контроля подключаемых устройств, типа Device Lock. Такие средства вполне могут функционировать и в серверной части описанной системы. Однако все, кто пытался решить задачу контролируемого использования флешек в организации, знают, что этого недостаточно и что необходимо не только применять флешки внутри защищенного контура по определенным правилам, но и исключить их применение за пределами контура, иначе все предпринятые усилия никак не помешают ни вынести информацию наружу, ни привнести вредоносное ПО извне.

Для комплексного решения этой задачи необходимо использовать флешки на базе защищенных служебных носителей. Работа с такими флешками (линейки "Секрет" [21], а именно "Секрет особого назначения") в режиме терминальной сессии поддержана в МКТ-card long, а локальная работа с ними в собственной ОС терминала — дело ближайшего будущего: выход версии "Секрета особого назначения" для Linux запланирован на второе полугодие 2016 г.

Есть еще одна особенность данной системы, которая не была вынесена в отдельный пункт, поскольку не является архитектурной, но явно заметна по сюжету. Это подверженность системы частым модернизациям по различным причинам.

Эта особенность важна потому, что, казалось бы, находится в некотором противоречии с идеей зафиксированности и неизменности вычислительной среды, лежащей в основе линейки компьютеров МКТ. Противоречие это разрешено — для микрокомпьютеров реализована возможность обновления защищенной ОС. Если систему планируется модернизировать часто и радикально, лучше заказывать МКТ-card long с поддержкой системы защищенных обновлений. В противном случае вносить изменения в его защищенную от перезаписи операционную систему будет возможно только в сервисном центре.

Заключение

Рассмотрена система, представляющая собой практически эталон предбарочной российской церковной архитектуры XVII в., когда за многочисленными пристроечками и новыми полезными элементами малореально рассмотреть изначальный замысел архитектора. В строительстве автоматизированных систем так же, как и в архитектуре, этот период тоже будет преодолен. Но хотелось бы преодолеть его минимально травматично и постараться при этом максимально сохранить инвестиции.

Защищенный терминал МКТ-card long представляется именно тем решением, которое будет одинаково эффективно и в "переходные периоды" модернизаций системы, и в периоды ее стабильных состояний.

Литература

1. *Конявская С. В., Рябов А. С., Лыдин С. С.* О том, почему не надо бояться "зоопарка" технических средств, или как самому себе аттестовать ИСПДн // Защита информации. Inside. СПб. 2015. № 5. С. 24—27.
2. *Конявский В. А.* Не надо оплачивать уязвимости // Аналитический банковский журнал. — М., 2014. № 10 (222). С. 62—64.
3. *Конявский В. А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. С. 31—34.
4. *Конявская С. В.* Информатизация без нагрузки // Национальный банковский журнал. — М., 2016. № 2. С. 58, 59.
5. *Конявский В. А.* Эпохе бурного развития — компьютер с динамической архитектурой // Национальный банковский журнал. — М., 2016. № 3. С. 102, 103.
6. *Реформатский А. А.* Лингвистика и поэтика. — М., 1987. С. 52—76.
7. Компьютер типа "тонкий клиент" с аппаратной защитой данных. Патент на полезную модель № 118773. 27.07.12. Бюл. № 21.
8. Компьютер с аппаратной защитой данных от несанкционированного изменения. Патент на полезную модель № 137626. 20.02.2014. Бюл. № 5.
9. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.
10. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 139532. 20.04.2014. Бюл. № 11.
11. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.
12. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 151264. 27.03.2015. Бюл. № 9.
13. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой. Патент на полезную модель № 153044. 27.06.2015. Бюл. № 18.
14. Trusted Cloud Computers [Электронный ресурс]. URL: www.trustedcloudcomputers.ru.
15. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ "Об электронной подписи".
16. Приказ ФСБ России от 27.12.2011 № 796. Приложение 1.
17. *Кравец В. В.* Идеальный токен // Комплексная защита информации. Матер. XX науч.-практ. конф. — Минск, 19—21 мая 2015 г. — Минск: РИВШ, 2015. С. 114, 115.
18. *Ладынская Ю. П., Батраков А. Ю.* Хранение данных СКЗИ: выбор носителя // Информационная безопасность.

Матер. XIII Междунар. конф. — Таганрог, 2013. Ч. 1. С. 129—134.

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

20. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014. Бюл. № 31.

21. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010. Бюл. № 15.

MKT-card long — the safe microcomputer — in mixed type remote access systems usage

S. V. Konyavskaya
Closed Joint Stock Company "OKB SAPR", Moscow, Russia
Moscow institute of physics and technology (state university),
Dolgoprudny, Moscow region, Russia

The article draws the directions of optimization the diffused system owning by modernization of the client work-stations park.

Keywords: client workstation, remote access system, the variability of infrastructure decisions.

Bibliography — 21 references. *Received June 26, 2016*