*Конявская С. В.*

**«Специальное» vs «универсальное» как базовая дихотомия всеобщей теории всего**

Противопоставление специального и универсального (чего угодно – питания, одежды, автомобилей, вычислительной техники, средств связи, косметики – ряд может быть бесконечным и разноуровневым на столько, на сколько позволит внутренняя свобода автора) – видимо, в природе человека ровно в той же мере, в какой и стремление к их смешению и перестановке.

Джинсы стали универсальной одеждой из специальной, а сарафаны и кокошники – наоборот, хаммер стал обыкновенной машиной, а пежо – полицейской, радиотелефоны и скремблеры стали бытовыми приборами, а пейджеры – средствами оперативной связи врачей. Чтобы не затягивать вступление, не стану множить примеры, они все примерно одинаковы.

Развитие средств вычислительной техники не исключение из общего правила, эта тенденция на ней тем заметнее, чем вообще заметнее ее развитие, по сравнению с остальными областями жизни. В отношении операционных систем об этом, в частности, писал В. А. Конявский [1. С. 211–212, 2. С. 808], где отмечал, что универсальные ОС постепенно становятся в определенном смысле тоже специализированными – для «дома и офиса», для информационных задач, а для решения задач, требующих работы в реальном масштабе времени становятся все менее пригодны, требуя бесконечного наращивания ресурсов аппаратуры. Об аппаратной стороне дела он писал там же в менее явной форме [Там же. С. 809–811], и в последующие годы во вполне явной – например, в [3, 4] и др.

Казалось бы, в сфере защиты информации эта дихотомия проявиться не может в принципе, потому что средство защиты информации – это уже само по себе довольно высокий уровень специализированности. Однако, нет.

В первую очередь эта дихотомия проявляет себя, действительно, в сущностном, категориальном признаке технической защиты информации вообще – техническая защита информации – это ограничение универсальности СВТ. Защищенный компьютер – уже не универсальный компьютер, на нем можно не все, не всем и не всегда.

Предельный случай, ярко выпячивающий эту черту – функционально замкнутая среда (ФЗС), когда «целый компьютер» (в принципе – универсальный, фон-Неймановский, машина Тьюринга, можно сказать) используется в один момент времени только для одной задачи, и тем избегается нежелательное взаимовлияние программ [2. С. 739].

Если вынести эту задачу в отдельное специализированное устройство, то компьютер можно не лишать универсальности, а делать специализированным только на время – на время доверенного сеанса связи (ДСС), подключая к нему это самое специальное средство обеспечения доверенного сеанса связи (СОДС) МАРШ!.

Другой пример – HSM (hardware security module). Как правило, это отдельный компьютер, «начиненный» различным программным обеспечением, выполняющим функции, связанные с безопасностью. Обычно это межсетевой экран, криптомаршрутизатор, сервер ЭП и др. С функциональной компьютерной системой HSM интегрируется обычно через сетевые интерфейсы, и в связи с этим значительно упрощается аттестация системы [Там же. С. 809–810]. Строится этот специальный компонент системы на обыкновенных универсальных ПЭВМ со всеми свойственными им проблемами – как надежности, так и безопасности.

И вторая ветка – РКБ (резидентный компонент безопасности) – узкоспециализированный примитивный компьютер, встраиваемый в защищаемую систему (любого масштаба и размера – например, в планшет).

В то же время легко заметить, что эти примеры не совсем параллельны ни ситуации с универсальными и специальными ОС, ни ситуации с универсальными и специальными компьютерами.

Если предельно обострить формулировку противопоставления универсальных и специализированных СВТ, то универсальные средне делают все, а специализированные – очень хорошо делают что-то одно. Еще раз подчеркну, что это намеренно грубая формулировка, призванная подчеркнуть отличие приведенных примеров из области технической защиты информации.

Казалось бы, параллельность тут и невозможна, ведь трудно сформулировать, какой могла бы быть сфера применения действительно универсальных СЗИ – делающих все подряд с неким средне приемлемым уровнем качества. Более того, если на этапе преобладания стационарных универсальных ПК такие СЗИ могут быть желательны по принципу 1 ПК – 1 СЗИ (волшебная таблетка – съел и порядок), то по мере перехода на сетевые и облачные технологии это тоже теряет смысл – обработка данных становится распределенной, распределенными неизбежно становятся и технологии защиты.

Этот тезис существенным образом укрепляется тем, что предпосылки к тому, чтобы средства становились именно специализированными, имеют совершенно разную природу.

Во-первых, это дешевле. И для разработчика, и для покупателя. При не очень продуманном проектировании это может получиться несколько дороже в производстве – несколько маленьких партий дороже в производстве одной большой – но если ошибок в проектировании не допускать, то этого можно избежать.

Это дешевле даже сертифицировать, так как на стоимость сертификационных исследований непосредственно влияет объем и сложность необходимых проверок.

Во-вторых, чем меньше сложность – тем меньше ошибок, значит, повышается надежность и живучесть продукта, меньше трудоемкость его сопровождения и обслуживания.

В-третьих, чем меньше сложность – тем легче использовать, меньше требования к эксплуатирующему персоналу, меньше вероятность неправильного применения и неосуществления защитных функций в результате неправильного применения.

Поддержка тенденции к специализации средств со стороны регулятора отражается в изменении подхода к оценке сертифицируемых продуктов в этом направлении сразу в двух разных аспектах.

1. Во-первых, определено некоторое множество функциональных направлений безопасности: антивирусная защита, доверенная загрузка, контроль съёмных носителей информации и др. И объект оценки при сертификации с этой точки зрения – средство защиты информации, реализующее требуемый набор элементарных функций безопасности строго в рамках одного целевого направления: средство антивирусной защиты, средство доверенной загрузки, средство контроля съёмных носителей и др. Комплексные средства, реализующие функции, относящиеся к разным направлениям, не приветствуются.
2. Во-вторых, при этом для каждого объекта оценки при сертификации строго обозначается среда функционирования и требования к ней. То есть с этой точки зрения объект оценки при сертификации – средство, реализующее функцию в строго оговоренных условиях (например, ОС указанной версии; определенная аппаратная платформа; известные модели и версии сторонних аппаратных средств, таких как программные библиотеки, аппаратные идентификаторы).

Таким образом, «универсальность» СЗИ «ограничивается» регулятором сразу по двум направлениям. Это явно не случайность, а ясно осознаваемая позиция.

Получается, что все доводы со стороны разработчика, эксплуататора и регулятора – за специальные средства, а не за универсальные.

Есть только одна причина на то, чтобы в СЗИ наращивался набор функций – это конкурентная борьба за участие и по возможности победу в конкурсах и аукционах по 44-ФЗ. Естественно, что чем большему спектру требований удовлетворяет продукт, тем под условия большего числа конкурсов он подпадает, хотя ни одной из будущих эксплуатирующих организаций фактически не требуется универсальное СЗИ с избыточной функциональностью.

Разумеется, невозможно противодействовать разумными средствами как тому, чтобы в качестве конкурсных требований фигурировали уникальные особенности продукта, который в итоге хотела бы приобрести будущая эксплуатирующая организация, так и тому, чтобы эти уникальные особенности перекочевывали в конкурентные решения. Думается, что выход, способный примирить логику развития техники с логикой организации закупок, все же в том, чтобы наращивать ассортимент узкоспециализированных средств, а не ассортимент функций в тяжелой универсальной системе.

Мы идем именно по такому пути, и получаются довольно любопытные семейства решений.

Наиболее наглядно идея просматривается на примере семейства продуктов на основе USB-накопителей с управляемым доступом к памяти.

В этой родовой формулировке обозначены два параметра, значения которых можно менять, создавая разные продукты – можно менять атрибуты доступа к памяти (доступ только на чтение (read only, RO), на чтение и запись (read/write, RW), только на добавление (add only, AO)) и можно менять протокол доступа пользователя к памяти (всем и везде; только зарегистрированным; всем, но только на зарегистрированных компьютерах; зарегистрированным с разными ролями – доступ с разными правами (или даже атрибутами), и так далее).

Если добавить сюда умение разбивать память на нужное количество разделов с разными атрибутами доступа, то на общей (во всяком случае, достаточно унифицированной, в рамках разумных экономических ограничений) аппаратной базе получается целый спектр продуктов следующих групп функциональности:

1. Защищенные USB-накопители – для которых главным свойством является возможность ограничить те СВТ, на которых устройство будет работать – это семейство защищенных флешек Секрет и специализированные ответвления – Программно-аппаратный журнал (ПАЖ) и Идеальный токен, по существу и не являющийся флешкой;
2. Носители персональной среды – для которых ключевым является загрузка из неизменяемой памяти – это СОДС МАРШ! и носители ПО Центр-Т, а также ответвление, в котором из неизменяемой памяти загружается не среда, а прикладное ПО – это мобильный носитель лицензий (МНЛ).

В рамках этой темы описание этих продуктов имеет смысл ограничить тем, что касается проявления в них тенденции специализации.

**1 группа: защищенные USB-накопители**

Флешка – устройство универсальное. Оно работает на любом компьютере, данные могут как читаться с ее диска, так и записываться на него, как любым пользователем, так и системой (так происходит с вирусами, для их чтения с флешки и записи на флешку усилий пользователя не требуется).

Достаточно часто предпринимаются попытки разной степени успешности специализировать их для определенных пользователей – добавить механизмы аутентификации пользователя флешки. Разумеется, мы тоже эти механизмы в свои USB-накопители всегда добавляем, но по ряду причин часто делаем опциональными.

В первую же очередь, создав семейство «Секрет», мы специализировали флешки для применения только на тех компьютерах, на которых явно разрешено, а не на всех. Причем решение принимает не компьютер, а устройство – задача снабдить каким-то программном обеспечением решительно все компьютеры в мире для нас, пожалуй, слишком амбициозна, а вот все устройства, которые выпускаем только мы – более реально.

Так получилось устройство, диск которого монтируется только на тех компьютерах, которые известны устройству как разрешенные для работы, а пользователю он становится доступным после его аутентификации. Таким образом, записать на такую флешку вирус, или считать его с нее, невозможно на неразрешенном компьютере никак, даже при желании пользователя.

Решая задачу необходимости работать без установки какого-либо ПО на компьютеры, на которых предполагается работа с «Секретами», мы создали модификацию «Секрет особого назначения», диск которого разбит на разделы – доступный на любом ПК, но только для чтения, с которого стартует его ПО, доступный для чтения и записи, но только на разрешенных ПК и только для пользователя, где хранятся собственно данные пользователя, и раздел для записи собственного журнала устройства, доступный на любом ПК на запись, а на чтение – только для администратора устройства.

Затем оказалось, что это еще не предел специализации. В некоторых случаях оказалось полезным введение дополнительного ограничения – на время действия политики. Допустим, на какой-то определенный день или несколько дней, может быть нужно снять ограничение на подключение к «чужим» компьютерам (на время командировки или сдачи отчета куда-то), а затем снова его возобновить. Или на время установить (или снять) режим работы без пароля пользователя. Для корректной реализации такой возможности нужны встроенные часы – RTC. Этот компонент удорожает изделие, и в большинстве случаев является избыточным, поэтому мы не стали добавлять его во все виды «Секретов», а сделали отдельную модификацию с часами – на базе только той модели, для которой эта функция оказалась востребованной, так получился «Секрет руководителя».

 А еще жизнь подсказала, что областью применения устройства, похожего на «Секрет» может стать сбор и хранение журналов событий, потому что накопитель, различающий компьютеры – прекрасный помощник админа в том, чтобы не смешать случайно журналы с разных ПК, что в дальнейшем приведет неизбежно к путанице при попытке анализа. Но есть нюанс, журналы должны храниться на носителе, защищенном от перезаписи. Для этой задачи мы сделали программно-аппаратный неперезаписываемый журнал «ПАЖ», в котором диск находится в режиме Add only.

Проанализировав специфику работы с журналами, мы поняли, что в каждой организации в отношении манипуляций с этими данными могут задаваться довольно серьезно различающиеся ролевые политики. Функции сбора журналов, их просмотра, установки политик работы с устройством, просмотра собственного журнала работы устройства – могут распределяться по в среднем 4 типам ролей – оператор, администратор, администратор информационной безопасности и аудитор (контролер). Поэтому здесь мы решили оставить пространство для специализации политик собственными силами эксплуатирующей организации и сделали роли настраиваемыми – администратор устройства создает роли, называет их и наделяет набором прав самостоятельно.

Наконец еще одна специализированная потребность – иногда может быть вовсе не нужен диск массторадж. Это случай хранения ключевой информации, токен. Устройство Идеальный токен мы снабдили механизмом распознавания разрешенных компьютеров, но не стали оснащать диском, он ключевому носителю не нужен.

**2 группа: носители персональной среды**

Вторая группа ограничений, наложенных нами на универсальные USB-накопители – это ограничение на запись в память. Это кажется довольно абсурдным, однако, это только на первый взгляд, так как для загрузочных устройств, вообще говоря, это совершенно естественная функциональность.

При этом если для Центр-Т носитель должен иметь как минимум один раздел памяти RW (поскольку необходимо хранить параметры, которые должны настраиваться и не могут быть зафиксированы раз и навсегда), но может иметь еще RO, в котором будут храниться скачанные образы ОС для ускорения процесса загрузки, то для СОДС МАРШ! необходимо разбиение памяти на разделы с разными атрибутами доступа – RO для основной загружаемой ОС, AO для журналов, RW Hidden для ключей, в некоторых случаях еще RW в качестве «почтового ящика» для хранения пользовательских данных.

Однако не только для загрузочных устройств имеет смысл ограничивать возможности записи в память. Загрузочным устройством называется такое, с которого загружается ОС. А если это не ОС, а прикладное ПО? Или вообще не ПО, а данные, но которые должны оставаться в неизменном виде и загружаться с USB-накопителя? Такое устройство загрузочным уже не называется, но в остальном подход применим и к нему.

По такому принципу мы сделали Мобильный носитель лицензий (МНЛ). Это устройство, которое позволяет сгенерировать лицензию с учетом данных конкретной системы без обращения к фирме-производителю ПО, на основании данных о количестве приобретенных лицензий. На диске устройства при этом хранится только неизменное программное обеспечение комплекса, поэтому он при производстве переводится в RO режим.

И последнее решение, о котором имеет смысл упомянуть в этом контексте – это комбинация 1 и 2 групп – однонаправленный шлюз на базе «Секрета особого назначения», функциональность которого в интересующем нас аспекте сводится к тому, что на одной группе разрешенных СВТ открытый раздел устройства доступен на чтение и запись (например, это компьютер, с которого будут записываться какие-нибудь обновления), а на другой группе – только на чтение (это в нашем примере будут те СВТ, куда нужно раздать обновление, но не подхватить вирус).

Важно, что ограничительные механизмы могут комбинироваться в разнообразных сочетаниях, а не накапливаться в одном устройстве, делая его по сложности почти человеком.

Развитие идеи специализации универсального устройства в другом направлении можно продемонстрировать на примере уже упомянутых МАРШ! и Центр-Т в аспекте создания специальных образов АРМ вместо поддержки тяжеловесных универсальных ОС. В этом смысле функциональное различие между МАРШ! и Центр-Т в том, что они предназначены для систем с разной степенью унифицированности ПО клиентских СВТ. Если это работа в веб-системе с минимумом локальных программных средств – идеален МАРШ!, образ которого формируется на стадии производства – для каждой конкретной системы, для которой выпускается именно эта партия, а если это терминальная система или смешанная система с разными требованиями к разным клиентским АРМам, то идеален администрируемый эксплуатирующей организацией Центр-Т, где каждый образ клиента создается предоставленным администратору инструментарием. Индивидуализация загружаемых образов позволяет делать их неизбыточными, что важно как для производительности, так и для защищенности – контролировать маленький образ проще, чем тяжеловесную ОС.

Эта же логика – формирования образа ПО на заказ и запись его постоянной части в память RO – лежит и в основе работы с микрокомпьютерами с вирусным иммунитетом – семейства MKT. Это парадигма микрокомпьютеров, в которой есть компьютеры с одной (защищенной) или двумя (защищенной и обыкновенной) ОС, с экраном (планшеты) и без, со стационарной док-станцией (MKT-card и MKT-card long) и полностью мобильные. Мы не стали делать один «большой» микрокомпьютер, а сделали ассортимент подходящих для разных задач – в конце концов, что не понравится, можно перестать выпускать. А общая их ключевая особенность – Новая гарвардская архитектура – предполагающая необходимость формировать образ ПО продуманно, так, чтобы его не приходилось систематически менять, поскольку сделать это можно только в специальной сервисном режиме, повлекла за собой и следующий шаг развития – отдельный компьютер на отдельную задачу. Эдакое идеальное состояние с точки зрения безопасности – один компьютер для одной задачи, никакого взаимовлияния. При этом рабочее место может состоять из большого числа таких компьютеров, набор которых можно менять в по мере необходимости без перенастройки и даже без остановки процессов, выполняющихся в это время на других компьютерах этого рабочего места. Такому решению будет посвящен отдельный доклад.

Люди моего поколения легко вспомнят, что первое мы слышали про компьютеры на уроках информатики – в основе компьютера лежит магистрально-модульный механизм. Модули – это очень удобно на всех уровнях. В том числе и на уровне закупок.

Список литературы:

1. Научные проблемы национальной безопасности Российской Федерации. Вып. 4. М., 2007.
2. Конявский В. А., Лопаткин С. В. Компьютерная преступность. Т. II. М., 2008.
3. Конявский В. А. Иммунитет как результат эволюции ЭВМ // Защита информации. Inside. Спб., 2017. № 4. С. 46–52.
4. Конявский В. А. Компьютерная техника: плач по импортозамещению // Защита информации. Inside. Спб., 2017. № 5. С. 26–29.