УДК 004

Отношение дихотомии "универсальное"/"специальное" СЗИ к понятию комплексной защиты информации

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

Проводится граница между понятиями "универсальное" и "комплексное", разграничиваются подходы, при одном из которых средства защиты информации (СЗИ) снабжаются как можно большим числом функций, а при другом — создаются линейки средств с разными наборами функций, из которых можно выбрать целесообразный для конкретной системы набор. Приводятся примеры построения таких линеек.

Ключевые слова: универсальное, комплексное, специальное, средство защиты информации.

Противопоставление специального и универсального в самых различных областях (питания, одежды, автомобилей, вычислительной техники, средств связи, косметики и т. д.), по-видимому, свойственно природе человека как само по себе, так и в плане различных нарушений этого противопоставления.

Так, джинсы из спецодежды превратились в универсальный предмет гардероба, а повседневные наряды прошедших эпох становятся сценическими костюмами, Hummer и Gelandewagen стали универсальными автомобилями, а Peugeot — полицейской, радиотелефоны и скремблеры стали бытовыми приборами, а пейджеры — средствами оперативной связи медиков и экстренных служб. Аналогичных примеров множество.

Развитие средств вычислительной техники — не исключение из общего правила. Эта тенденция здесь тем заметнее, чем заметнее изменения данной отрасли в целом по сравнению с другими, не столь стремительно развивающимися областями жизни. В отношении операционных систем об этом, в частности, писал В. А. Конявский (см. [1], С. 211, 212, [2], С. 808). Он 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 в менее явной форме (см. например, [2], С. 809—811, [3, 4]).

Казалось бы, в сфере защиты информации эта дихотомия проявиться не может в принципе, потому что средство защиты информации само по себе представляет высокоспециализированное техническое (или программное) средство, однако это не так.

В первую очередь дихотомия проявляет себя действительно в сущностном, категориальном признаке технической защиты информации: техническая защита информации — это ограничение универсальности СВТ. Защищенный компьютер — уже не универсальный компьютер, на нем возможности пользователя существенно ограничены.

Предельный случай, ярко проявляющий эту черту, — функционально замкнутая среда (ФЗС), когда компьютер (полноценный, универсальный, являющийся фон-неймановской реализацией машины Тьюринга) используется в каждый момент времени только для одной задачи, в результате чего избегается нежелательное взаимовлияние программ (см. [2], С. 739).

Если вынести эту задачу в отдельное специализированное устройство, то компьютер можно не лишать универсальности, а делать специализированным только на время доверенного сеанса связи (ДСС), подключая к нему 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 без-

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

Статья поступила в редакцию 11 мая 2018 г.

опасностью. Обычно это межсетевой экран, криптомаршрутизатор, сервер электронной подписи (ЭП) и т. д. С функциональной компьютерной системой HSM интегрируется обычно через сетевые интерфейсы, в связи с чем значительно упрощается аттестация системы (см. например, [2], С. 809—810). Строится этот специальный компонент системы на обыкновенных универсальных ПЭВМ со всеми свойственными им проблемами, как надежности, так и безопасности.

Вторая ветка — РКБ (резидентный компонент безопасности) — узкоспециализированный примитивный компьютер, встраиваемый в защищаемую систему (под системой здесь понимается компьютерная система любого масштаба и физического размера, например планшет).

Очевидно, что эти примеры не совсем отвечают ситуации с универсальными и специальными ОС, а также ситуации с универсальными и специальными компьютерами.

Если предельно упростить формулировку противопоставления универсальных и специализированных СВТ, то универсальные *посредственно* выполняют *любые задачи*, а специализированные *на высоком уровне* выполняют *узкий круг задач*. Следует подчеркнуть, что это намеренно грубая формулировка, призванная подчеркнуть отличие приведенных примеров из области технической защиты информации.

Казалось бы, параллельность здесь невозможна, поскольку сложно сформулировать, какой могла бы быть сфера применения по-настоящему универсальных СЗИ, выполняющих любые защитные функции 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 ("серебряная пуля"), то по мере перехода на сетевые и облачные технологии это также теряет смысл: обработка данных становится распределенной, распределенными неизбежно становятся и технологии защиты.

Этот тезис существенным образом укрепляется тем, что предпосылки к специализации средств защиты имеют совершенно разную природу.

Во-первых, это экономические предпосылки. Специализированные средства имеют более низкую стоимость и для разработчика, и для покупателя. При не очень продуманном проектировании специализированные средства могут иметь более высокую стоимость производства, так как производство нескольких маленьких партий в общем случае дороже одной большой, но если ошибок в проектировании не допускать, то этого можно избежать.

Ниже будет также и стоимость сертификации, так как на стоимость сертификационных исследований непосредственно влияют объем и сложность необходимых проверок.

Во-вторых, сложность продукта прямо влияет на количество ошибок в нем, поэтому при снижении сложности повышаются надежность и живучесть продукта, снижается трудоемкость его сопровождения и обслуживания.

В-третьих, чем менее сложен продукт, тем проще он в эксплуатации, тем менее жесткие требования предъявляются к эксплуатирующему персоналу, снижается 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 аспектах.

- Регулятором определено некоторое множество функциональных направлений безопасности: антивирусная защита, доверенная загрузка, контроль съемных носителей информации и т. д. 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 съемных носителей и т. д. Комплексные средства, реализующие функции, относящиеся к разным направлениям, не приветствуются.
- Для каждого объекта оценки при сертификации строго обозначаются среда функционирования и требования к ней. Таким образом, 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).

Итак, "универсальность" СЗИ "ограничивается" регулятором сразу по двум направлениям. Это, разумеется, не может интерпретироваться как случайность, а является проявлением определенной позиции.

Таким образом, как со стороны разработчика, так и со стороны эксплуатирующих организаций и регулятора обнаруживаются доводы исключительно в пользу специальных средств, а не универсальных.

Единственной причиной для наращивания набора функций СЗИ является конкурентная борьба за участие и, по мере возможности, победу в

конкурсах и аукционах по 44-ФЗ. Очевидно, 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.

Противодействие 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 переходили в конкурентные решения, не представляется возможным никакими рациональными путями. Выход, способный примирить логику развития техники с логикой организации закупок, может быть в наращивании ассортимента узкоспециализированных средств, а не в наращивании ассортимента функций в тяжелой универсальной системе.

Рассмотреть детально такую логику подхода к разработке можно на примере специализированных линеек средств защиты информации ОКБ САПР.

Наиболее наглядно этот подход можно проиллюстрировать с помощью семейств продуктов на основе USB-накопителей с управляемым доступом к памяти.

В этой родовой формулировке обозначены два параметра, значения которых можно менять, создавая концепты разных продуктов: 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 протокол доступа пользователя к памяти (без ограничений пользователей и компьютеров; только зарегистрированным пользователям, но на всех компьютерах; всем пользователям, но только на зарегистрированных компьютерах; зарегистрированным с разными ролями пользователям (доступ с разными правами или даже атрибутами) и т. д.).

Если добавить к этому возможность 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:

- Защищенные USB-накопители, чьим главным свойством является возможность ограничить те СВТ, на которых устройство будет работать. Это семейство защищенных служебных носителей "Секрет" и специализированные ответвления данного семейства: "Программно-аппаратный журнал" (ПАЖ) и "Идеальный токен", который, будучи токеном, не является USB-накопителем в прямом смысле слова, не имеет диска mass-storage;
- 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 (мобильный носитель лицензий — МНЛ).

В рамках данной темы описание продуктов имеет смысл ограничить тем, что касается проявления в них тенденции специализации. Продукты представлены на сайтах производителя. Для более детального знакомства с ними можно обратиться к их официальным описаниям.

Первая группа: защищенные USB-накопители

USB-накопитель ("флешка") является универсальным устройством. Он работает на любом компьютере. Данные могут как читаться с его диска, так и записываться на него как любым пользователем, так и системой (так происходит с вирусами; для их чтения с USB-накопителя и записи на него усилий пользователя не требуется).

Достаточно часто предпринимаются попытки (в разной степени успешные) сделать эти устройства специализированными путем ограничения числа пользователей, т. е. добавить механизмы аутентификации пользователя USB-накопителя. В устройства ОКБ САПР также добавлены соответствующие механизмы, но по ряду причин они являются в основном опциональными.

Созданием семейства "Секрет" в первую очередь удалось специализировать USB-накопители для применения только на тех компьютерах, на которых это явно разрешено. При этом решение о возможности монтирования принимает не компьютер, а устройство: задача снабдить каким-либо программным обеспечением все компьютеры в мире представляется мало реалистичной в отличие от обеспечения определенными функциями всех служебных носителей собственного выпуска.

В результате этого подхода разработано 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 такой USB-накопитель вирус или считать с него вирус на неразрешенном компьютере невозможно даже при содействии пользователя.

При необходимости работы с "Секретами" без установки какого-либо ПО на компьютеры создана модификация "Секрет особого назначения",

диск которого разбит на разделы: доступный на любом ПК, но только для чтения (с этого раздела стартует ПО продукта), доступный для чтения и записи, но только на разрешенных ПК и только для пользователя (на этом разделе хранятся собственно данные пользователя), для записи собственного журнала устройства, доступный на любом ПК и при работе под правами любого пользователя на запись, а на чтение — только для администратора устройства.

Однако выяснилось, что этим возможности специализации продукта не исчерпываются. При некоторых сценариях использования может быть полезным введение дополнительного ограничения на время действия политики. Допустим, на какой-то определенный день или несколько дней нужно снять ограничение на подключение к "чужим" компьютерам (на время командировки или санкционированной передачи каких-то данных, предположим отчета, из системы), а затем снова его возобновить, или на время установить (или снять) режим работы без пароля пользователя. Для корректной реализации такой возможности необходим независимый от компьютера инструмент контроля времени — встроенные часы (RTC). Этот компонент удорожает изделие и в большинстве случаев является избыточным, поэтому он не добавлен во все виды "Секретов". Создана отдельная модификация с часами на базе только той модели, для которой эта функция оказалась востребованной. Так был разработан продукт "Секрет руководителя".

В ходе взаимодействия с пользователями устройств ОКБ САПР было установлено, что областью применения устройства, похожего на "Секрет", могут стать сбор и хранение журналов событий, поскольку накопитель, "различающий" компьютеры, может быть весьма полезен администратору системы, собирающему журналы событий с разных рабочих станций для их последующего раздельного хранения. Запись журналов с разных ПК на один носитель в дальнейшем может привести к путанице при попытке анализа, а вероятность перепутать носители при сборе журналов и случайно записать журнал с одного ПК в архив с другого очень велика. Носитель, различающий компьютеры, не даст совершить такую ошибку, однако журналы должны храниться на носителе, защищенном от перезаписи. Для этой цели был создан программно-аппаратный неперезаписываемый журнал "ПАЖ", в котором диск находится в режиме Add only.

Анализ специфики работы с журналами показал, 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 в среднем по 4 типам ролей: оператор, администратор, администратор информационной безопасности и аудитор (контролер). Поэтому было принято решение оставить возможность для специализации политик собственными силами эксплуатирующей организации: сделать роли настраиваемыми (администратор устройства создает роли, называет их и наделяет набором прав самостоятельно).

Нельзя не учитывать, что некоторые виды данных хранятся в защищенных носителях вообще не на диске mass-storage. Последний в этом случае может быть избыточен. Это случай хранения ключевой информации, токен. Устройство "Идеальный токен" снабжено механизмом распознавания разрешенных компьютеров, но освобождено от диска, не нужного ключевому носителю.

Вторая группа: носители персональной среды

Вторая группа ограничений, накладываемых в продуктах ОКБ САПР на универсальные USB-накопители, — это ограничение на запись в память. На первый взгляд такая постановка вопроса звучит несколько экстравагантно, однако это совершенно естественная функциональность для загрузочных устройств, о которых преимущественно и пойдет речь в этом разделе.

Ограничения эти могут быть различными. Если для "Центр-Т" носитель должен иметь как минимум один раздел памяти RW (для хранения параметров, 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, а в некоторых случаях еще и RW — в качестве "почтового ящика" для хранения пользовательских данных.

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

По такому принципу сделан 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 хранится только неизменное программное обеспечение комплекса, поэтому он при производстве переводится в RO-режим.

Последнее решение, о котором имеет смысл здесь упомянуть, — это комбинация 1-й и 2-й групп, однонаправленный шлюз на базе "Секрета особого назначения", функциональность которого в данном контексте 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-либо обновления), а на другой группе — только на чтение (это в данном примере будут те СВТ, куда нужно передать обновление, но не подхватить оттуда вирус).

Важно, что ограничительные механизмы могут комбинироваться в разнообразных сочетаниях, а не накапливаться в одном устройстве, приближая его по сложности к разумному существу.

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 состоит 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 записи его постоянной части в память RO лежит в основе работы с микрокомпьютерами с "вирусным иммунитетом" семейства МКТ. Это парадигма микрокомпьютеров, в которой есть компьютеры с одной (защищенной) или двумя (защищенной и незащищенной) ОС, с экраном (планшеты) и без него, со стационарной докстанцией (МКТ-card и МКТ-card long) и полностью мобильные. Вместо того чтобы реализовать все эти возможности сразу в одной модели, принято решение создать ассортимент микрокомпьютеров, подходящих для разных задач, поскольку такой подход облегчает в числе прочего и отказ от неудачных решений: их можно перестать выпускать, и это никак не затронет остальные продукты линейки.

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 специальном сервисном режиме, повлекла за собой и следующий шаг развития — отдельный компьютер на отдельную задачу. Это идеальное состояние с точки зрения безопасности — один компьютер для одной задачи, ФЗС в собственном смысле слова с гарантированным отсутствием взаимовлияния. При этом рабочее место может состоять из большого числа таких компьютеров, набор которых можно менять по мере необходимости без перенастройки и даже без остановки процессов, выполняемых в это время на других компьютерах данного рабочего места.

Когда в школах только появился предмет "информатика", первым, что узнавали школьники о компьютере, было то, что в его основе лежит магистрально-модульный механизм. По-видимому, уже настало время для того, чтобы этот принцип перешел на новый виток спирали.

Литература

1. Научные проблемы национальной безопасности Российской Федерации. — М., 2007. Вып. 4.

2. *Конявский В. А., Лопаткин С. В.* Компьютерная преступность. — М., 2008. Т. II.

3. *Конявский В. А.* Иммунитет как результат эволюции ЭВМ // Защита информации. Inside. 2017. № 4. С. 46—52.

4. *Конявский В. А.* Компьютерная техника: плач по импортозамещению // Защита информации. Inside. 2017. № 5. С. 26—29.

The ratio of the dichotomy "universal"/"special" information security tool to the concept of complex information protection

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 a boundary between the concepts of universal and complex. The two approaches are distinguished, with one of which information security tools are supplied with as many functions as possible, and with the other — a line of tools with different sets of functions are created, from which it is possible to choose a suitable set for a particular system. Examples of construction of such lines are given.

Keywords: universal, complex, special, information security tool.

Bibliography — 4 references. *Received May 11, 2018*