О происхождении видов, или Как лечить болезнь, а не симптомы

En

On the Origin of Species, or the Way to Treat the Disease Rather than Its Symptoms

S. V. Konyavskaya,
PhD (Philology), Deputy General Director
OKBSAPR,
Lecturer of the Information Security Department
Moscow Institute of Physics and Technology
cd@okbsapr.ru

The two main directions of computers' architecture change in order to execute the principle architecture violence of Turing machine models are briefly descripted in the article. Also some examples of these approaches realizations are shown.

Keywords: computers' architecture, trusted startup, trusted startup hardware module, new harvard architecture, secure microcomputers, USB-drive, tokens, log storages

В статье тезисно описаны два основных направления изменения архитектуры компьютера, направленные на то, чтобы компенсировать принципиальную архитектурную уязвимость вычислительных устройств, моделирующих машину Тьюринга, и приведены примеры реализаций этих подходов.

Ключевые слова: архитектура компьютера, доверенная загрузка, аппаратный модуль доверенной загрузки, новая гарвардская архитектура, защищенные микрокомпьютеры, флеш-накопители, токены, хранилища журналов

Светлана Валерьевна Конявская,
кандидат филологических наук,
заместитель генерального директора
ЗАО «ОКБ САПР»,
преподаватель кафедры «Защита информации» факультета радиотехники и кибернетики
Московский физико-технический институт
cd@okbsapr.ru

Введение

Каждый день, выходя из дома, мы, даже не задумываясь, запираем дверь, так как накопленный за многие годы опыт однозначен – это полезно для сохранения в неприкосновенности принадлежащих нам вещей. Конечно, дверь, замок и ключ не решают проблему воровства полностью, но ни у кого не возникает сомнения, что дверь все же должна быть, и чтобы вор в нее не влез, необходимо не носить ее с собой, а запирать по месту установки. Другими словами, находящиеся в квартире вещи будут в *большей безопасности*, если предпринять некоторые шаги по защите квартиры.

Аналогия верна и для компьютера. Программы и данные, составляющие информационные ресурсы, легче сохранить, если компьютер будет защищен.

Как мы уже говорили, запертая дверь не гарантирует того, что вещи не украдут. Защита компьютера – тоже не гарантия от нарушения целостности программ, но это *абсолютно необходимый* рубеж защиты. Вещи из квартиры *точно* украдут, если дверь оставить нараспашку. Без защиты компьютера невозможно обеспечить защиту программ.

Однако даже если ваши вещи будут находиться внутри защищенной квартиры, вовсе не обязательно, что они сохранятся в первозданном виде. Если вы в этом не уверены, попробуйте, *не выходя из квартиры*, вместе с рубашкой постирать паспорт. В виртуальном мире одна программа в процессе исполнения также вполне может изменить состояние данных другой программы и даже код дру-

гой программы. Так, собственно, и ведут себя вирусы, да и не только они [1].

Исторически сложилось так, что современные компьютеры являются реализацией идеи «машины Тьюринга» [2], то есть универсального исполнителя. Это означает, что принципиально – архитектурно – они созданы так, чтобы выполнить любую задачу. Любую, а не только те, что мы бы от них хотели.

Удивительно, но, скорее всего, не обладая в большинстве своем знаниями о машине Тьюринга и ее архитектурных особенностях, эту довольно специфичную проблему компьютерной безопасности хорошо чувствуют гуманитарно ориентированные люди – писатели, поэты, священнослужители – формулируя в тех или иных словах мысль, что пусть компьютеры и могут всё, но наша задача – заставить их делать только то, что требуется человеку. Мы, пожалуй, довольно далеки от опасений насчет бунта компьютеров и захвата ими власти над миром, но полностью разделяем убежденность в том, что универсальность современных компьютеров является основным источником всех связанных с компьютерной сферой угроз. Если компьютер способен выполнить любую задачу, то он выполнит и вредоносную.

Именно в этом состоит цель мероприятий по обеспечению информационной безопасности, если посмотреть на нее с определенной дистанции: нам необходимо добиться того, чтобы все наши (то есть легальные) задачи решались, а задачи злоумышленников (нелегальные) – не решались.

Защита информации – это ограничение универсальности средств вычислительной техники.

Ниже изложим тезисно основные направления, двигаясь в которых, можно этого добиться.

Поскольку архитектуру компьютера нельзя изменить программным путем, то никакие программные средства не помогут нам защититься от хакеров надежно. Если говорить о совершенствовании архитектуры, то здесь мы подходим к первому, самому радикальному разделению направлений. Мы можем либо усовершенствовать архитектуру *уже существующих технических средств*, либо использовать *новые технические средства*, созданные на базе более совершенной архитектуры.

Следуя первому направлению, эксплуатирующие организации, приобретая новую технику, устанавливают на нее те или иные средства защиты, следуя второму – приобретают технику, спроектированную тем или иным особым образом.

I. Средства защиты, изменяющие архитектуру устройств (наложенные средства защиты информации)

Чтобы убедиться в неизменности аппаратной и программной среды компьютера, необходимо провести контрольные процедуры. Однако очевидно, что если последние производятся измененным в свою очередь компонентом, то в них нет никакого смысла.

Именно поэтому нельзя контролировать неизменность среды программными средствами: программа может быть изменена. Для убежденности, что этого не произошло, ее нужно сначала проверить. Если мы станем это делать с помощью другой программы, то сначала придется проверить ту программу, которой мы проверяем первую… И так до бесконечности: мы попадаем в зону действия известного парадокса «кто будет сторожить сторожей?». В области защиты информации попытки контролировать целостность среды программными средствами носят название «синдром Мюнгхаузена», поскольку они аналогичны попыткам вытащить из болота себя самого за волосы [1, 3, 4].

Продолжая эту аналогию, легко прийти к правильным выводам: вытащить себя из болота за волосы – нельзя, потому что нет точки опоры. А вот если тянуть за ветку дерева, растущего на кочке, то можно, потому что у дерева точка опоры есть.

Что может означать «точка опоры» применительно к компьютерной системе «фон неймановского» типа (а абсолютное большинство современных настольных компьютеров имеют именно такую архитектуру), не различающей команды и данные, в которой одним из основных действий является «запись», то есть системе принципиально модифицируемой? «Точка опоры» может означать только одно: контролирующие процедуры должны быть вынесены из этой модифицируемой среды в среду немодифицируемую и легко проверяемую, то есть простую и небольшую по объему (тогда легко обеспечить ее верифицируемость). На практике это означает, что требуется аппаратное устройство, независимое от компьютера, который оно проверяет.

Независимость контролирующего устройства – обязательное требование: если часть процедур или решений об обработке их результатов вынесены в основной (контролируемый) компьютер, то модифицированной системой могут быть навязаны любые результаты контроля. Эффект от применения аппаратуры сведется к нулю.

И наконец, самое главное – независимое аппаратное контролирующее устройство должно стартовать первым, до старта операционной системы (ОС), иначе у модифицированной системы будет возможность отключить контролера. «Кто первый встал, того и тапки»: стартовать первым должно то устройство, которому мы доверяем.

Такое аппаратное, простое, независимое от компьютера контролирующее устройство, стартующее первым, до загрузки ОС ЭВМ, называется резидентным компонентом безопасности (РКБ) [1].

Резидентный компонент безопасности – это встроенный в вычислительную систему объект, способный контролировать целостность среды путем сравнения ее параметров с эталонными.

Задача РКБ – сделать так, чтобы защищаемый компьютер переставал быть универсальным или «машиной Тьюринга» только на этапе прохождения контрольных процедур, а потом, после их успешного завершения, пользователю снова становились бы доступны все плюсы универсальности.

Ключевые характеристики РКБ:

- очень высокий уровень защищенности (его внутреннее программное обеспечение должно быть немодифицируемым);
- примитивная конструкция (иначе обеспечение его собственной защищенности эквивалентно задаче защиты компьютера, который он защищает);
- встроенность в контролируемую систему и старт до начала работы основной ОС (иначе его функционирование будет необязательным);
- независимость от контролируемой системы (автономное функционирование);
- перестраиваемость, предполагающая функционирование как в режиме управления, когда возможно изменение политик безопасности (только специальным привилегированным пользователем), так и в пользовательском режиме, когда изменение политик невозможно, и осуществляется только контроль их выполнения.

Концепция РКБ реализована во всех решениях, которые описаны в этом разделе. Каждое из них включает в себя аппаратный компонент (базис) и может включать в себя программную надстройку, неразрывно связанную с этим базисом.

Практическая реализация парадигмы аппаратной защиты в нашей стране и в мире началась с появления СЗИ НСД «Аккорд-АМДЗ», положившего начало линейке «Аккорд» [3].

«Аккорд-АМДЗ» – это аппаратный модуль доверенной загрузки, РКБ, обеспечивающий тот самый «правильный» старт компьютера, доверенную загрузку его операционной системы.

«Доверенная загрузка» – это загрузка заранее определенной операционной системы с заранее определенных постоянных носителей после успешного завершения специальных процедур проверки заранее определенных условий (целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя).

«Аккорд-АМДЗ» может быть реализован на различных контроллерах, различающихся принципиально только шинными интерфейсами: PCI или PCI-X, PCI-express, Mini PCI-express, Mini PCI-express half card, m.2 (в настоящее время других аппаратных электронных замков для этой шины расширения нет, хотя очевидно, что именно она в ближайшее время станет основной).

Существует также вариант исполнения «Аккорд-АМДЗ» на базе USB-устройства, которое называется «Инаф» (от английского *enough* – достаточно). Этот вариант имеет определенные ограничения, которые должны восполняться организационными мерами или применением дополнительных механизмов, однако в ряде случаев этого вполне достаточно, отсюда и название.

«Аккорд-АМДЗ» контролирует только старт компьютера и не работает в операционной системе. Поэтому в тех случаях, когда необходимо не только загрузить доверенную среду, но и разграничить доступ к ресурсам компьютера уже в ходе работы пользователей, особенно при многопользовательском режиме или в распределенных инфраструктурах, необходимо применять программно-аппаратные комплексы на базе «Аккорд-АМДЗ» – ПАК «Аккорд-Win32», «Аккорд-Win64» или «Аккорд-X». Они предназначены, соответственно, для разграничения доступа в 32-х и 64-х разрядных ОС Windows и в ОС Linux.

Функциональность комплексов одинакова – в них реализованы дискреционный (с использованием 13 атрибутов) и мандатный механизмы разграничения доступа, в том числе – контроль печати из любых приложений на принтеры любых типов (сетевые, локальные, виртуальные).

Для терминальных систем как на базе Microsoft, так и на базе Citrix, предназначены версии TSE (*Terminal Server Edition*), поддерживающие управление терминальными сессиями. Серверные и клиентские компоненты комплексов взаимодействуют в рамках протоколов ICA или RDP, формируя собственный виртуальный канал.

За счет совокупности своих функций, включающих, в частности, и контроль запуска задач в программной части комплекса, ПАК «СЗИ НСД Аккорд» позволяет блокировать атаку на «перехват управления», на которой, в свою очередь, базируется большая часть хакерских атак[1].

Блокировать эту атаку возможно именно потому, что установка «Аккорда» позволяет «изменить» «фон Неймановскую» архитектуру защищаемого компьютера: в нем появляется неизменяемая память, разделяются потоки команд и данных, контрольные процедуры производятся в доверенной среде до запуска ОС. То есть, оставаясь «машиной Тьюринга», компьютер перестает быть ею на момент старта.

Для виртуальных инфраструктур, на которых сейчас все чаще строятся центры обработки данных (ЦОДы), в линейке «Аккордов» предназначены программно-аппаратные комплексы «Аккорд-В.» и «ГиперАккорд». Первый необходим для виртуализации на базе VMware, второй – для виртуализации на базе Microsoft [6].

Работа конечных пользователей с ЦОДом может строиться несколькими различными способами: работа с виртуальными рабочими станциями, работа на основе терминального доступа, web-доступа или смешанно. Во всех этих случаях пользователь физически работает на каком-то средстве вычислительной техники (СВТ), и оно также является объектом защиты, поскольку именно с него осуществляется доступ к защищаемому ЦОДу [7–9].

II. Устройства с правильной архитектурой

Если точно известно, в чем состоит уязвимость архитектуры, почему бы не пойти по пути эволюции самой архитектуры, исключив «дурной ген» в зародыше?

[1] *Обобщенная схема атаки на «перехват управления» и механизма ее отражения была опубликована в прошлом номере журнала в статье В. А. Конявского [5].*

1. Компьютеры

Очевидно, что избежать влияния потенциально опасных программ на функционирование критически важных, тех, которым следует выполняться исключительно корректно, невозможно, не изолировав одни от других. Именно поэтому на «рабочих» компьютерах, а особенно – на машинах, участвующих в технологических процессах, как правило обеспечена изолированная, а то и функционально-замкнутая программная среда [1]. Однако как изолировать клиент-банк на компьютере пользователя от его онлайн-игры? Решение заключается в том, что далеко не всегда действительно нужен «универсальный» исполнитель, ведь играть онлайн и отправлять платежное поручение совершенно не обязательно с помощью одного и того же компьютера.

Если базовая уязвимость универсальных компьютеров – в их архитектуре, значит, компьютер, удовлетворяющий требованию one-touch-security[2], должен быть создан на основе принципиально иной архитектуры, не имеющей этой уязвимости.

Теоретические и исторические предпосылки и основы этой – новой гарвардской – архитектуры приведены в уже упомянутой статье В. А. Конявского в прошлом номере журнала [9].

Ключевой для нашего сюжета момент заключается в том, что у такого компьютера архитектура будет отличаться на разных этапах (по сути, так же, как это происходит у компьютера с установленным «Аккордом») – это и есть динамически изменяемая новая гарвардская архитектура.

Для долговременного хранения используется память, для которой установлен режим «только чтение». При загрузке команды и данные размещаются в сеансовой памяти, в которой и исполняются. Это обеспечивает неизменность операционной системы, «вирусный иммунитет», и в то же время не мешает возможности применения адаптированных стандартных ОС и всего написанного для них программного обеспечения.

На базе компьютеров, построенных на такой архитектуре (их на сегодняшний день серийно выпускается 7 видов [10]), можно создавать автоматизированные рабочие места (АРМ) для самых разных видов информационного взаимодействия. С учетом того, что цена самого экономичного из этих компьютеров – МКТ – в 10–15 раз ниже традиционного компьютера на базе x86, то понятно, что это и есть современное решение для потенциальных клиентов дистанционного банковского обслуживания (ДБО) [11], в отношении которого исключено (если здраво смотреть на вещи) применение «тяжелых» средств защиты.

Таким образом, клиент банка получает ненастраиваемое устройство, которое обеспечивает загрузку неизменяемой проверенной операционной системы, устанавливает защищенное с использованием криптографических алгоритмов соединение с защищенным центром обработки данных, в котором установлено программное обеспечение (клиент ДБО) для доступа к АБС банка. Риски клиентов и банка сведены к минимуму. Клиент ДБО размещается в ЦОД, отвечающем всем требованиям по защите информации, соответственно, доступ к АБС выполняется из одной, достоверно известной точки – ЦОД, по защищенному каналу.

Технология доверенного сеанса связи гарантирует безопасность доступа клиента банка к своему клиенту ДБО (и, соответственно, к банку) из любой точки мира.

То есть клиент банка (человек) с помощью защищенного микрокомпьютера МКТ из любого гостиничного номера, где есть телевизор, защищенно соединяется с клиентом ДБО (программным обеспечением), размещенным на защищенном ЦОДе и по защищенному каналу взаимодействующим с защищенной АБС банка. Данные клиента обрабатываются в защищенной вычислительной среде, а хранятся на устройстве.

Конечно, заставить всех клиентов всех банков приобрести такое изделие нельзя, но целесообразно *рекомендовать* сделать это, так как при такой защите успешные хакерские атаки на компьютер клиента невозможны при сегодняшнем уровне развития техники. Обеспечиваемый при этом уровень защищенности вполне позволяет предложить клиенту-человеку программу страхования от кибермошенничества.

Для формирования правильного решения следует в клиентском договоре представить обоснованный выбор: управление счетом с использованием защищенного компьютера – и тогда все риски покрывает банк (или ЦОД, или страховая компания), либо в ход идут любые другие механизмы – тогда все риски остаются на владельце счета. Так банк и себя обезопасит, и обеспечит высокий уровень защищенности клиента. Самому же банку целесообразно рассмотреть возможность использования в качестве рабочих мест защищенных компьютеров МКТ-card long. Пример такого использования приведен в [12].

Теоретически очевидно (и на практике так оно и есть), что устройством с правильной архитектурой может быть не только компьютер в бытовом понимании этого слова, поскольку не только он «страдает» от уязвимости универсальной архитектуры. По существу, те же проблемы касаются также являющихся компьютерами, но редко так называемых, служебных носителей: флешнакопителей (или попросту флешек), носителей ключей и пр. Устройства этих типов тоже можно создавать с правильной архитектурой, и уже есть примеры таких серийных продуктов.

2. Служебные носители

Яркий пример технического средства, в отношении которого постоянно ведутся разговоры о непреодолимости «человеческого фактора», это разного рода носители информации. В первую очередь, конечно, флешки. Однако недалеко от них отстоят и, например, токены – ключевые носители, на небрежном отношении пользователей к котором ос-

[2] *То есть такие, защищенный режим работы которых не* ***настраивается****, а* ***включается****.*

новывается большинство попыток вендоров оправдать утечки и потери, произошедшие «под защитой» их устройств.

Невозможно не согласиться с тем, что бороться с человеческим фактором бесполезно. Здесь так же, как и в предыдущем случае, не надо пытаться изменить человека, надо изменить то, что в наших силах – архитектуру «железки». Как и в случае с компьютером, универсальное устройство нужно сделать менее универсальным. Таким, чтобы оно выполняло те функции, которые нужно, на тех компьютерах, на которых можно, и совершенно ничего не выполняло в любых других условиях.

Если предельно обобщить (охватывая все возможные носители сразу), то их стандартная архитектура будет характеризоваться двумя важными для безопасности параметрами – памятью RW (для любых задач) и возможностью работы на любом ПК (универсальный инструмент).

Ограничивать универсальность этих параметров можно и нужно. Эта задача уже решена и решения запатентованы [13, 14].

Рассмотрим более подробно основные типы носителей, наиболее часто применяемые в реальных системах.

2.1. Флэш-накопители

В информационных системах – государственных, частных или личных – данные *хранятся, передаются и обрабатываются*. Средства хранения данных принято называть носителями.

Носители данных в информационной системе (как, впрочем, и средства их обработки) могут быть стационарными и мобильными. Помимо этого носители информации могут быть составной частью оборудования, выполняющего также и *обработку* данных, а могут быть носителями в собственном смысле слова – устройствами, с помощью которых информацию *носят*, и в то время, когда ее носят, она там *хранится*. Затем же, когда информацию *перенесли*, она обрабатывается с помощью какого-либо другого оборудования. И вновь сохраняется на носитель, чтобы быть *перенесенной* куда-то еще.

Являясь частью защищенной информационной системы, носители информации тоже должны быть защищенными.

Защищенность – характеристика объекта, определяющая его способность противостоять атакам. Поэтому тезис о том, что защищенность различных элементов информационных систем обеспечивается разными способами, очевиден: повышает защищенность объекта способность противостоять *именно тем атакам*, осуществление которых *наиболее вероятно* по отношению к данному элементу системы. Спасательный круг существенно повысит защищенность на воде, но оставит ее на прежнем уровне при пожаре или, скажем, морозе.

Что это означает применительно к вопросу защищенности мобильных носителей информации?

Носители информации являются частью информационной системы, следовательно, существенно бóльшая степень их защищенности по отношению к остальным ресурсам системы не имеет смысла (общий уровень защищенности определяется уровнем защищенности самого слабого звена или «дыра в заборе»[3]), так как она никак не усилит общую защищенность данных, и переплачивать за нее нецелесообразно. Нет практического смысла использовать сверхзащищенную флешку в незащищенной системе.

Однако даже для того, чтобы защищенность флешки соответствовала уровню защищенности самого обыкновенного домашнего компьютера, не защищенного ничем, кроме антивируса, эта флешка должна (а) находиться в квартире и нигде кроме, (б) быть каким-то мистическим образом защищена от возможного воздействия вирусов.

Теоретически это достижимо с помощью оргмер. Владелец флешки, которая используется только внутри защищенного помещения для переноса информации между несколькими защищенными от вирусов компьютерами, может быть спокоен – флешка не снижает общей защищенности его системы. К сожалению, такая идеальная с точки зрения безопасности ситуация даже если и возникает, то обычно длится недолго: флешку понадобится куда-то вынести.

Главная особенность мобильных носителей состоит в том, что они подвержены дополнительным угрозам (по отношению к угрозам, актуальным для основной («стационарной») системы), связанным с тем, что контур системы для них проницаем: они могут не только *выноситься* (и выносятся!) за пределы системы, но и *использоваться* там. Как следствие, это приводит к утечкам информации *из* системы и к притоку вредоносного ПО *в* систему.

Именно поэтому проекты защищенных информационных систем зачастую предусматривают полный запрет на использование USB-носителей. Флешки признаются абсолютным злом потому, что они *могут* использоваться *вне* системы. Значит, защищенный носитель – это такой носитель, который может использоваться *только внутри* системы (государственной, корпоративной, личной) и не может использоваться *вне* ее.

Назовем такой носитель служебным.

Служебным является носитель, позволяющий оперативно и просто переносить информацию *внутри системы* согласно ее внутренним правилам, но не позволяющий ни выносить хранимую на нем информацию *из системы*, ни приносить *в систему* информацию, записанную на него *вне системы*. Никому, в том числе и легальному пользователю. Только в этом случае носитель не будет снижать общего уровня защищенности системы даже при его физическом выносе за ее периметр.

Если посмотреть с этой точки зрения на продукты информационной безопасности, позиционируе-

[3] *Ситуация напоминает строительство забора на даче: его делают все выше, а клубнику как воровали, так и воруют. Видимо, где-то есть дыра. В этом случае важнее не наращивать высоту забора, а дыру забить [15].*

мые поставщиками как средства защиты информации на флешках, то выяснится, что при всех своих возможных плюсах необходимую задачу они не решают.

Критерии оценки, которые адекватны понятию «защищенный служебный носитель», следующие:

1) является ли продукт средством хранения и переноса информации (носителем);

2) удобно ли его использование (аппаратные требования, требовательность к навыкам эксплуататора, мобильность, дружественность);

3) снижает ли применение продукта степень негативных последствий кражи или утери носителя с данными для системы;

4) защищает ли продукт данные от доступа посторонних лиц;

5) при использовании вне защищенной системы способен ли продукт предотвратить заражение вредоносным ПО, которое в дальнейшем может попасть в систему;

6) можно ли при помощи продукта защитить данные от хищения мотивированным инсайдером;

7) имеет ли применение продукта нормативные ограничения в РФ;

8) сколько стоит продукт.

Ни одно из представленных до сих пор на рынке средств или решений по защите информации не давало возможности создать систему, включающую в себя защищенные служебные носители, поскольку не было предложено решения главной задачи: ***привязки носителя к системе.***

В ПАК линейки «Секрет» именно эта функция является основной.

Что может предпринять злоумышленник в отношении флешки как носителя информации, включенного в интересующую его систему?

1. Кража или находка.
2. Отъем.
3. Завладение оставленным без присмотра устройством.
4. Завладение устройством путем мошенничества и социальной инженерии.
5. Приобретение у мотивированного инсайдера.

Как правило, пункты 1, 2 и 5 имеют своей целью завладение данными с флешки, а пункты 3 или 4 могут также иметь целью внедрение подложных данных или вредоносного кода (реже, но тоже возможно, – уничтожение данных на флешке).

В отличие от угроз данным в сетях или на локальных компьютерах, которые реализуются весьма разнообразными атаками, угрозы, связанные с флешками, характеризуются очень мощными общими признаками возможных атак: *физическое завладение* устройством и получение доступа к его памяти на *каком-либо* ПК.

Атаки на флешки через сеть, например, весьма маловероятны и будут скорее атаками на *данные на дисках компьютера* (подключаемых), а не на *данные на флешке*. И, в любом случае, вряд ли возможность реализации такого рода угрозы может быть классифицирована как уязвимость флешки.

Очевидно, что защитить маленькое устройство от физической кражи (находки в результате целенаправленного поиска в местах возможных потерь, провокации потери) крайне сложно и практически невозможно сделать это техническими способами. Более того, применение организационных мер в этом случае также крайне затруднительно, поскольку на физическое владение столь маленьким предметом очень сильно влияет характер пользователя – рассеянный он или любит похвалиться, или нечист на руку, или доверчивый…

Значит, задача защиты флешки сводится к тому, чтобы сделать нелегальное физическое обладание ею бессмысленным. То есть, даже имея флешку, получить доступ к данным на ней на не разрешенном явно для этой флешки компьютере или не разрешенному явно пользователю должно быть невозможно. Тогда одинаково бесполезными (или, если смотреть с другой стороны баррикад, не опасными) становятся ее кража (потеря), отъем (передача), покупка (продажа) и т. д.

Для того чтобы флешка работала на одних компьютерах и не работала на других, она должна уметь *различать* компьютеры. Лишь после решения этой задачи можно обсуждать, по каким параметрам различать компьютеры правильно, а по каким нет, или каким образом добиваться изменения списка разрешенных (или запрещенных) компьютеров.

Очевидно, что все эти вопросы важны, но только в том случае, если флешка в *принципе* различает компьютеры. Обыкновенная флешка делать этого не может ввиду того, что у нее просто отсутствуют для этого какие-либо ресурсы. Если говорить упрощенно, флешка состоит из памяти и контроллера USB (рис. 1). Ни то, ни другое не является ресурсом, способным осуществлять произвольные операции.

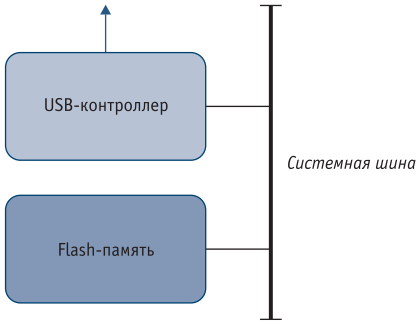

Рис. 1. ***Архитектура флешки***

Компьютер способен различать флешки по их уникальным идентификаторам – VID, PID и серийному номеру, если на нем установлены средства для этого (например, USB-фильтры), потому что у него, в отличие от флешки, есть необходимые вычислительные ресурсы. Стоит иметь в виду, что эти уникальные идентификаторы не всегда и не совсем уникальны (все флешки некоторых производителей имеют один и тот же серийный номер, а с помощью специального технологического ПО эти «уникальные параметры» можно менять). Однако в любом случае для анализирования того или иного признака объекта (флешки ли, компьютера ли) анализирующий должен обладать ресурсами, предназначенными для такого анализа.

Вывод очевиден: чтобы различать компьютеры, флешка должна сама быть компьютером. Именно в этом и состоит отличие служебных носителей (СН) «Секрет», архитектура которых изменена так, как это показано на рис. 2.

Управляющий элемент в различных модификациях СН «Секрет»

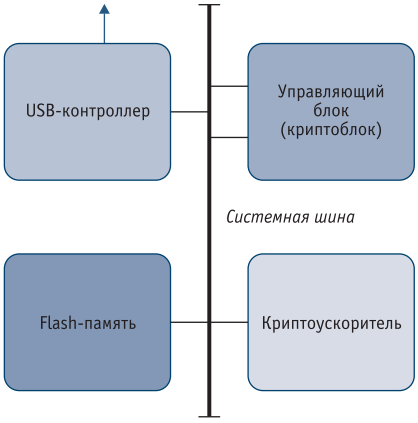

Рис. 2. ***Архитектура СН «Секрет»***

реализован по-разному, однако общая логика остается единой: управляющий элемент «коммутирует» компьютер с диском «Секрета» (собственно флешкой) только после успешного завершения контрольных процедур: взаимной аутентификации СН, компьютера и пользователя. До того, как сценарий аутентификации будет успешно разыгран до конца, диск «Секрета» не будет примонтирован, не появится в списке дисков и не окажется доступен не только для пользователя, но и для системы (с ее потенциальными закладками или вирусами).

Дополнительно защитные свойства «Секрета» могут быть усилены шифрованием данных при записи на диск. Выбирать такой носитель целесообразно, когда разумно предположение, что злоумышленник может попытаться считать данные с флеш-памяти напрямую, например, выпаяв ее из устройства. Однако надо иметь в виду, что ввиду применения аппаратного шифрования заметно снижается скорость чтения/записи, это неизбежные издержки. В СН «Секрет», лишенных функции шифрования, скорость чтения/записи не отличается от показателей обычных флешек.

Такова принципиальная структура и логика защитных свойств *служебного носителя* «Секрет», а *продукты* этой линейки различаются организацией управления процессом взаимной аутентификации компьютера, СН и его пользователя.

2.2. Ключевые носители

Ключи, как и любые другие данные, существуют в трех процессах: хранятся, обрабатываются (в том числе – создаются и уничтожаются) и передаются. Никаких иных состояний у данных, и ключей (как явлений этой сущности) не бывает, но компрометация ключей, как правило, заметно более критична. Поэтому никаких специфических приемов для защиты именно ключей не требуется, просто к обеспечению мер защиты здесь следует подходить тщательнее, чем в отношении прочих данных.

Почему более тщательно – очевидно на уровне здравого смысла. Сравним случай компрометации документа и компрометации ключа. Если скомпрометирован документ, то наступают некоторые негативные последствия. Безусловно, они могут быть весьма существенными, поэтому защищать необходимо отнюдь не только ключи. Но если происходит компрометация ключа (например, ключа ЭП), злоумышленник получает воможность создавать от имени пользователя, чей ключ скомпрометирован, неограниченное количество документов.

К сожалению, здравый смысл не всегда детерминирует безопасное поведение, потому более жесткие требования к защите ключей (хотя вернее было бы сказать – систем с ключом) предъявляются и регуляторами.

В свете требований к средствам электронной подписи (СЭП), в которых взаимоувязаны все три состояния ключа, это приобретает особенную наглядность: мы можем руководствоваться самыми разными соображениями, выбирая тип желательной для нас в тех или иных обстоятельствах ЭП, выбирая подходящее для нас СЭП, но как только мы выбрали усиленную ЭП (то есть ЭП с ключом) мы попадаем в зону действия существенно более высоких требований.

Таким образом, с точки зрения безопасного существования криптографических ключей в автоматизированной системе (АС) принципиальное значение имеют два фактора:

- защищенное хранение ключа (и, соответственно, носитель ключа);
- условия доступа к ключу и работы с ним, то есть среда функционирования криптографии (СФК).

Очевидно и не нуждается в детализации, что второй фактор (условия доступа к ключу) касается и обработки, и передачи ключей как части технологии, реализуемой СКЗИ (СЭП) при выполнении своих функций. В то же время очевидно, что криптография, как правило, является вспомогательным механизмом, а не основной целевой функцией системы, поэтому условно выделяемым третьим фактором можно считать степень влияния средства хранения ключей на информационную инфраструктуру. Естественно, что удорожание и усложнение системы обычно желательно минимизировать, поэтому средство хранения ключей, требующее, например, изменения применяемых в системе протоколов взаимодействия, замены операционных систем и/или внедрения не требующихся ни для чего более средств защиты каналов связи, может считаться удачным решением только для подрядчика, который будет нанят на все эти работы.

Этот раздел посвящен средству хранения ключей (токену), которое позволяет решить несколько более широкий круг задач, чем обычно применяемые в этом качестве устройства, не требуя серьезных инфраструктурных изменений АС. Поэтому назовем его «идеальный токен».

2.2.1. Сложившаяся практика

Сложившаяся практика применения ключей такова, что в качестве их носителей используются универсальные накопители (дискеты, флешки), идентификаторы пользователей, если они представляют собой устройства с доступной для чтения/записи памятью (TM-идентифкаторы) или специализированные устройства (смарт-карты, USB-токены).

Обзор этих видов «хранилищ ключей» (нельзя использовать эту формулировку без кавычек, так как далеко не все эти объекты хотя бы минимально приспособлены к хранению именно ключей) приведен ниже. Из обзора исключены дискеты, так как побочным эффектом развития вычислительной техники, все реже имеющей соответствующие дисководы, стало постепенное отмирание их применения и в этом качестве.

Здесь невозможно снова не вспомнить аксиому о том, что для специальных целей логично применять специализированные средства.

Однако и специализированные средства – токены[4] – не идеальны.

Токены предоставляют возможность использования хранящихся на них ключей и сертификатов после предъявления PIN-кода (авторизации пользователя). Казалось бы, таким образом блокируются все уязвимости, связанные как с хранением, так и с доступом к ключу. Однако очевидно, что ограничение доступа к ключу только применением PIN-кода недостаточно. Токен должен использоваться только в той системе, в которой обеспечена защита от несанкционированного доступа (а именно – доверенная СФК), а PIN-код можно правильно ввести в любой среде. Токен не может определить, в какой системе производится попытка работы с ним, у него нет для этого никаких механизмов. Невозможность расширения функций токена проистекает не из лени программистов, а из ограниченности его архитектуры (рис. 3).

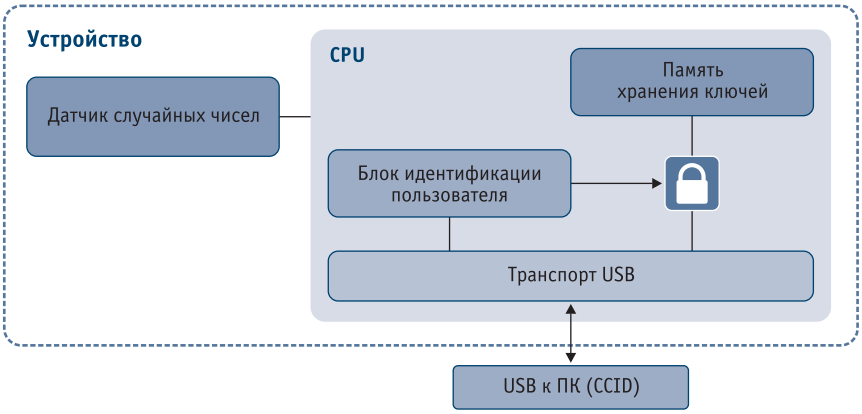

Рис. 3. ***Архитектура токена***

Чем же опасна невозможность контролировать внешнюю среду. Например, в ней могут быть предустановлены программные закладки, предназначенные для перехвата криптографической информации или перехвата управления компьютером. При правильно введенном PIN-коде (а в некоторых случаях и до введения PIN-кода) это вредоносное ПО получит доступ к ключам.

В части доступа к ключу очевидна необходимость учитывать как условия доступа пользователя (человека), так и условия доступа СКЗИ и другого системного и функционального программного обеспечения. При этом необходимо учитывать особенности сред и систем, в которых пользователи выполняют задачи, связанные с криптографическими преобразованиями: работа в различных ОС, загруженных на СВТ различных архитектур из различных источников различными способами, может иметь целый ряд особенностей, существенно влияющих на безопасность ключа.

Отсюда вытекают требования к защищенному ключевому носителю, который в идеальном случае должен быть способен контролировать:

- доступ к ключу *через любые интерфейсы*, в том числе и путем применения разрушающего программного воздействия (РПВ);
- среду, в которой производится попытка доступа к ключу.

Естественно, защищенный ключевой носитель не должен контролировать корректность работы СКЗИ или обеспечивать среду его функционирования (это функция средства доверенной загрузки). Задача «контроля» среды, из которой осуществляется доступ к ключу, сводится к тому, чтобы этот доступ предоставлялся не только исключительно легальному пользователю, но и исключительно на заданных рабочих местах (наличие «правильной» среды на которых обеспечивается в установленном в организации порядке). Принципиально эта задача та же, что и для флеш-накопителей: ограничение числа компьютеров, на которых технически возможна работа с токеном.

В случае реализации такой защитной меры при случайном или преднамеренном подключении токена к неразрешенному (то есть недоверенному) компьютеру устройство не будет примонтировано, значит, ключи не будут доступны ни пользователю (даже легальному), ни системе (с потенциально функционирующими в ней вирусами и закладками). Кроме того, будет исключено несанкционированное использование ключей легальным пользователем токена вне рамок его служебных задач. Это важно, так как само по себе СКЗИ не может определить правомерность формирования данного документа на данном компьютере и подписания его с помощью того или иного ключа.

Вероятность подмены рабочего места выглядит не очень страшно только по одной причине – кажется, что в этом никто особенно не заинтересован (например, трудно представить, что бухгалтер вознамерится осуществить с домашнего ноутбука нелегальный перевод, подписав платежное поручение своей ЭП). Однако на самом деле представить себе сценарий как случайной, так и злонамеренной компрометации ключа и документа несложно. Предположим несколько самых явных.

Начнем с добросовестного бухгалтера (таких, все-таки, мы уверены, большинство). Из лучших побуждений – выполнять часть работы сверхурочно – он может организовать себе дополнительное рабочее место на дому, разделив при этом работы по уровню критичности: для офиса – выполнение платежей, для дома – только подготовку и отправку в налоговую инспекцию отчетов в электронном виде. Последнее реализуется с помощью одной из специальных программ («Фельдъегерь», «Доклайнер», «Контур-Экстерн»), и бухгалтеру на его домаш-

[4] *Это слово используется в разных значениях, но в рамках этой статьи условимся понимать термин «токен» только в одном из них – как защищенное тем или иным способом хранилище ключей в виде объектов PKCS.*

нем компьютере даже не потребуется «Клиент-банк».

Скорее всего, из средств защиты от НСД на этом «дополнительном рабочем месте» будет в лучшем случае только антивирус. Эта ситуация создаст предпосылки для компрометации ключа с помощью широко распространенных вредоносных программ. В случае направленной атаки это позволит злоумышленнику в дальнейшем использовать украденный ключ в своих целях. Если же компьютер используется и для проведения платежей, а не только для подготовки и отправки отчетов, то задача злоумышленника и вовсе упрощается. Всё становится еще хуже, если злоумышленником является сам бухгалтер (надеемся, что не доведем никого до греха).

Итак, если бухгалтер задумал провести нелегальный платеж, что его может остановить? Теоретически, его должна сдержать неотказуемость от ЭП на его ключе. Однако в действительности при наличии технической возможности передачи ключевого носителя другому лицу и одновременно возможности применения ключа на произвольном СВТ, неотказуемость от ЭП – это уже вопрос алиби, а не криптографии.

Сочиним такой «детектив».

Злоумышленник организует рабочее место с необходимым для проведения платежа ПО. На собственном рабочем месте он подготавливает накануне несколько платежных поручений, подписанных его ЭП, но не отправляет их. Вечером токен с ключом ЭП бухгалтер передает сообщнику и договаривается о времени проведения незаконного платежа таким образом, чтобы сам владелец ключа в это время был на рабочем месте на глазах у свидетелей.

В результате, в условленное время злоумышленник находится на виду у будущих свидетелей и отправляет заранее подготовленные платежки со своей легальной ЭП (токен ему для этого не нужен, ведь документы подписаны заранее). В это же время в другом месте с другого компьютера другое физическое лицо (сообщник) подписывает ключом нашего героя другое платежное поручение, используя токен.

Во время разбора инцидента злоумышленный владелец ключа имеет все шансы отказаться от своей электронной подписи, так как находился в это время на собственном рабочем месте и даже отправлял другой документ с подписью на том же ключе, а никаких следов отправки нелегального платежа на его рабочем СВТ нет. Очевидно, что он совершенно не при чем.

Во избежание обвинений в предвзятости к бухгалтерам, приведем пример, никак не связанный с платежами.

Предположим, что злоумышленником движет желание осуществить атаку на корпоративную информационную систему, обрабатывающую информацию ограниченного доступа, что система эта распределенная, централизованная (допустим, система терминального доступа или web-система), что документы обрабатываются на надлежащим образом защищенном сервере, клиентские СВТ не содержат средств обработки информации (тонкие клиенты), загружаются с обеспечением доверенности клиентской ОС, а каналы между клиентами и сервером тоже защищены. Ключи СКЗИ, защищающего канал, хранятся в токене.

Наиболее очевидный в данном случае план действий злоумышленника – это подключение в качестве терминального клиента произвольного СВТ, оснащенного программами для осуществления какой-либо атаки на систему. Если атаку осуществляет легальный пользователь системы, он обладает идентификатором к СЗИ НСД на сервере и токеном с ключами СКЗИ, защищающего канал (зачастую это одно и то же устройство).

Именно таких случаев касается п. 31 Требований к средствам электронной подписи [16]: «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…».

Предотвратить эту атаку может только применение комплексной системы защиты, включающей взаимную аутентификацию клиентского СВТ и сервера. Это не рядовая функция, зачастую относительно сервера аутентифицируется только пользователь.

Все эти леденящие кровь сценарии невозможны, если токен различает СВТ, к которым его подключают.

Итак, защищенный ключевой носитель должен:

1) быть персональным отчуждаемым устройством;

2) быть специализированным именно для хранения ключей устройством, то есть обеспечивать возможность защищенного хранения криптографических ключей с применением интерфейсов работы со смарт-картой (CCID или PKCS#11);

3) предоставлять доступ к ключам только легальному пользователю после успешной аутентификации в устройстве;

4) предоставлять доступ к ключам легальному пользователю только на тех СВТ, на которых ему разрешено работать с данным ключевым носителем.

Функции токена и функцию ограничения числа разрешенных компьютеров объединяет в себе «Идеальный токен» – токен с несколько измененной архитектурой: она включает в себя блок идентификации компьютера, до прохождения проверки которым недоступен в том числе и блок идентификации/аутентификации пользователя (рис. 4).

В «Идеальном токене» у пользователей есть две роли – «Администратор» и собственно «Пользователь». Список компьютеров, на которых разрешена работа с «Идеальным токеном», определяется пользователем с ролью «Администратор», который с точки зрения информационной системы должен быть администратором информационной безопасности или лицом, которому делегированы соответствующие функции.

Для добавления компьютера в перечень разрешенных «Администратор» подключает к нему «Идеальный токен», программное обеспечение токена определяет, а внутреннее программное обеспечение запоминает внутри устройства ряд па-

раметров этого рабочего места. При каждом последующем подключении «Идеальный токен» определяет параметры текущего компьютера и сравнивает с теми данными, которые соответствуют разрешенным рабочим местам. Если они совпадают, разрешается доступ к токену со стороны внешнего ПО, то есть, собственно, со стороны СКЗИ (СКЗИ – это внешнее по отношению к «Идеальному токену» программное обеспечение), в противном случае в доступе отказывается.

Очевидно, что ни одно другое устройство, применяемое для защищенного хранения ключей, не выполняет более трех требований к защищенным ключевым носителям одновременно (см. таблицу). При этом важнейшее требование, касающееся СФК, не выполняется ни одним из них.

«Идеальный токен» является специализированным устройством, которое предназначено именно для хранения ключей СКЗИ и поддерживающим все необходимые для этого интерфейсы. Использование «Идеального токена» возможно только после успешного завершения взаимной аутентификации токена и компьютера, к которому его подключили, а затем – успешной аутентификации пользователя в токене и СКЗИ.

Таким образом, при корректной настройке системы управляющим персоналом исключена возможность сознательной или случайной компрометации ключей из-за подключения к незащищенному компьютеру, на котором могут быть предустановлены программные закладки, предназначенные для перехвата ключей или перехвата управления компьютером. Не менее важно – исключено несанкционированное использование ключей легальным пользователем токена вне рамок его служебных задач, что невозможно предотвратить при использовании обычных токенов, не различающих служебные и любые другие ПК. В то же время «Идеальный токен» лишен каких бы то ни было избыточных функций, негативно влияющих на цену изделия.

Технология «Идеального токена» запатентована [14].

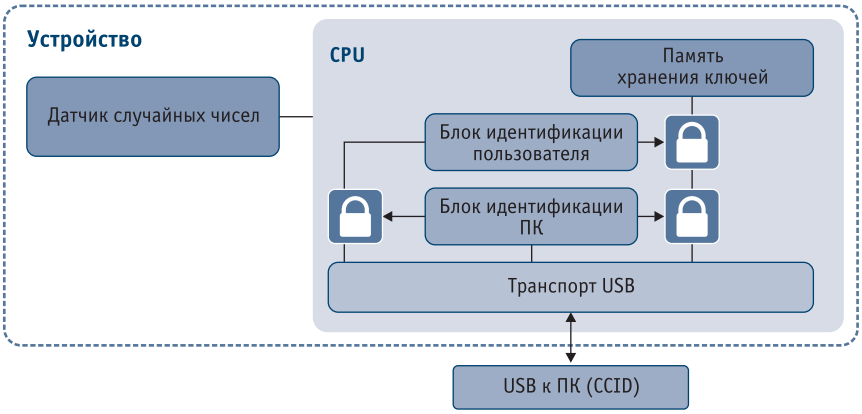

Рис. 4. ***Архитектура «Идеального токена»***

2.2.2. Обзор ключевых хранилищ

Смарт-карты

Смарт-карты обычно обладают весьма скромным объемом памяти данных (десятки килобайт), однако этого достаточно для хранения ключей или сертификатов. Для доступа к данным необходим ввод PIN-кода. Устройство может быть заблокировано после некоторого количества неверных вводов PIN подряд, что делает затруднительным его подбор. Смарт-карты обладают хорошей совместимостью, так как используют стандартный протокол, но для их использования требуется кардридер. Одна из основных проблем смарт-карт – их возможный отказ, так как тонкий пластиковый корпус чипа не может обеспечить надежную защиту при физических воздействиях.

Если злоумышленник завладел и смарт-картой, и ее PIN-кодом, он получит доступ к данным. Владелец смарт-карты технически может (хотя и не должен бы) использовать ее вне доверенной среды, при этом PIN-код может быть перехвачен с устройства ввода, ключи – списаны из оперативной памяти или из памяти смарт-карты после разблокировки хозяином.

Разумеется, хранение ключей – это не единственная функция смарт-карты, но одна из основных.

Токены

Токены зачастую заключают в себе более широкие возможности по сравнению со смарт-картами. Например, устройство может содержать собственную клавиатуру для ввода PIN-кода, что значительно усложняет перехват последнего. Обычно для работы с токеном необходима установка драйверов.

Если злоумышленник завладел и токеном, и необходимым кодом доступа, он сможет получить доступ к данным. Владелец токена технически может (хотя и не должен) использовать его вне доверенной среды, при этом ключи могут быть списаны из оперативной памяти или прямо из устройства после его разблокировки хозяином.

Хранение ключей – это не единственная и не основная функция

Таблица. ***Выполнение различными устройствами требований к защищенным ключевым носителям***

Требование \ Устройство	Смарт-карта	Токен	Флешка	ТМ-идентификатор
Персональное отчуждаемое устройство	+	+	+	+
Поддержка интерфейсов CCID и\или PKCS#11	+	+	–	–
Контроль легальности пользователя*	+	+	–	–
Контроль легальности СВТ	–	–	–	–

* *«+» или «–» в строке «Контроль легальности пользователя» оценивает наличие в ключевом носителе собственных механизмов, независимых от механизмов СКЗИ. То же справедливо и для остальных параметров, однако именно в отношении указанного возможна неоднозначная интерпретация.*

токенов, их основное назначение – двухфакторная аутентификация.

Флэш-накопители

Обычные флэшки не обладают никакой защитой, могут быть украдены или утеряны, в этом случае любой человек способен получить доступ к данным. Зато они обладают значительным объемом памяти, совместимы практически со всеми устройствами, имеющими USB-порты и могут быть использованы на любом АРМ в любых условиях.

Нелепо даже рассматривать вопрос о том, является ли хранение ключей сколь-нибудь специальной функцией флэш-накопителей.

ТМ-идентификаторы

В основном так же, как и флешки, не обладают никакими защитными механизмами, кроме необходимости наличия специального считывающего устройства, впрочем, свободно продаваемого.

Содержимое ТМ-идентификаторов можно копировать, поэтому данные, хранящиеся в устройстве в открытом виде (в том числе и ключи) могут быть легко скомпрометированы.

Основное предназначение ТМ-идентификаторов, как и токенов – двухфакторная аутентификация. Если аутентифицирующей информацией являются не непосредственно хранящиеся в ТМ-идентификаторе данные, а результат преобразования, которое производится резидентным компонентом безопасности с данными, полученными по разным каналам, то копируемость памяти ТМ-идентификатора не является критичным фактором. В отличие от считывания хранящихся в «таблетке» в открытом виде ключей.

2.3. Другие служебные носители

По принципу, впервые реализованному в служебных носителях «Секрет», кроме «Идеального токена» построены и другие служебные носители для различных более узких целей. Например, это программно-аппаратный неперезаписываемый журнал ПАЖ, где свойства «Секрета» дополнены тем, что память, в которой сохраняются журналы событий различных устройств и приложений – Add only, то есть в нее можно только добавлять, а что-либо удалять или изменять в ней нельзя. Также ПАЖ характеризуют некоторые особенности реализации ролей пользователей, связанные с особенностями работы именно с журналами, но они не касаются архитектуры и являются, в общем-то, частными деталями.

Еще один пример – мобильный генератор лицензий – устройство, позволяющее распространять лицензии на программное обеспечение, избегая основных типов проблем, с которыми сталкиваются при этом вендоры ПО.

Более того, решений такого рода может быть очень много, потому что базовый принцип – изменение архитектуры как способ решения проблем с нею – является научным, а значит, экспериментально подтверждаемым и воспроизводимым.

Заключение

В заключение представляется необходимым попытаться сформулировать ответ на вопрос: как же, собственно, лучше поступать – менять архитектуру универсального устройства с помощью РКБ или применять устройства с «правильной» с точки зрения безопасности архитектурой? Вопрос, чем-то напоминающий извечное «кто кого победит – кит или слон?». Если все хорошо, то никто никого не победит, потому что они не встретятся. Если же встретятся, то либо кит оказался в саванне, либо слон в океане, что одинаково плохо. Нельзя такого допустить. Так и с защитой информации: для решения разных задач объективно нужны разные СВТ, и заменять уместное на идеологически правильное – нецелесообразно и даже вредно. А вот определить на этапе проектирования ли, модернизации ли, какие рабочие места рационально применять в той или иной системе – универсальные или специализированные – довольно несложно и точно полезно. ■

ЛИТЕРАТУРА

1. *Конявский В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией. – Мн.: Серия «Библиотека журнала „УЗИ“». – 2004. – 327 с.*
2. *Википедия. Машина Тьюринга [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Машина_Тьюринга/.*
3. *Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь. – 1999. – 325 с.*
4. *Конявский В. А., Лопаткин С. В. Компьютерная преступность. Т. I, II. – М.: 2006, 2008. – 560 с., 840 с.*
5. *Конявский В. А. Иммунитет как результат эволюции ЭВМ // Защита информации. Инсайд. – 2017. – № 4. – С. 46–52.*
6. *Конявский В. А. Безопасное «облако» // Федеральный справочник. Связь и массовые коммуникации в России: [информационно-аналитическое издание]; Т. 12. – М.: НП «Центр стратегического партнерства». – 2012. – С. 325–330.*
7. *Счастный Д. Ю., Конявская С. В. Облако ЦОДов, или Сон разума: о том, почему необходимо мыть руки перед едой, даже если они «чистые» // Защита информации. Инсайд. – 2014. – № 5. – С. 57–61.*
8. *Конявская С. В. Защита терминальных клиентов в идеологии «клиент всегда прав» // Information Security/Информационная безопасность. – 2016. – № 5. – С. 35.*
9. *Конявская С. В. К вопросу о классификации объектов защиты информации // Безопасность информационных технологий. – 2013. – № 3. – С. 14–18.*
10. *Trusted Cloud Computers [Электронный ресурс]. – Режим доступа: http://www.trustedcloudcomputers.ru/.*
11. *Конявский В. А. Защищенный микрокомпьютер МК-TRUST – новое решение для ДБО // Национальный банковский журнал. – 2014. – № 3.*
12. *Конявская С. В. Применение защищенных микрокомпьютеров МКТ-card long в системах удаленного доступа смешанного типа // Вопросы защиты информации. – 2016. – Вып. 3, № 114. – С. 23–30.*
13. *Специальный съемный носитель информации // Патент России на полезную модель № 94751. 2010. Бюл. № 15.*
14. *Съемный носитель ключевой и конфиденциальной информации. Патент России на полезную модель № 147529. 2014. Бюл. 31.*
15. *Конявский В. А. Научно-методические проблемы создания защищенных информационных технологий // ВККС Connect! – 2006. – № 1 (34). – С. 41–43.*
16. *Требования к средствам электронной подписи (Приложение № 1 к приказу ФСБ России от 27 декабря 2011 года № 796).*