

импортозамещение: идеология и логика

ТЕКСТ

Светлана Конявская, зам. генерального директора ЗАО «ОКБ САПР», к. ф. н.



Вообще говоря, почти все люди за хорошее и против плохого. И в этом смысле импортозамещение как процесс, направленный на ослабление технологической зависимости от других стран, развитие собственной промышленности и за счет этого повышение уровня национальной безопасности, вряд ли может кому-то не нравиться.

Однако дело портит вопрос, почему и кто конкретно имеет моральное обязательство оплачивать плохие копии и наклеивание шильдиков. В целом понятно, кто и почему: замена лучшего на худшее призвана создать условия для развития собственной промышленности. К счастью, это не единственный вариант. Замена избыточного на соответствующее – нормальная экономическая позиция. Зачем покупать огромные вычислительные мощности, когда можно обойтись на порядок меньшими?

И наконец, идеальный вариант – замена худшего на лучшее – безупречная позиция, за которую не требуется никого дополнительно агитировать.

Если отделить логику от идеологии (зерна от плевел, а мух от котлет), то становится довольно легко выявить те точки, где импортозамещение не только стратегически полезно стране, но и экономически выгодно банку прямо сейчас.

Именно сейчас, с созданием новой гарвардской архитектуры, специализированные автоматизированные рабочие места (АРМ) на базе защищенных микрокомпьютеров этой архитектуры становятся той самой не номинальной, а вполне рациональной, в том числе и с экономической точки зрения, отечественной альтернативой универсальному настольному импортному (хорошему!) ПК. При этом они имеют вирусный иммунитет – не заражаются вирусами, что позволяет перевести их внедрение из категории «замена избыточного на соответствующее» в категорию «замена худшего на лучшее».

Вот несколько примеров защищенных АРМ на базе микрокомпьютеров линейки МКТ, которые банк может эффективно применять, не занимаясь адаптацией решения под свои нужды.



Рисунок 1.
Компьютер MKT-card long

КОМПЬЮТЕРЫ

МКТ-card long на базе новой гарвардской архитектуры (рис. 1).

1. Имеют вирусный иммунитет.
2. Работают в защищенном режиме локально и в сетях, в «облаках» под VMware, Hyper-V, KVM и Parallels, в терминальном режиме и режиме веб-доступа.
3. Работают с сертифицированными средствами криптографической защиты информации (СКЗИ).
4. В 10-15 раз дешевле обычного компьютера на базе x86.
5. Платите за то, что вам действительно нужно! Не платите за возможность играть в сетевые игры и невозможность защититься, если вам нужно рабочее место для фронт- или бэк-офиса.



Рисунок 2.
Планшет TrusTPad

ПЛАНШЕТЫ

TrusTPad: защищенный и обычный планшеты в одном корпусе (рис. 2).

1. Переключение между защищенным и обычным режимом физическим переключателем, каналы утечки данных блокированы.
2. Интернет-серфинг без ограничений + защищенные сервисы.
3. Мобильный доступ к защищенной информационной системе.
4. Вирусный иммунитет.
5. Платите за один, получаете два в одном.

ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ (ДБО)

МКТ на базе новой гарвардской архитектуры (рис. 3).


1. Всего 7-8 тыс. рублей, и клиент банка живет без забот.

Рисунок 3.
Микрокомпьютер МКТ



2. One-touch security – клиент своими действиями не может снизить ни защиту банка, ни свою безопасность.
3. Вирусный иммунитет.
4. Защищенность как новая услуга банка для клиентов.
5. Защищенность как эффективный бизнес-аксессуар для клиента.

В заключение сформулируем еще одну не всегда оцениваемую по достоинству при принятии решения о покупке

особенность действительно отечественных разработок – мы предлагаем не универсальный компьютер с некоторым набором ресурсов и потенциальных возможностей, который каждый должен использовать, как сможет, а готовое АРМ, разработанное и настроенное специально для той функции, в которой оно будет применяться, именно в той системе, для которой его заказывают. А диалог с разработчиком намного удобнее вести на одном языке. 

ГЛАВНОЕ СОБЫТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ



infosecurity

RUSSIA

Деловая программа

Информационная безопасность критически важных объектов
 Защита от современных угроз и целенаправленных атак
 Противодействие мошенничеству
 Карты: Платежи. Идентификация. Мобильность
 Информационная безопасность на предприятиях ритейла
 Современные подходы к обеспечению ИБ в банковской сфере
 Интернет вещей и информационная безопасность
 Безопасность виртуальной среды

Реклама

Прием заявок на участие открыт:
www.infosecurityrussia.ru

19–21
 сентября
 2017

Groteck
 Business Media