



Технологии  
информационной  
безопасности  
Решения и услуги

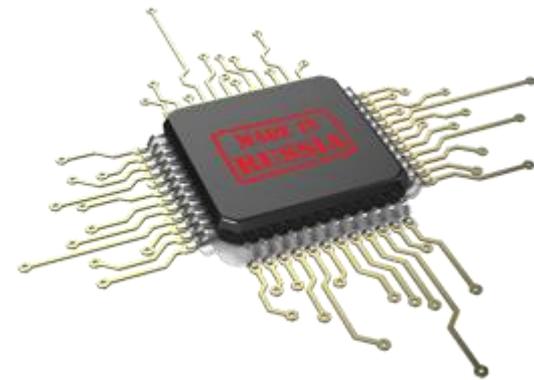
## Развитие безопасных технологий в России в условиях курса на импортозамещение

Сергей Вихорев,  
Роман Кобцев

- ✓ Проблема импортозамещения в ИТ-сфере
- ✓ Риски и угрозы импортозамещения
- ✓ Пути нейтрализации угроз
- ✓ «Гибридное импортозамещение» - реальный путь

Итог дискуссий 2014 года:

Обеспечить **100%** импортозамещение в России в сфере ИТ **сегодня** (и в короткой перспективе) невозможно.



Минпромторг о доле импорта в потреблении в России:

- станкостроение (по разным оценкам более 90%);
- тяжелое машиностроение (60-80%);
- легкая промышленность (70-90%);
- **электронная промышленность (80-90%);**
- фармацевтическая, медицинская промышленность (70-80%);
- машиностроение для пищевой промышленности (60-80%).

Из интервью Сергея Цыбы, заместителя министра промышленности и торговли РФ  
Российской газете 05.08.2014

Минпромторг о доле импорта в потреблении в России:

В случае реализации продуманной политики импортозамещения **к 2020 году** можно рассчитывать на снижение импортозависимости по разным отраслям промышленности с уровня 70-90% до уровня **50-60%**.

Из интервью Сергея Цыбы, заместителя министра промышленности и торговли РФ  
Российской газете 05.08.2014

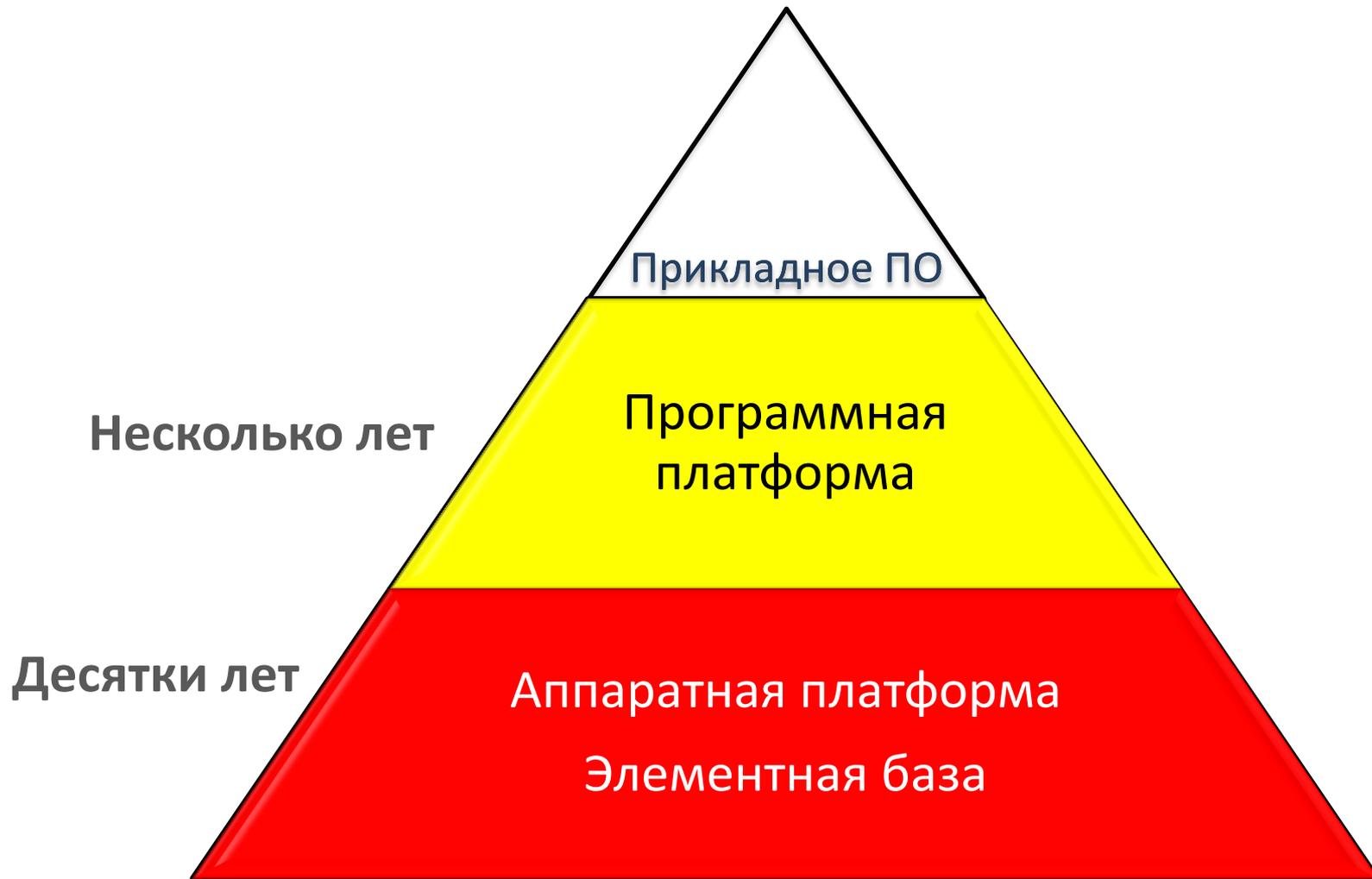
## Проблема импортозамещения в ИТ-сфере



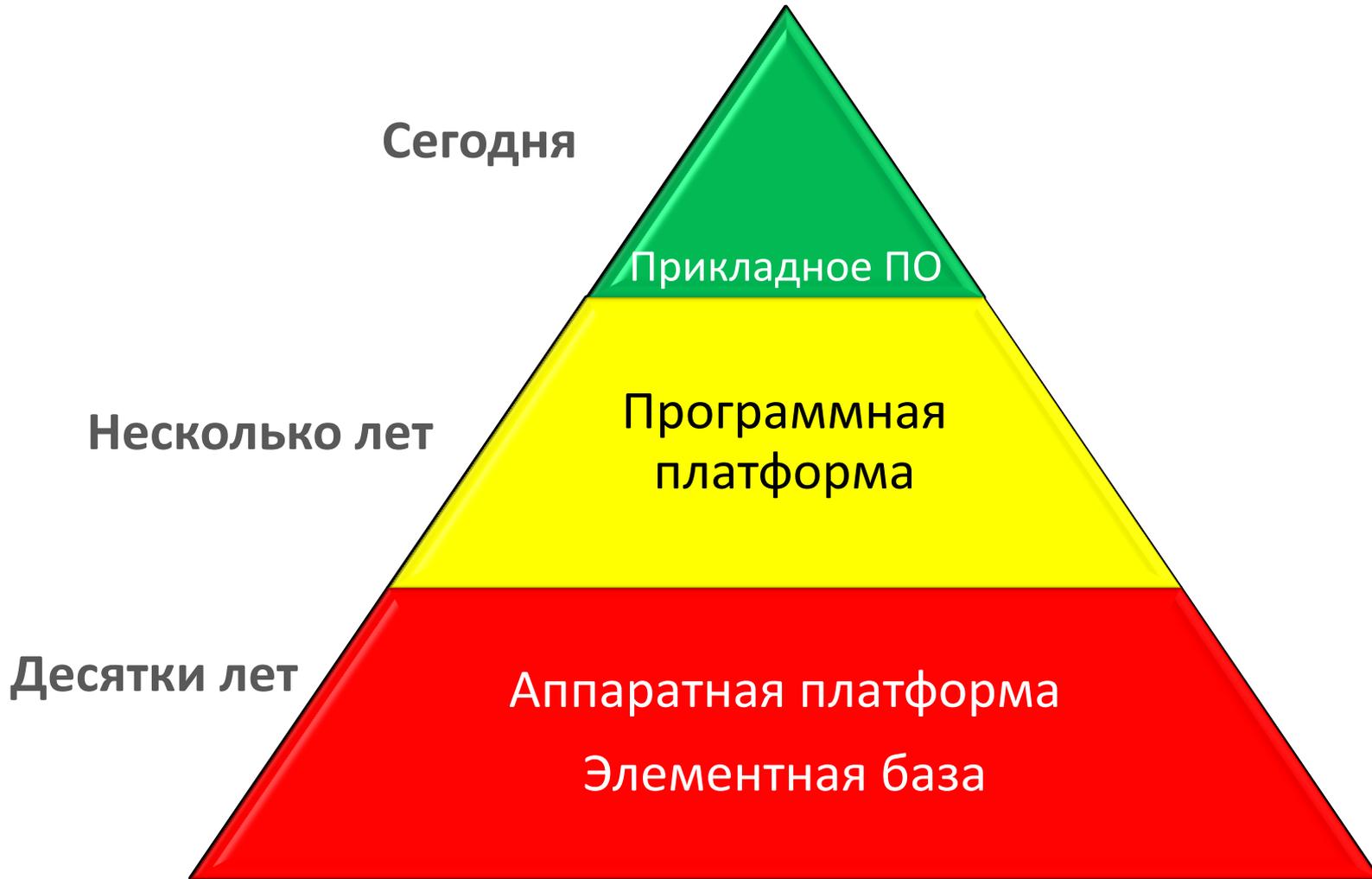
## Проблема импортозамещения в ИТ-сфере



# Проблема импортозамещения в ИТ-сфере



# Проблема импортозамещения в ИТ-сфере



ВЫВОД:

Ближайшие несколько лет мы будем **вынуждены** продолжать строить (поддерживать) инфраструктуру с использованием зарубежных технологий.

**Какие риски?**



# Риски и угрозы импортозамещения



# Импортозамещение в сфере ИТ с целью снижения экономических рисков

## Мотивирующие факторы

### Снижение ВВП

Только объем лицензионных отчислений за рубеж крупнейших иностранных вендоров в России оценивается экспертами в сумму порядка 300 млрд руб., что составляет более 40% общего объема российского рынка ИТ\*

\*По данным ассоциации НАИРИТ

## Ограничения

### Требует огромных государственных инвестиций (время/деньги/кадры)

Доля информационных технологий в ВВП страны будет оставаться на уровне **1-1,3%\***

\*По данным АПКИТ и McKinsey & Company

Масштабная поддержка импортозамещения ИТ-технологий для снижения экономических рисков имеет больше ограничений, чем мотивирующих факторов.





Отрасль информационных технологий не вошла в список отраслей, нуждающихся в государственной поддержке с целью наладить отечественное производство ныне импортируемой продукции.

Источник: РБК 20.01.2015, 21:26  
<http://top.rbc.ru/economics/20/01/2015/54be941b9a79473ac2a44d29>

Импортозамещение в сфере ИТ с целью снижения рисков реализации угроз безопасности инфраструктуре и безопасности информации

### Мотивирующие факторы

Утечки госсекретов

Нарушение работы КВО

Нарушение работы ГИС

### Ограничения

Требует огромных государственных инвестиций (время/деньги/кадры)

100%  
импортозамещение



Если 100% импортозамещение невозможно сегодня, то  
что делать?



## Риски и угрозы импортозамещения



Развитие в российской промышленности процессов импортозамещения не означает сворачивание кооперационных и интеграционных направлений, которые позволяют сконцентрироваться на наиболее перспективных направлениях, рационально построить схемы ресурсобеспечения.

*Валерий Платонов,  
Председатель Комитета ТПП РФ по  
промышленному развитию*

Из заявления на расширенном заседании Комитета 21 мая 2014г. Цитата с официального сайта trprf.ru

## Еще раз об источниках угроз

### Санкции

Запрет на поставки в Россию технологий зарубежных производителей, а также прекращение поддержки уже внедрённых продуктов

Угрозы  
инфраструктуре

Угрозы  
информации

### Закладки

Возможное наличие в иностранных технологиях умышленных аппаратных или программных уязвимостей (логических бомб, backdoors и др.)

## Борьба с санкциями

### Формирование стратегии импортозамещения

Необходимо не только определить наиболее критичные направления импортозамещения и форсировать развитие российских технологий, но на сегодняшний день необходимо от стратегии запрета сдвинуться в сторону обеспечения необходимого уровня доверия и контроля.

## Борьба с санкциями

### Обеспечение необходимого уровня доверия

Категорирование зарубежных производителей «по степени доверия» и формирование списка стратегических технологических поставщиков в РФ

Переход на использование оборудования иностранных производителей, не связанных обязательствами по введению санкций и ограничений (Китай, Индия, Корея, Сингапур, и пр.)

## Борьба с санкциями

### «Противопожарный план»

Подготовка на крайний случай резервных логистических схем и плана действий на случай «жестких условий», включающего в себя все возможные меры, включая «неджентльменские» (к примеру «китайский путь»)

## Борьба с Закладками

### Обеспечение необходимого уровня доверия

Категорирование зарубежных производителей «по степени доверия» и формирование списка стратегических технологических поставщиков в РФ

Внедрение средств мониторинга процесса обработки информации, позволяющих выявить аномальную активность и нестандартные обращения к командам управления, в том числе и по каналам техподдержки

## Борьба с Закладками

### Обеспечение необходимого уровня доверия

Усиление контроля над технологиями, внимание анализу исходных кодов, более глубокое изучение архитектуры.

Использование средств, прошедших сертификацию и имеющих высокий уровень доверия (ОУД) согласно ГОСТ ИСО/МЭК 15408

## Борьба с Закладками

### «Противопожарный план»

Подготовка плана действий на случай «жестких условий», включающего в себя все возможные меры (в том числе полное отключение от сети, возможность перехода на «ручное» управление и др.)

### Обеспечение необходимого уровня доверия через «гибридное импортозамещение»

При невозможности замены всей технологии на российскую, разработка и внедрение отечественных технологий, обеспечивающих контроль над исполнением критичных функций безопасности, реализуемых зарубежными продуктами, частичный отказ от использования отдельных функций зарубежных продуктов и дублирование отечественными продуктами для замещения этих функций.

## Обеспечение необходимого уровня доверия

Наиболее известный пример сегодня – замена зарубежной криптографии на отечественную.

Примеры – решения компаний  
Аладдин Р.Д., ЭЛВИС-ПЛЮС, С-Терра СиЭсПи



## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

### Задача

Создание решения для работы с конфиденциальной информацией на мобильной платформе (ультрабук, планшет, смартфон) с физическим разделением доверенной и недоверенной сред на одном устройстве и обеспечение всей цепочки доверия, начиная от загрузки.



## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

На одном мобильном компьютере должны быть одновременно **две среды** – доверенная и недоверенная, **физически разделенные** и никогда не пересекающиеся между собой.





## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

На одном мобильном компьютере должны быть одновременно **две среды** – доверенная и недоверенная, **физически разделенные** и никогда не пересекающиеся между собой.

Недоверенная система



Доверенная система





## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль



Полное шифрование всех  
файлов доверенной ОС

Контроль загрузки доверенной  
ОС с первых тактов работы  
процессора

Надежное хранение ключей на  
аппаратном уровне



## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

### Проблемы с ультрабуками и планшетами:

- Невозможность использования возможностей встроенной системы безопасности из-за западной криптографии;
- Отсутствие встроенного аппаратного корня доверия (чипов безопасности) российского производства;
- Невозможность использования в мобильных компьютерах наложенных АМДЗ и электронных замков (отсутствуют шины mini PCI и т.п.).



## «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль



**Отечественное ПО**

Аппаратная платформа  
с учетом снижения  
рисков санкций

Аппаратный корень  
доверия используется  
только для функции  
аутентификации,  
остальные функции не  
используются

Остальные функции  
безопасности реализует  
специальное отечественное  
ПО, которое использует  
ГОСТ 28147-89



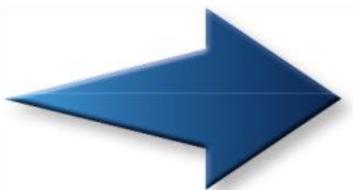
# «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

## Базовый режим работы

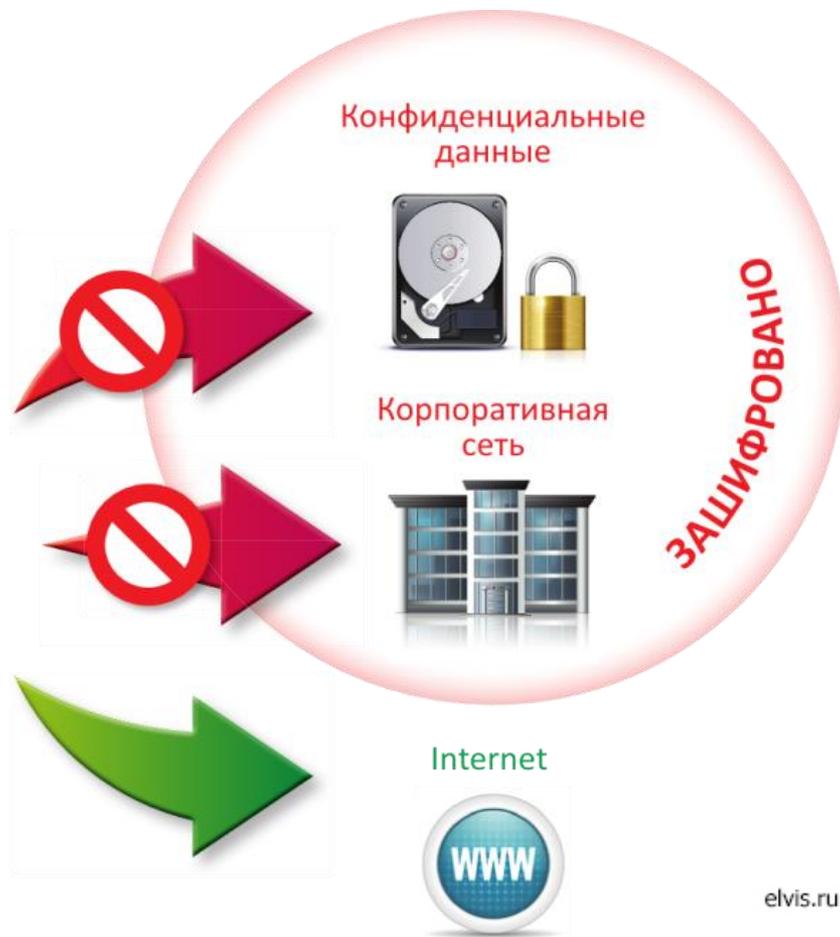
Встроенный чип безопасности



Загрузка базовой ОС.  
Конфиденциальные  
данные зашифрованы



Недоверенная  
среда





# «Гибридное импортозамещение» на примере технологии Базовый Доверенный Модуль

## Доверенный режим работы



A woman with long, wavy brown hair is looking down at a laptop in a server room. The room is filled with server racks and cables. The text is overlaid on the left side of the image.

Технологии  
информационной  
безопасности  
Решения и услуги

Ваши вопросы?