Взгляд российского разработчика на рынок ИБ в государственном секторе

СЕРГЕЙ КУЗНЕЦОВ

КОММЕРЧЕСКИЙ ДИРЕКТОР,
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

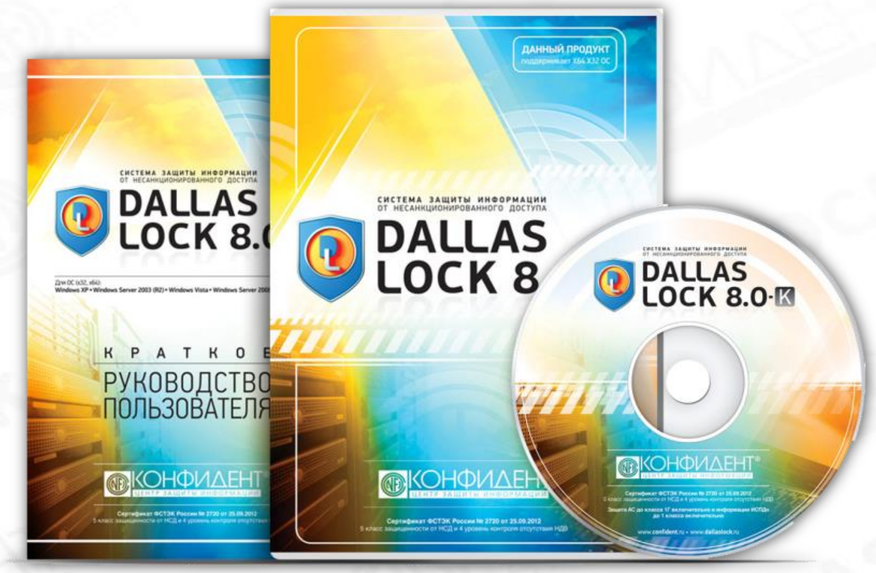
E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Кратко о ГК «Конфидент»

…в 2017 году у нас юбилей

Кратко о продуктовой линейке DALLAS LOCK

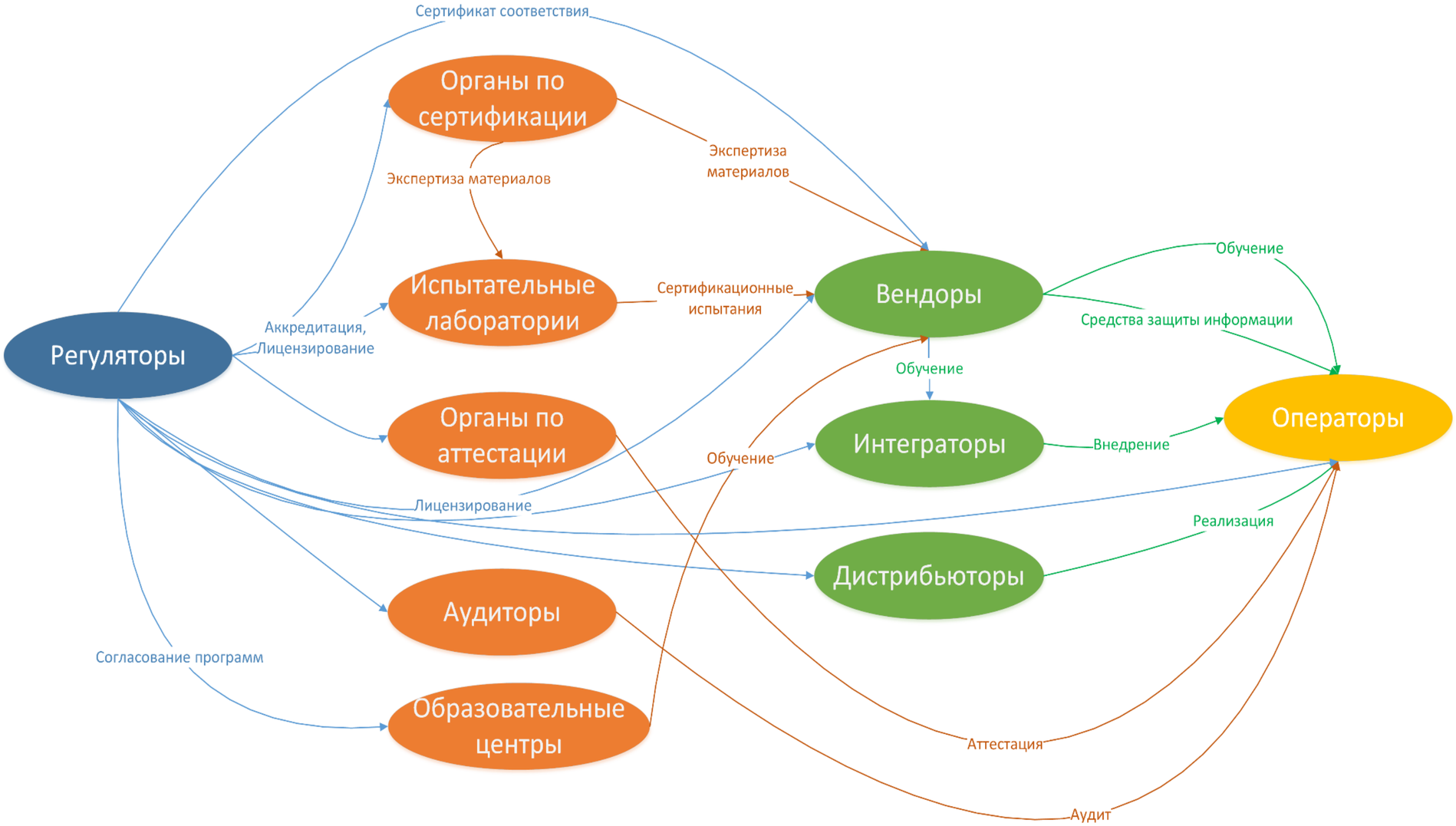


Каждые 36 минут

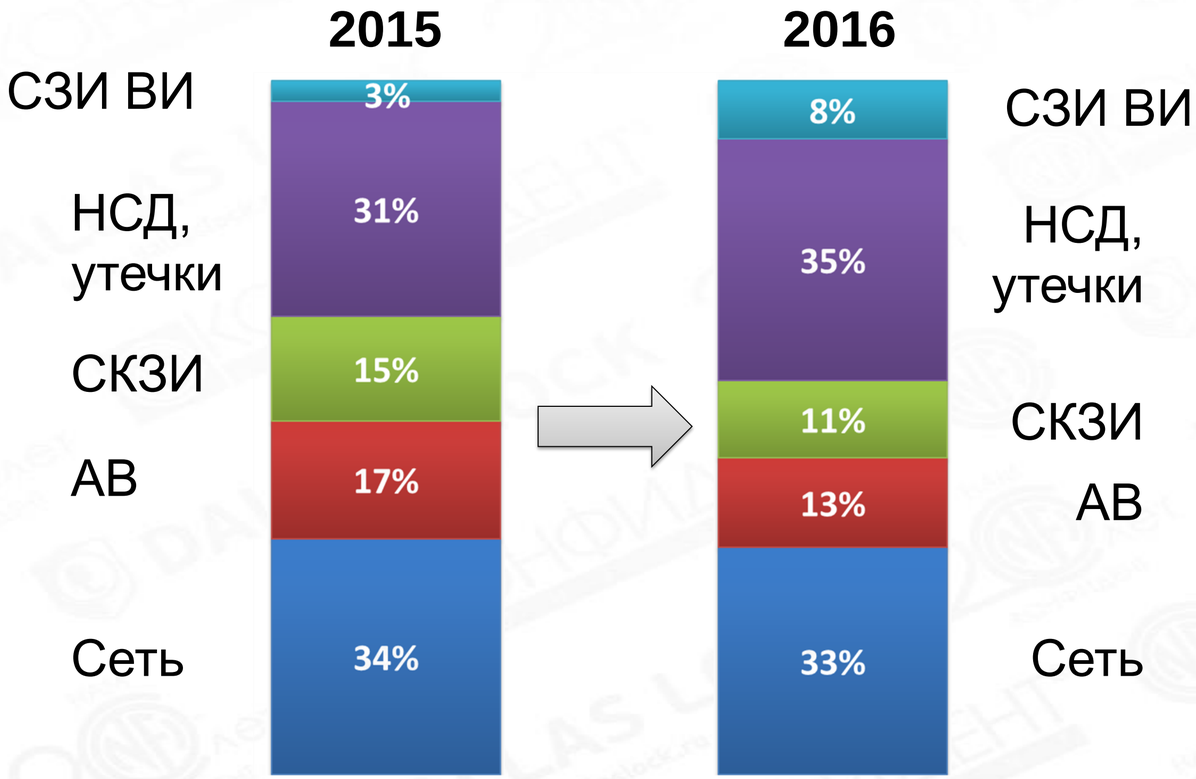
в России реализуется проект с использованием продуктов Dallas Lock

Рынок ИБ в России

Рынок ИБ в России весьма запутан



Основные СЗИ и их доля в общей ИБ-инфраструктуре*



* 1. Без учета MDM, IAM, CA3, WCF, SIEM.
2. Сегмент «Сеть» включает МЭ, СОВ, VPN (для корпоративного сегмента поставляются единым продуктом – UTM), а также UTM.
3. Сегмент «НСД, утечки» включает СЗИ НСД, СДЗ, DLP, Endpoint.

Основные тенденции на рынке ИБ. Регуляторы

Совет безопасности РФ. Доктрина информационной безопасности РФ

Особенности, нововведения:

- Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры
- Рост влияния внешних угроз
- Расширение списка участников системы обеспечения ИБ

Основные тенденции на рынке ИБ. Регуляторы

ФСТЭК России

ФСБ России

Роскомнадзор

Минкомсвязи России

Банк России

Министерство обороны РФ

Основные тенденции на рынке ИБ. Регуляторы

ФСТЭК России

Есть

- Приказ № 21 (ПДн)
- Приказ № 17 (ГИС), Меры ГИС
- Приказ № 31 (АСУ ТП)
- Требования к СОВ, САВЗ, СДЗ, СКН, МЭ, ОС
- Банк данных угроз, уязвимостей
- Безопасная разработка ПО

В планах 2017 – 2018

- Новая редакция Приказа № 17
- Требования к СУБД, BIOS, DLP, средствам управления потоками информации
- Методические документы АСУ ТП/КВО/КСИИ
- Обновление СЗИ
- Методика моделирования угроз

Основные тенденции на рынке ИБ. Регуляторы

ФСБ России

Есть

- Приказ № 378 (использование СКЗИ для защиты ПДн)
- Приказ № 432 (предоставление информации для декодирования эл. сообщений в Интернет)
- Принципы разработки и модернизации СКЗИ (ТК26)

В планах 2017 – 2018

- Приказ о национальном CERT
- Серия документов о СОПКА

Основные тенденции на рынке ИБ. Регуляторы

Минкомсвязь России

Есть

- ФЗ № 242 (хранение ПДн)
- Приказ № 96 (импортозамещение)
- Реестр российского ПО
- План перехода на российское офисное ПО (РП-1588-р)

В планах 2017 – 2018

- Реестр российского IT-оборудования

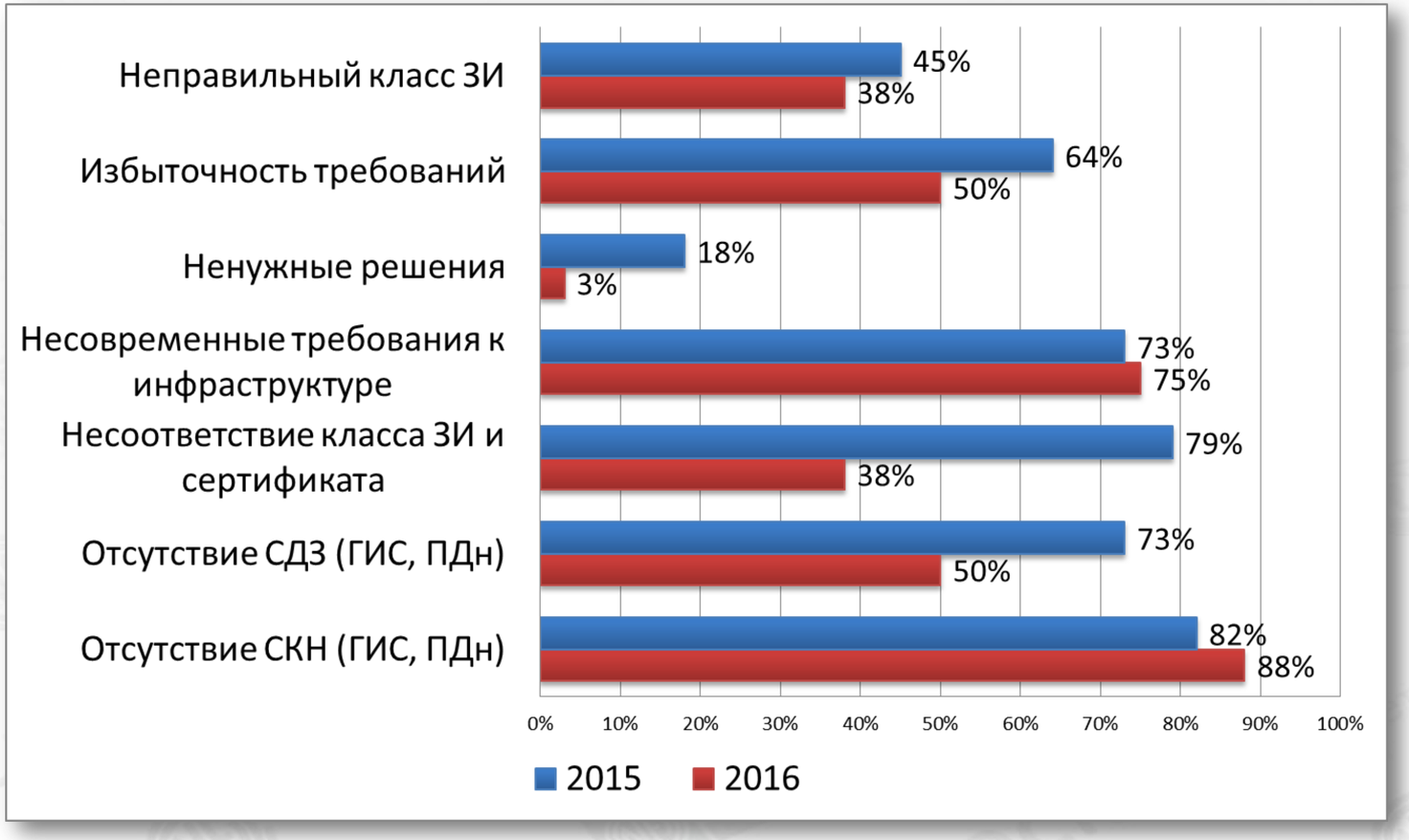
Сертифицированные СЗИ

Миф

«раз есть требования,
то они соблюдаются»

Сертифицированные СЗИ

Основные неточности в конкурсной документации 2016*



* Статистика по результатам анализа специалистами ЦЗИ ГК «Конфидент» требований к конкурсной документации (портал Госзакупок).

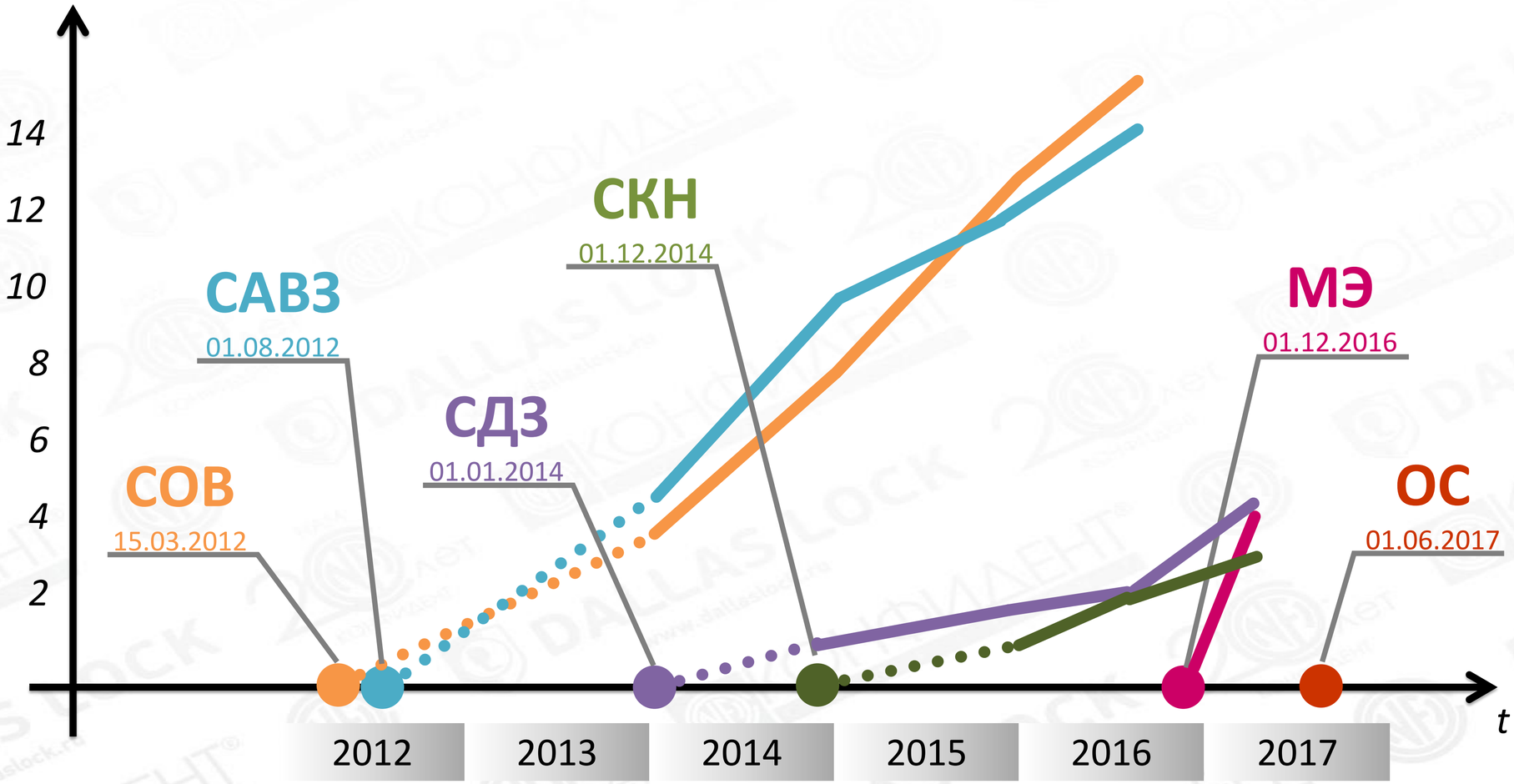
Сертифицированные СЗИ

Миф

«сертифицированные СЗИ защищают только от Регулятора»

Сертифицированные СЗИ

Выпуск сертифицированных решений



Сертифицированные СЗИ

Как проводятся испытания и проверки

- Разработчик
- Испытательная лаборатория
- Орган по сертификации
- ФСТЭК России
- Орган по аттестации
- Оператор
- ФСТЭК России

сертифицированные СЗИ

- Разработчик
- Оператор

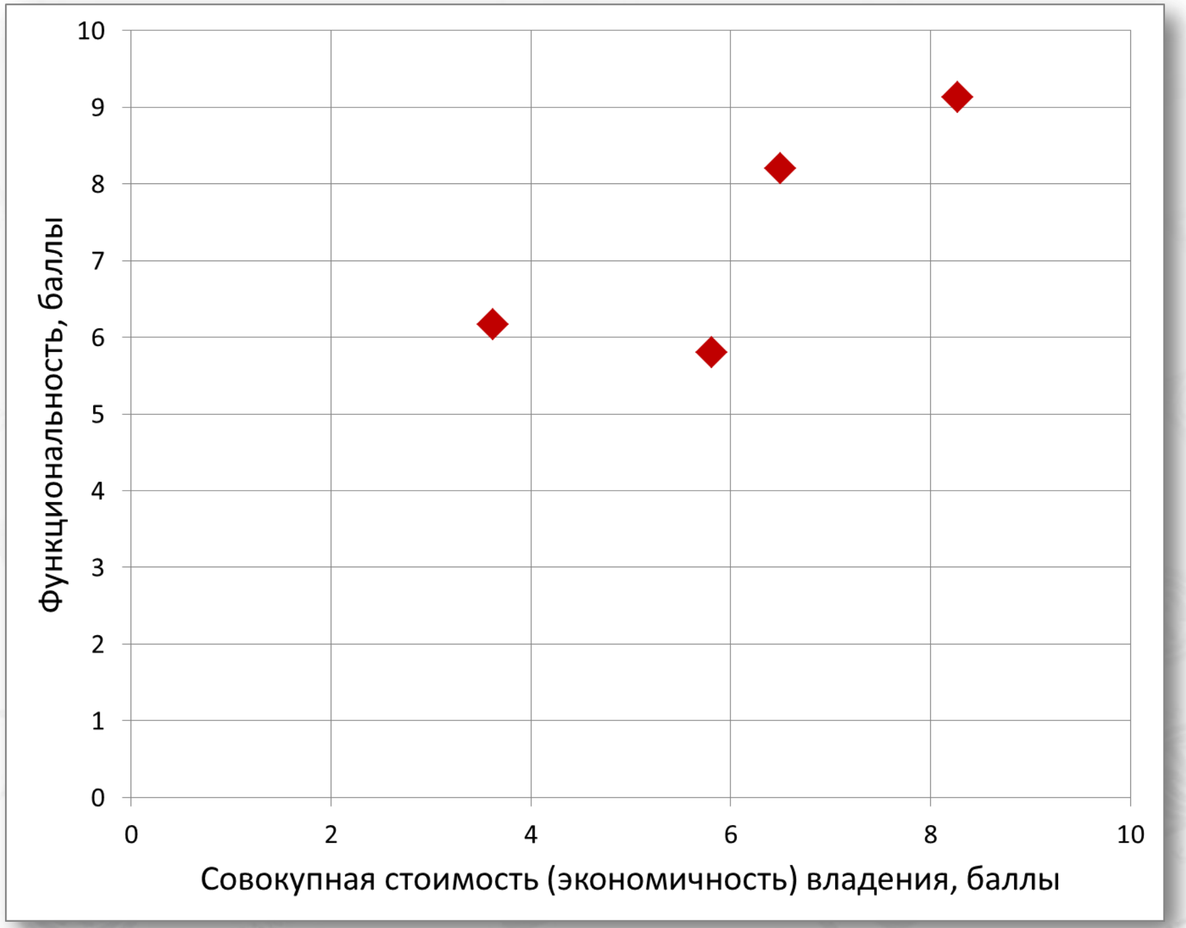
не сертифицированные СЗИ

Сертифицированные СЗИ

Миф

«все сертифицированные СЗИ одинаковы»

Субъективное мнение потребителей* о некоторых СЗИ



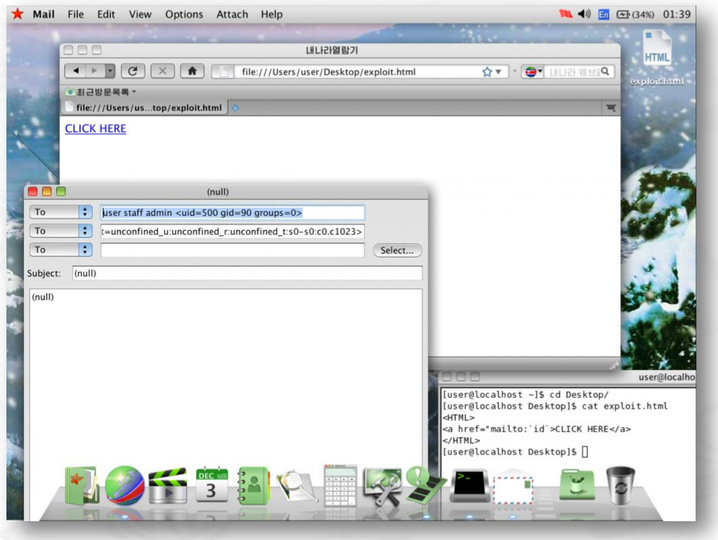
* Результаты опроса партнёров ЦЗИ ГК «Конфидент».

Импортозамещение

Миф

«российское ПО
на базе свободного ПО
безопасно»

Уязвимость в северокорейской ОС



Red Star представляет собой операционную систему на базе ядра Linux, разработанную и используемую в КНДР.
Эксперты обнаружили **ряд уязвимостей, позволяющих получить на системе права суперпользователя**, и в годовщину утечки Red Star раскрыли подробности об уязвимости, с помощью которой **можно удаленно внедрить произвольные команды**.

Источник: http://www.securitylab.ru/news/484636.php

Статистика уязвимостей CVE Details за 2016 год

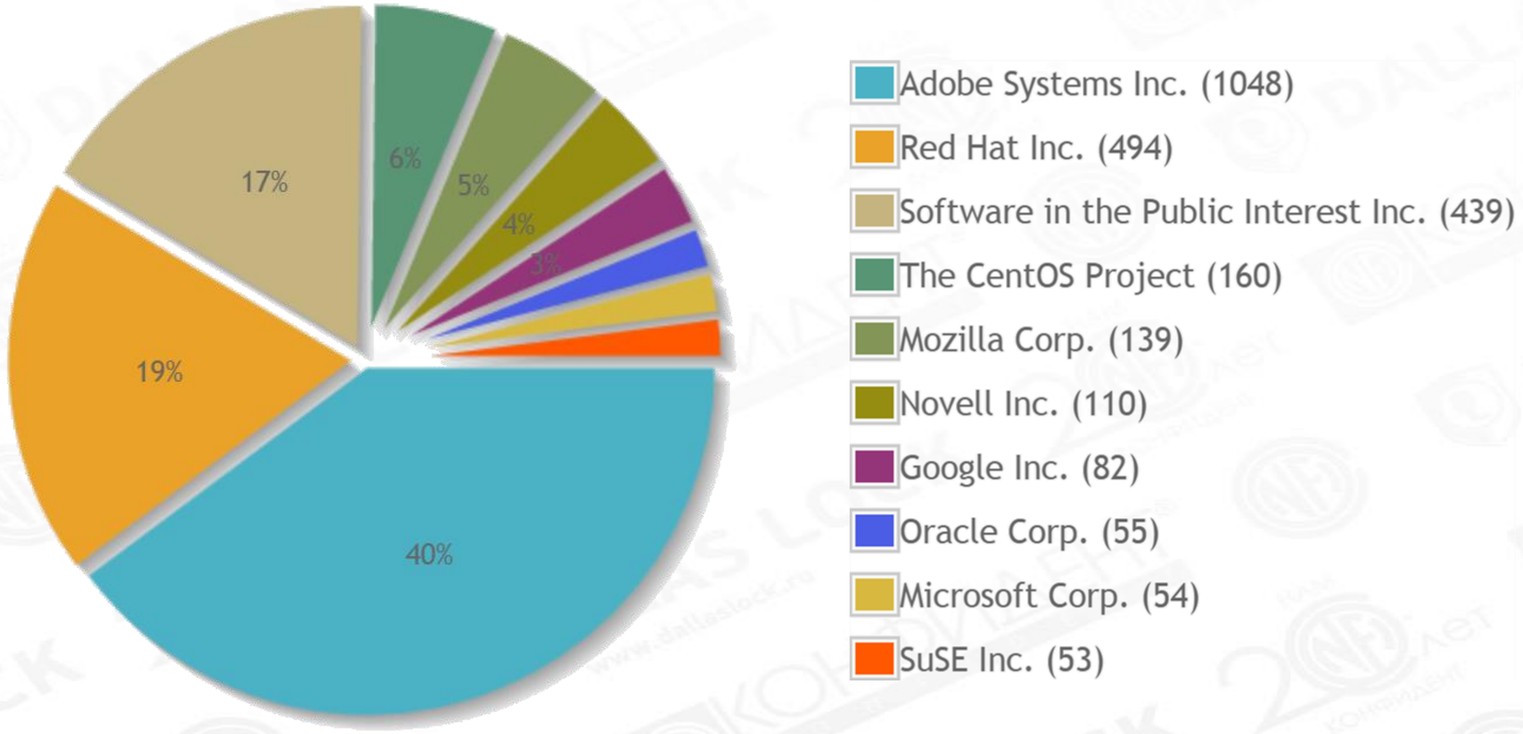
Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2016

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	523
2	Debian Linux	Debian	OS	319
3	Ubuntu Linux	Canonical	OS	278
4	Flash Player	Adobe	Application	266
5	Leap	Novell	OS	259
6	Opensuse	Novell	OS	228
7	Acrobat Reader Dc	Adobe	Application	227
8	Acrobat Dc	Adobe	Application	227
9	Acrobat	Adobe	Application	224
10	Linux Kernel	Linux	OS	217
11	Mac Os X	Apple	OS	215
12	Reader	Adobe	Application	204
13	Chrome	Google	Application	172
14	Windows 10	Microsoft	OS	172

Источник: http://safe.cnews.ru/news/top/2017-01-09_sistemy_windows_okazalis_naimenee_dyryavymi

Количество критических уязвимостей в ПО различных производителей



Источник: Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/charts)

Импортозамещение

Миф

«Реестр российских программ и БД сформирован»

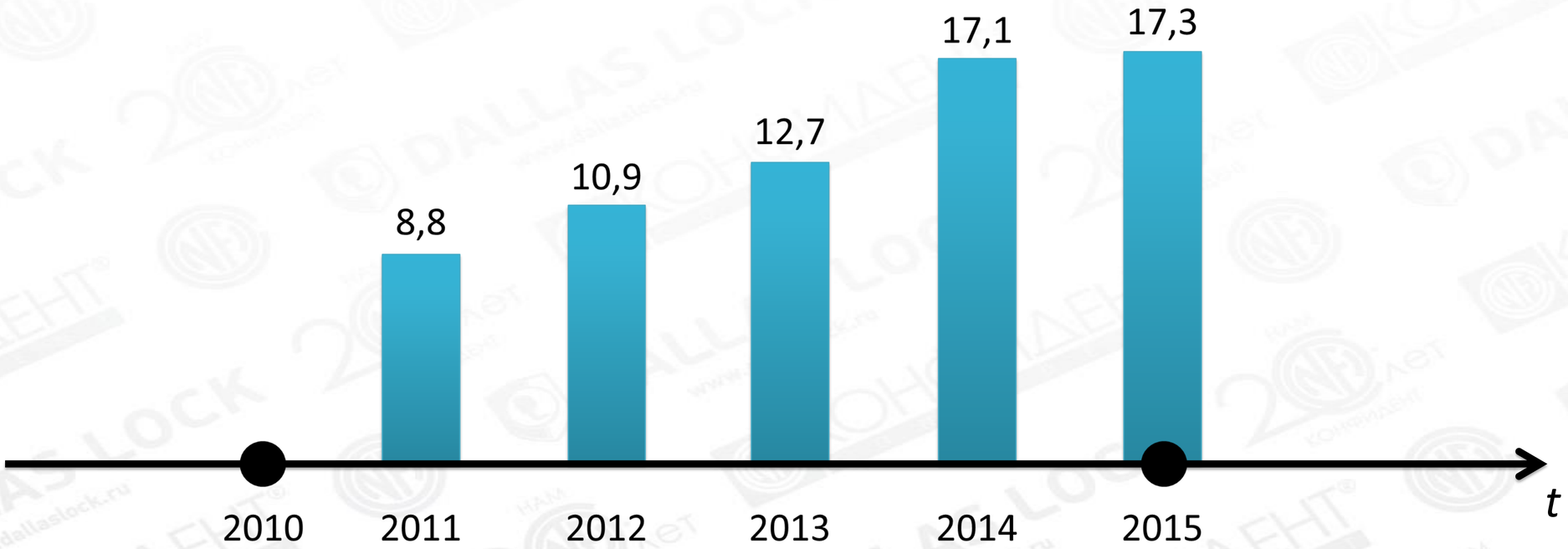
Импортозамещение

Распоряжение Правительства РФ от 17 декабря 2010 г. № 2299-р
Утверждён план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения

Постановление Правительства РФ от 16 ноября 2015 г. № 1236
«Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств...»

Доля ОС с открытым исходным кодом (например, Linux) в организациях по данным Росстата

Импортозамещение



Импортозамещение

ПОТРЕБНОСТЬ В ПО

Определяется перечень программного обеспечения с указанием требований к функционалу.

ВЫБОР В РЕЕСТРЕ

ПО в реестре распределено по классам, что упрощает поиск.

ЗАКУПКА российского ПО

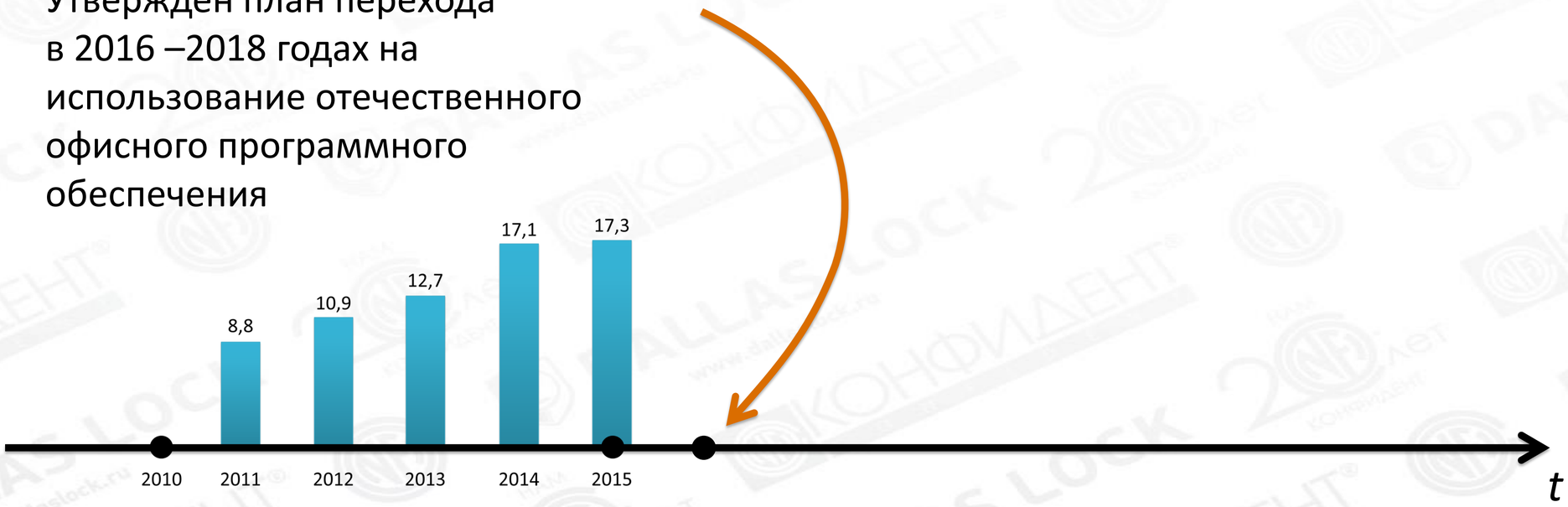
или

ЗАКУПКА

иностранного ПО с обоснованием невозможности закупки отечественного

Импортозамещение

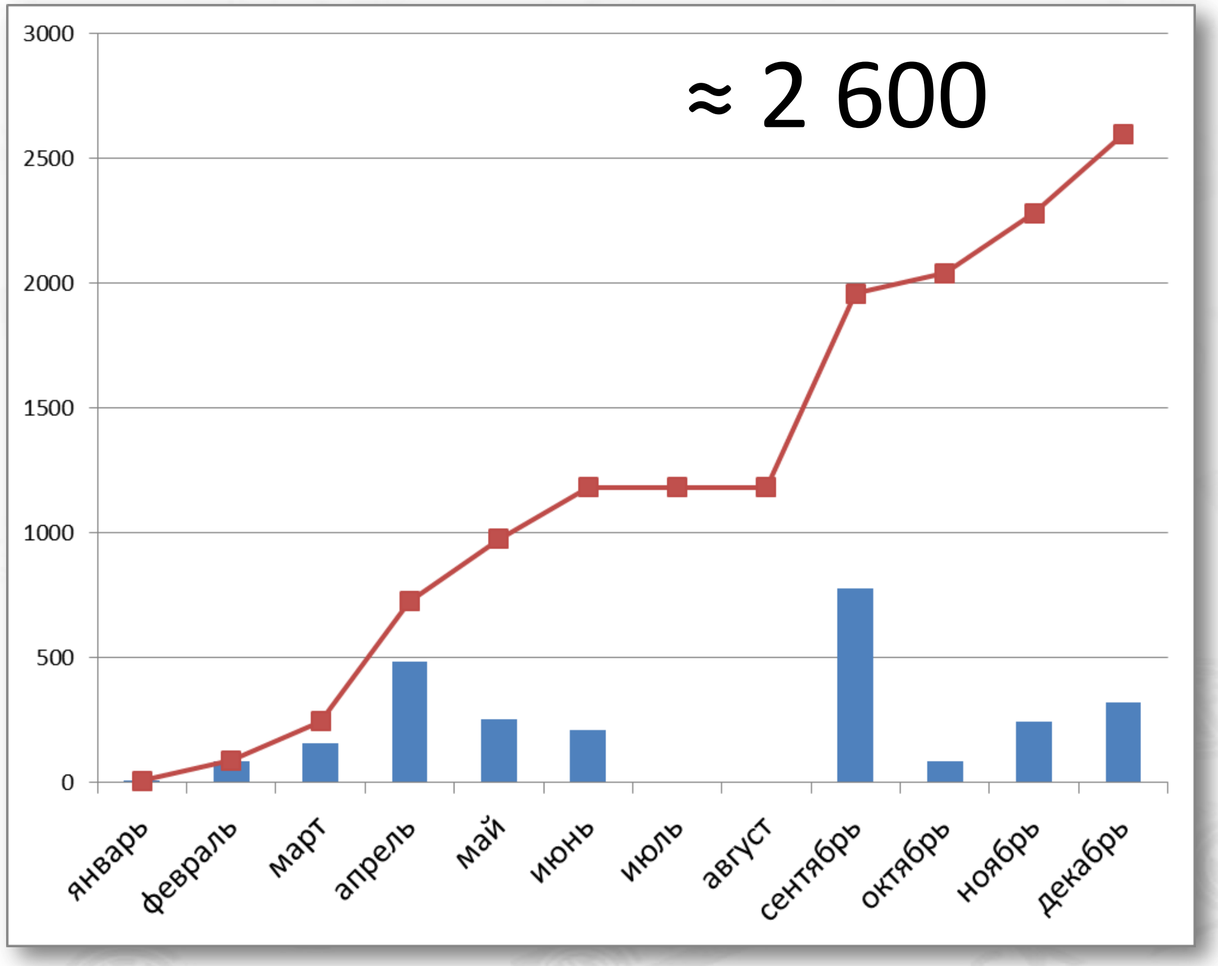
Распоряжение Правительства РФ от 26 июля 2016 г. № 1588-р
Утверждён план перехода в 2016 –2018 годах на использование отечественного офисного программного обеспечения



Импортозамещение

Утверждённый Правительством РФ План перехода в 2016 –2018 годах на использование отечественного офисного программного обеспечения

Импортозамещение



Динамика регистрации ПО в Едином реестре российских программ для ЭВМ и БД

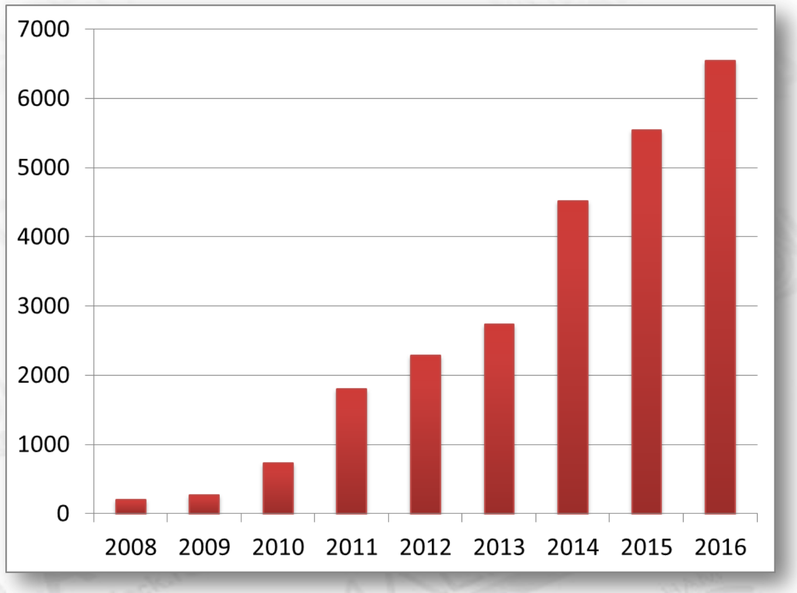
Импортозамещение

Минкомсвязь России

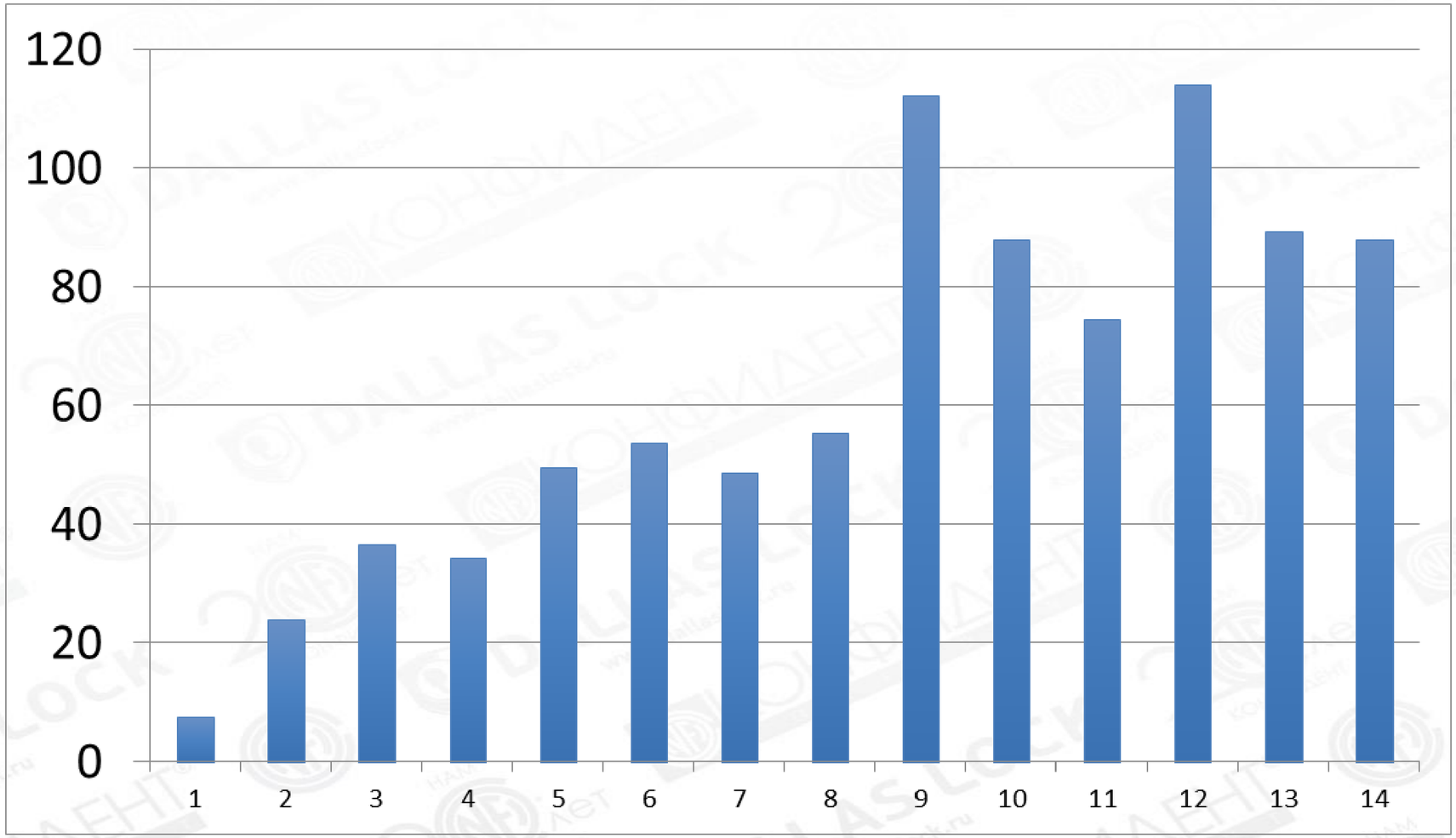
Реестр аккредитованных организаций, осуществляющих деятельность в области ИТ
(по состоянию на 29.12.2016 г.)
http://minsvyaz.ru/ru/activity/govservices/1/

6 599
разработчиков

«… [российская] организация осуществляет разработку и реализацию программ для ЭВМ и баз данных… и (или) оказывает услуги (выполняет работы) по адаптации программ ЭВМ и баз данных… установке, тестированию и сопровождению программ ЭВМ и баз данных».



Среднее время ожидания (в днях) за 2016 год



Импортозамещение

Миф

«если ПО нет в Едином реестре,
то оно не российское»

Импортозамещение

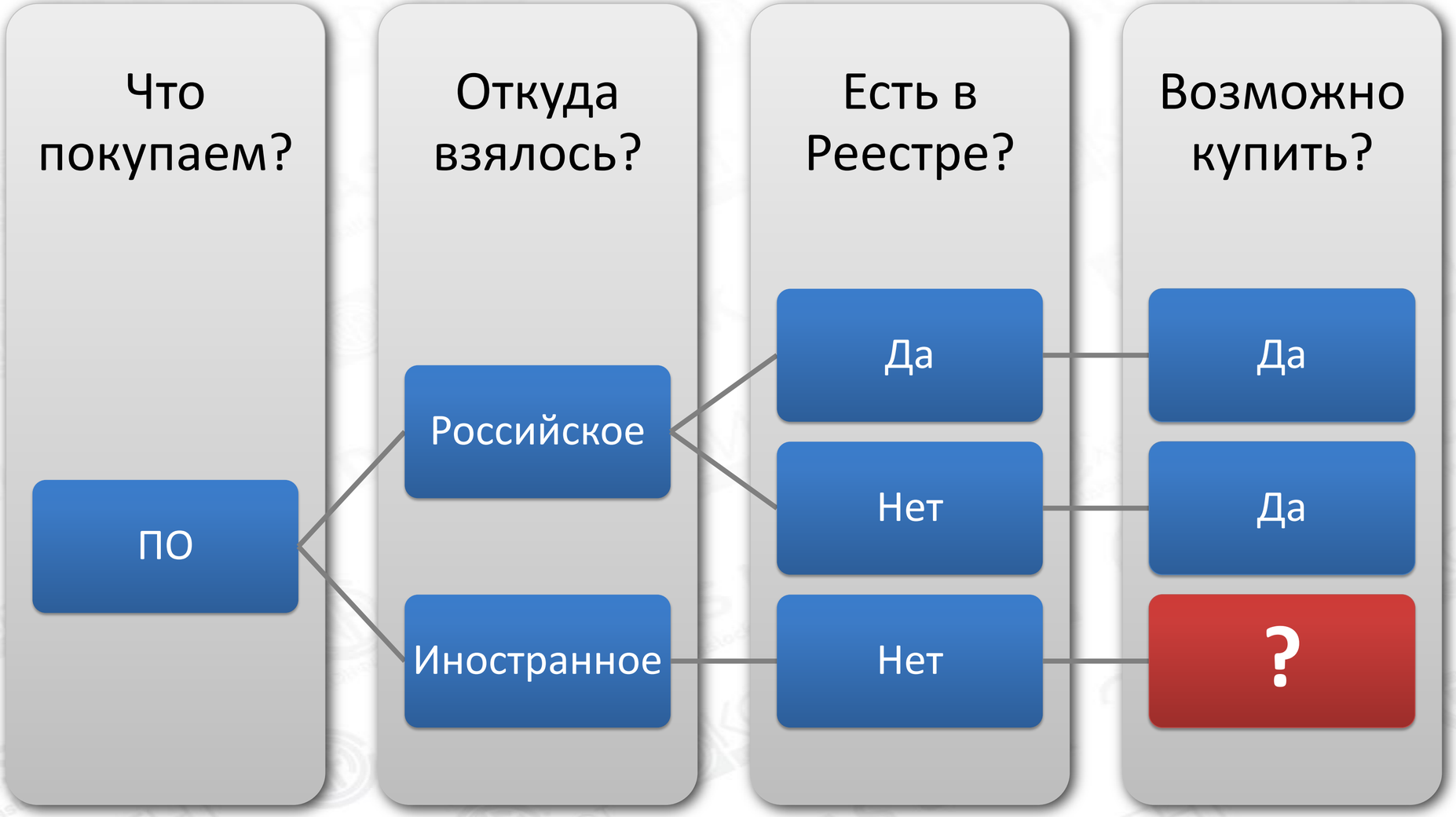
В Постановлении Правительства РФ от 16 ноября 2015 г. № 1236 «*Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств...*» **нет требования, что для подтверждения российского происхождения софт должен обязательно находиться в реестре отечественного ПО**

Импортозамещение

Миф

«Реестр отечественного ПО защищает от импортного ПО»

Импортозамещение



Как поступают некоторые недобросовестные организации при закупке импортного программного обеспечения

1. **Поиск отечественных аналогов в других классах программного обеспечения**. Необходимо определить не только ответственного за классификацию, но и методику такой оценки.

2. **Указание на специфическую функциональность в импортном программном обеспечении**. Нужны ли именно эти функции для обеспечения государственных и муниципальных нужд?

Условия для функционирования отечественного ПО

Подавляющее большинство программ в инфраструктуре заказчиков работает под управлением ОС Windows.

Выводы

- ИТ-инфраструктура и нормативные требования в области ИБ развиваются.
- Само наличие требований не означает их мгновенное исполнение. Реальные проекты появляются только через некоторое время.
- Действующая система сертификации позволяет защитить информацию с помощью продуктов, которые прошли независимые проверки.
- Сертифицированные СЗИ имеют различия в уровнях и классах сертификации, функциональности, производительности, качестве технической поддержки, совокупной стоимости владения.
- Степень безопасности ПО определяется не страной происхождения, а качеством продукта и системой его проверки независимыми организациями.
- Единый реестр отечественного ПО пока ещё не заработал в полную силу.
- Исходя из текущей ИТ-инфраструктуры заказчиков, нормативных требований и динамики их развития, накладные сертифицированные средства защиты информации являются наиболее востребованными решениями.

Спасибо за внимание!

https://dallaslock.ru