Актуальные вопросы защиты государственных информационных систем в период перехода на импортозамещающие технологии

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Кратко о ГК «Конфидент»

КОНФИДЕНТ
ГРУППА КОМПАНИЙ

…в 2017 году у нас юбилей

Государственные информационные системы

Федеральный закон от 27.07.2006 № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»

Статья 13. п.1

Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

- ✓ **Существует множество точек зрения на вопрос отнесения ИС к ГИС.**
- ✓ **Фактически, любая ИС в органе государственной власти является ГИС.**

ФСТЭК России

Обязательные Требования ФСТЭК России:

- Приказ ФСТЭК России от 11.02.2016 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции Приказа ФСТЭК России от 15.02.2017 № 27).

- Методический документ «Меры защиты информации в ГИС», утвержден ФСТЭК России 11 февраля 2014 г.

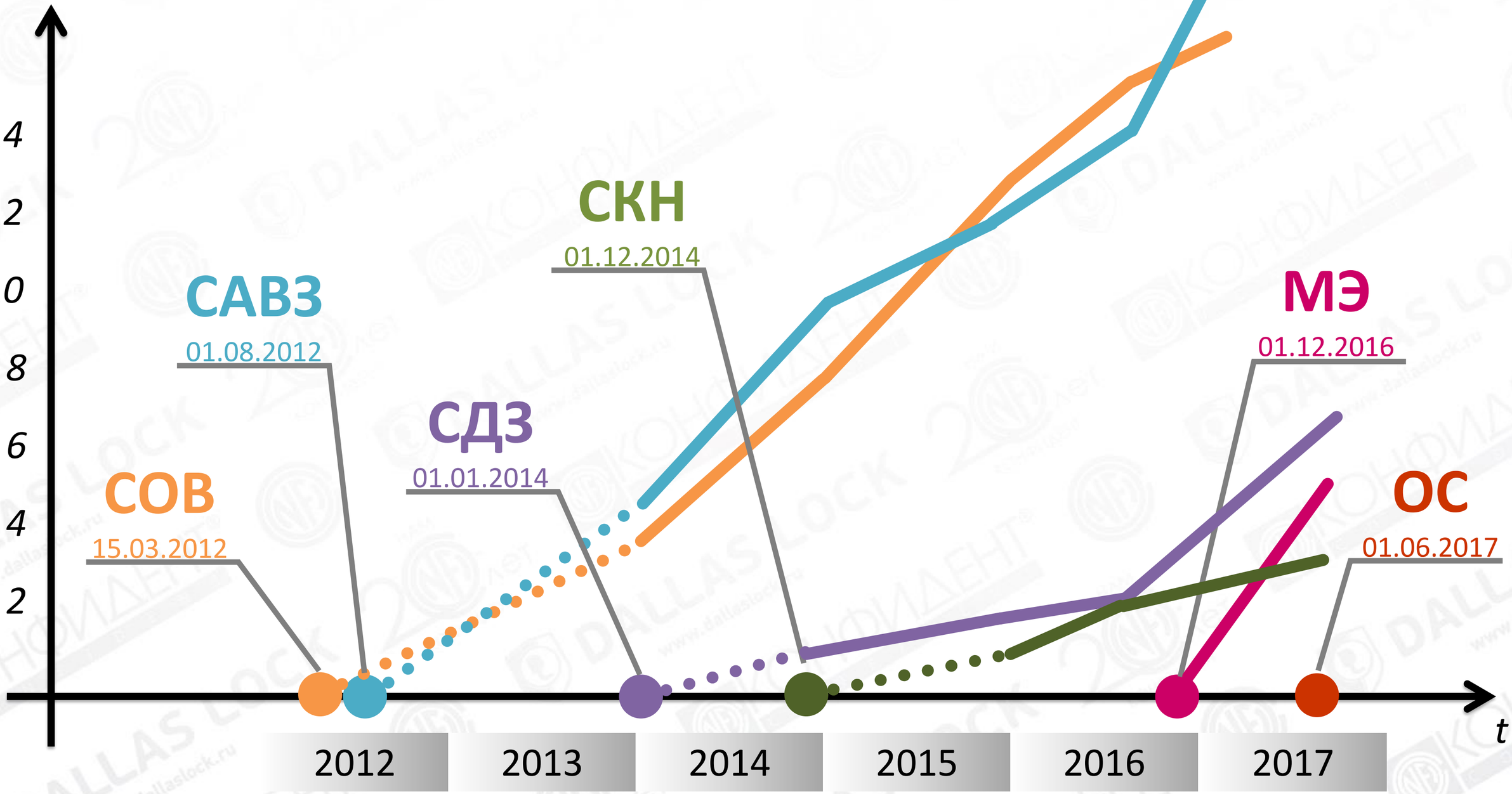
Сертифицированные СЗИ

ФСТЭК России

- **СЗИ НСД** - средства защиты информации от несанкционированного доступа
- **САВЗ** - средства антивирусной защиты
- **СДЗ** - средства доверенной загрузки
- **МЭ** - межсетевые экраны
- **СОВ** - системы обнаружения и предотвращения вторжений
- **СКН** - средства контроля съёмных машинных носителей информации

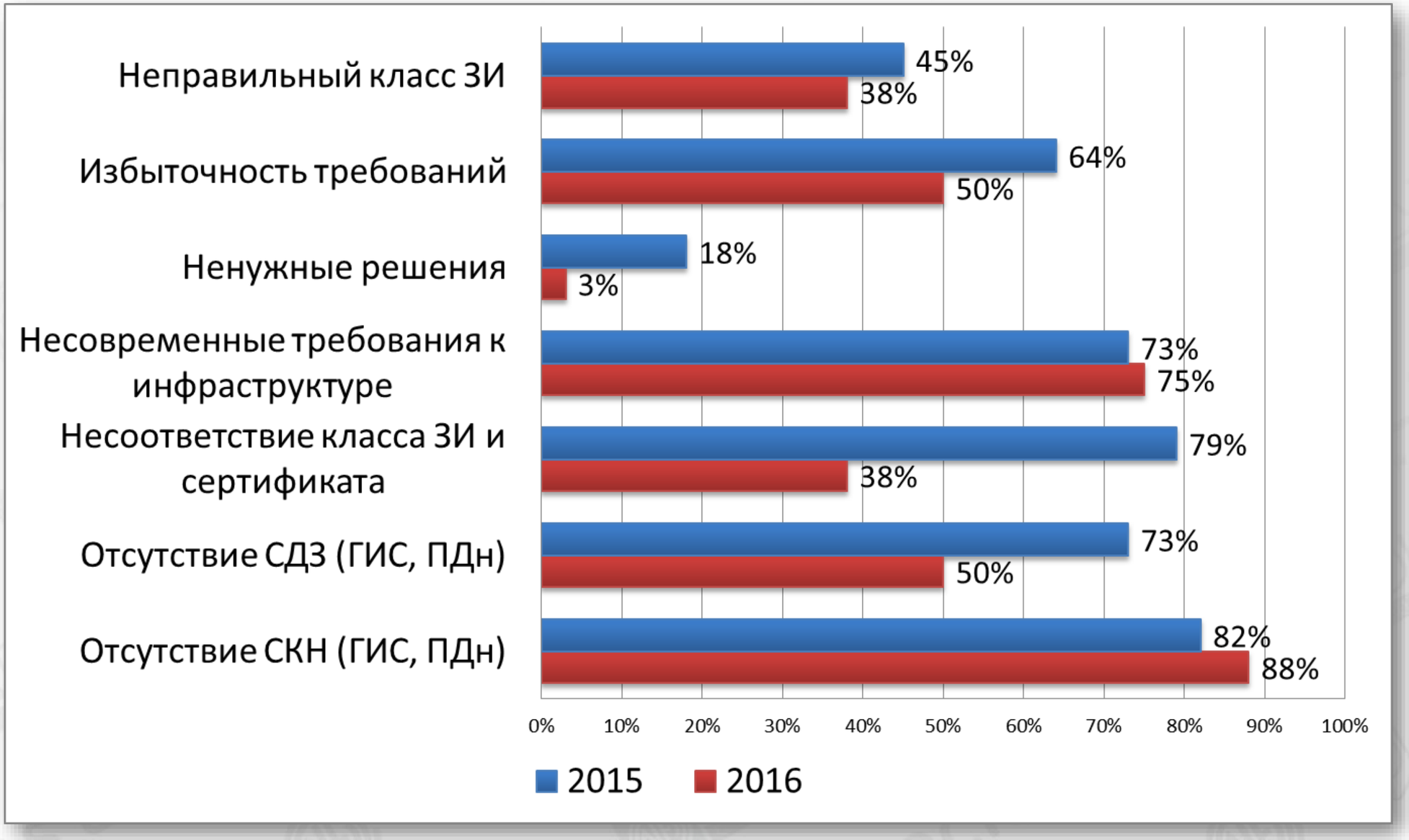
СЗИ, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России

Количество сертифицированных СЗИ



Соблюдение требований операторами

Основные неточности в конкурсной документации 2016*



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

Импортозамещение

Распоряжение Правительства РФ от 17 декабря 2010 г. № 2299-р

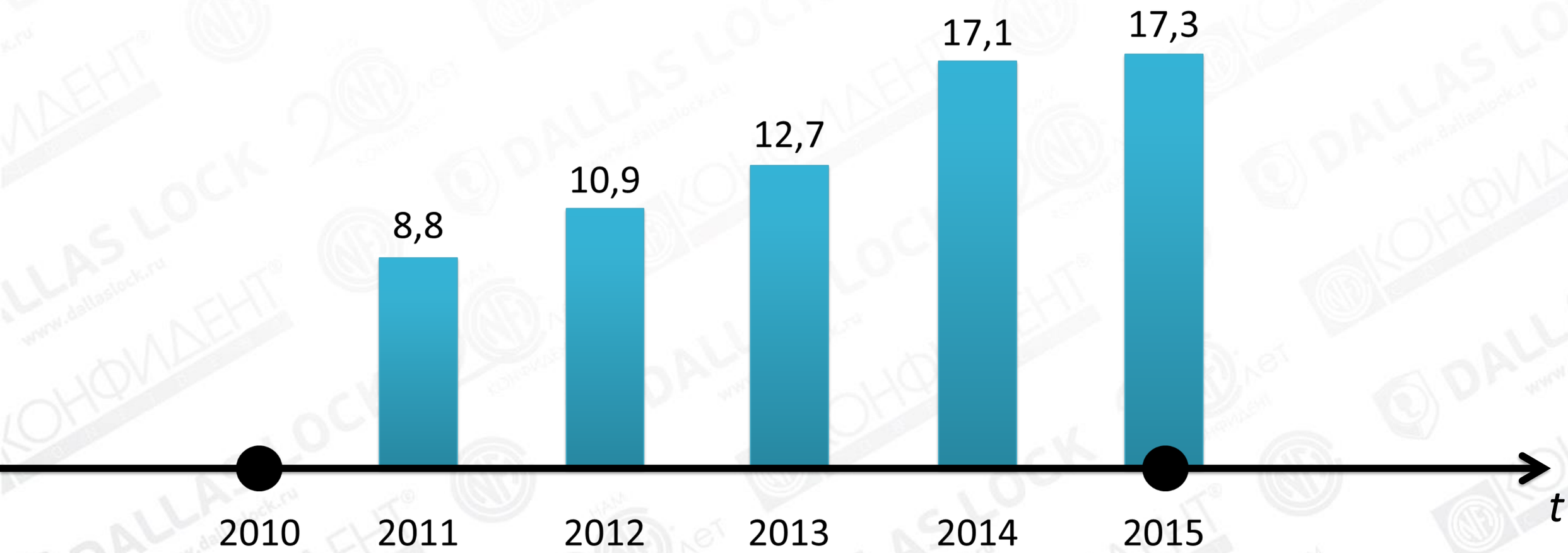
Утверждён план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения

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.

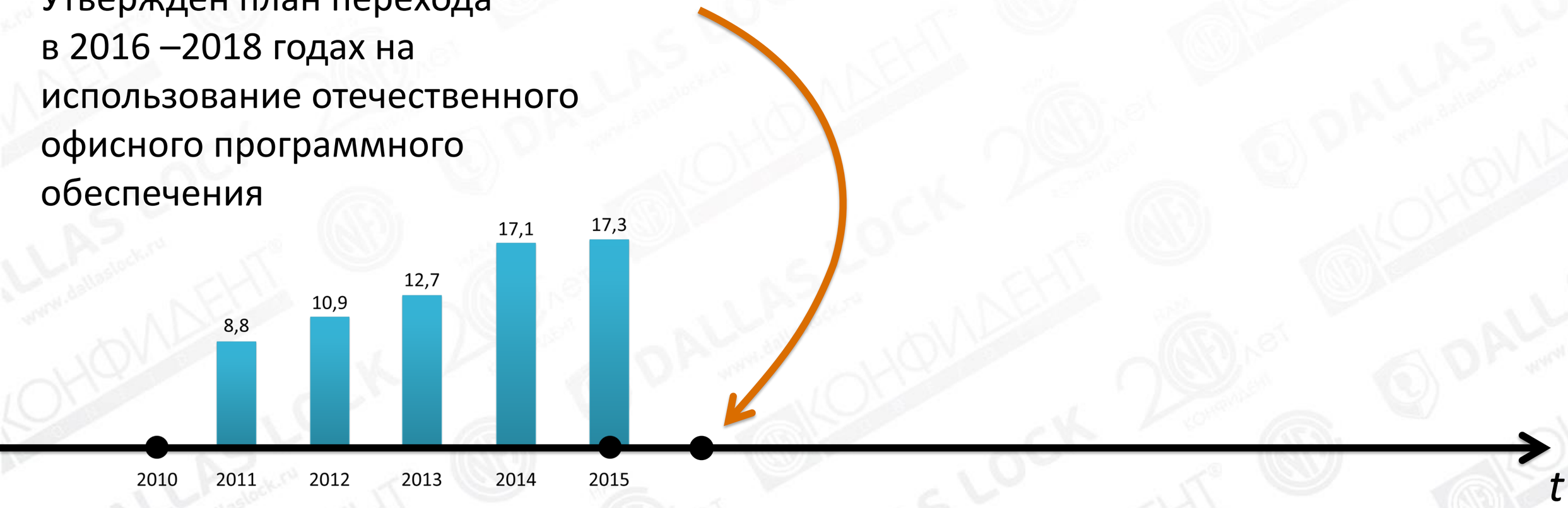
ЗАКУПКА российского ПО

ИЛИ

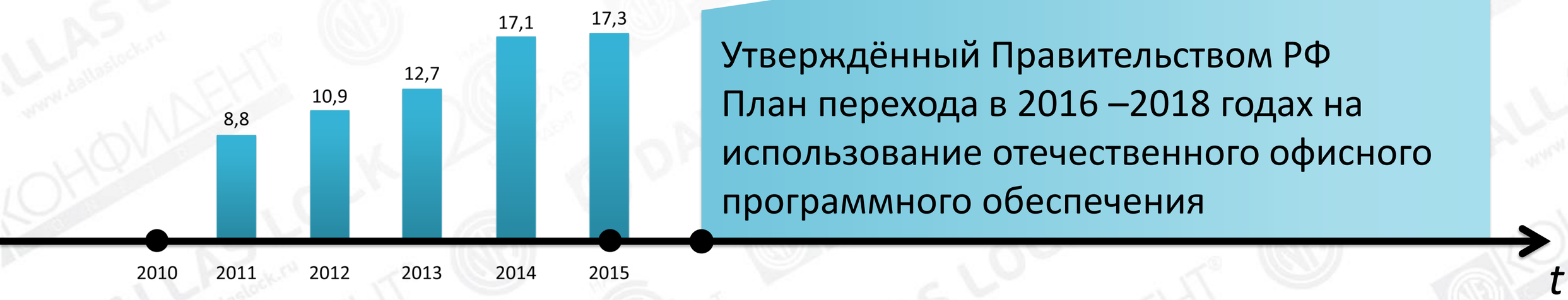
ЗАКУПКА иностранного ПО с обоснованием невозможности закупки отечественного

Импортозамещение

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



Инфраструктура заказчиков действительно меняется



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

В Реестре российских программ для ЭВМ и БД содержится почти 3000 записей

Условия для функционирования отечественного ПО

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

Российские ОС – это важно

Направления развития:

- отечественные ОС
- прикладное ПО (включая офисное)
- средства разработки
- системное ПО и средства защиты информации

} под управлением отечественных ОС

Влияет ли факт российского происхождения ПО на защиту информации?

Критерии «российскости» ПО

ФЗ-188 от 25.06.2015г.

- Принадлежность исключительных прав российским лицам
- Возможность свободной реализации на территории РФ
- Ограничения по суммам выплат иностранным лицам
- Отсутствие сведений, составляющих государственную тайну
- Прочие требования.

Какая часть программного кода отечественного ПО написана российскими разработчиками?

Позиция регуляторов

Минкомсвязь России

Письмо «О необходимости соблюдения государственными заказчиками требований по защите информации» от 15 марта 2016 года N НН-П11-4736

- самостоятельное принятие решений государственными и муниципальными заказчиками в части необходимых требований по защите информации, содержащейся в ГИС, в том числе в части выбора из Реестра общесистемного, прикладного, специального программного обеспечения, информационных технологий, а также средств защиты информации в соответствии с требованиями 17-го приказа ФСТЭК России, а также ФЗ-149 от 27.07.2006 и ПП-1119 от 01.11.2012
- защита информации в соответствии с 17-м приказом ФСТЭК России является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) её создания и в ходе эксплуатации путём принятия организационных и технических мер защиты информации

Отечественные ОС

Российские ОС из Реестра, имеющие сертификаты ФСТЭК России:

- Операционная система Альт Линукс СПТ 7.0 — сертифицирована по 4 классу РД СВТ, по 3 уровню отсутствия НДВ и ТУ. Сертификат действителен до 14.03.2023 г. (на сайте разработчика указан срок 22.03.2020 г.).
- Операционная система специального назначения «Astra Linux Special Edition» — сертифицирована на соответствие РД СВТ по 3 классу и РД НДВ по 2 уровню. Сертификат действителен до 27.01.2018 г.
- Операционная система РОСА SX «КОБАЛЬТ» 1.0 со встроенными средствами защиты от несанкционированного доступа к информации — сертифицирована на соответствие РД СВТ по 5 классу и РД НДВ по 4 уровню контроля. Сертификат действителен до 07.07.2017 г.
- Программное изделие «Операционная система с открытым программным кодом «Синергия» — сертифицирована на соответствие РД СВТ по 3 классу и РД НДВ по 2 уровню. Сертификат действителен до 13.12.2019 г.

Отечественные ОС

Российские ОС из Реестра, имеющие сертификаты ФСТЭК России:

- Операционная система Альт Линукс СПТ 7.0 — сертифицирована по 4 классу РД СВТ, по 3 уровню отсутствия НДВ и ТУ. Сертификат действителен до 14.03.2023 г. (на сайте разработчика указан срок 22.03.2020 г.).
- Операционная система специального назначения «Astra Linux Special Edition» — сертифицирована на соответствие РД СВТ по 3 классу и РД НДВ по 2 уровню. Сертификат действителен до 27.01.2018 г.
- Операционная система РОСА SX «КОБАЛЬТ» 1.0 со встроенными средствами защиты от несанкционированного доступа к информации — сертифицирована на соответствие РД СВТ по 5 классу и РД НДВ по 4 уровню контроля. Сертификат действителен до 07.07.2017 г.
- Программное изделие «Операционная система с открытым программным кодом «Синергия» — сертифицирована на соответствие РД СВТ по 3 классу и РД НДВ по 2 уровню. Сертификат действителен до 13.12.2019 г.

Сертификация по РД СВТ, РД НДВ

Отечественные ОС

ФСТЭК России

- **САВЗ** средства антивирусной защиты
- **СДЗ** средства доверенной загрузки
- **МЭ** межсетевые экраны
- **СОВ** системы обнаружения и предотвращения вторжений
- **СКН** средства контроля съёмных машинных носителей информации

Сертифицированные СЗИ указанных типов
не содержатся в отечественных ОС

Совместимость ОС с накладными СЗИ

Операционная система	Техническая совместимость со сторонними решениями для защиты информации				
	САВЗ	СКН	СДЗ	МЭ	СОВ
Альт Линукс СПТ 7.0	+	-	+	+	*
Astra Linux Special Edition	+	-	+	*	*
РОСА SX «КОБАЛЬТ» 1.0	+	-	+	*	*
ОС «Синергия»	+	-	+	*	*

* поддерживаются только периметровые решения уровня сети (логических границ сети)

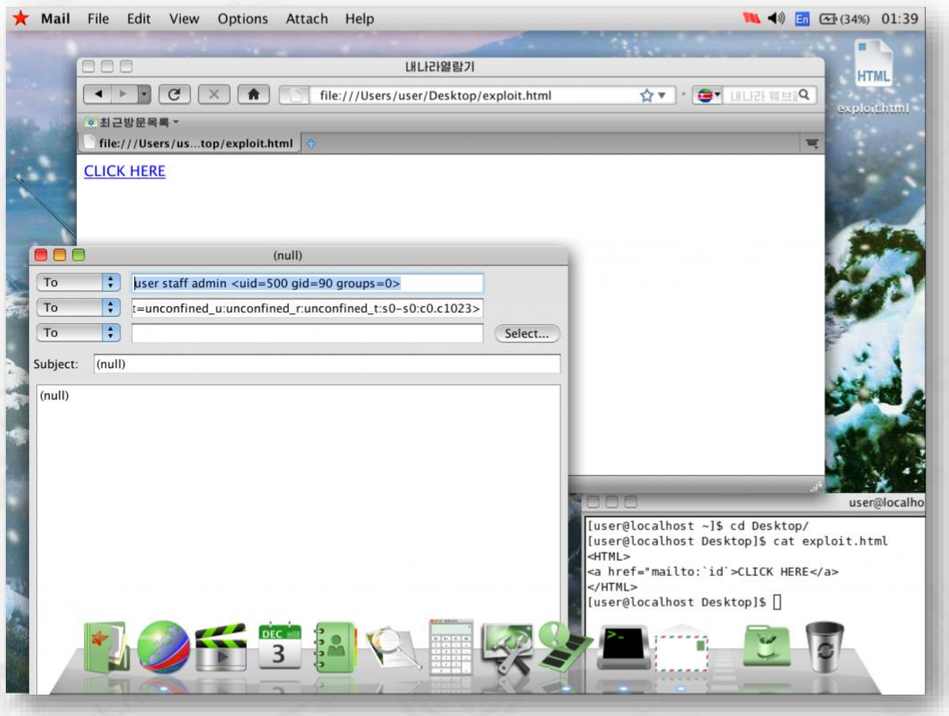
Аттестация информационной системы по требованиям защиты информации при использовании отечественных операционных систем…

во многих случаях не представляется возможной

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

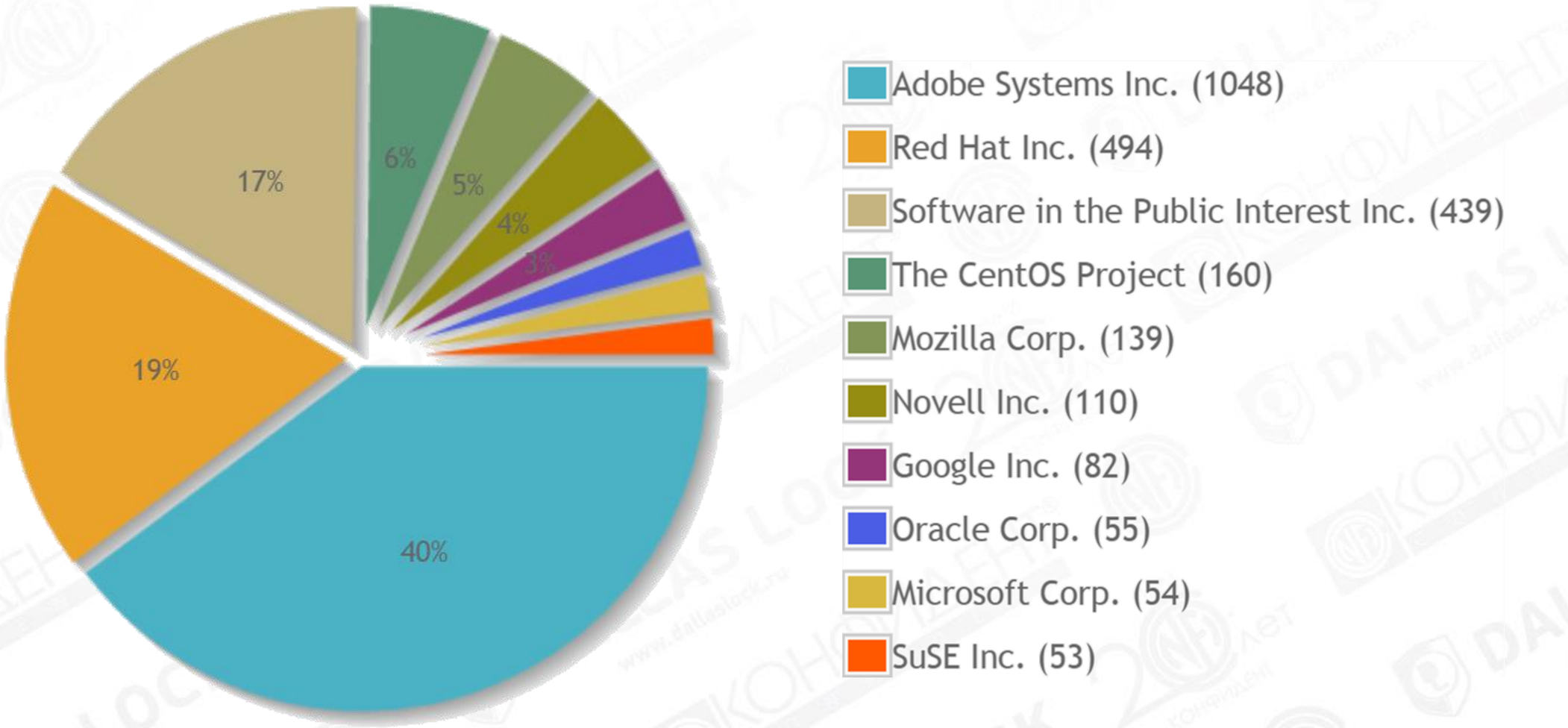
Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2016

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)

ФСТЭК России

Выявление и устранение уязвимостей в информационных системах проводится на следующих этапах жизненного цикла ИС:

- формирование требований к защите информации;
- внедрение системы защиты информации;
- аттестация ИС по требованиям защиты информации и ввод в действие.

Чем больше уязвимостей, тем выше совокупная стоимость владения ГИС

Импортозамещение

Количество выпущенных бюллетеней по безопасности:

Операционная система	2016	2017
Альт Линукс СПТ 7.0	1	1
Astra Linux Special Edition	1	1
РОСА SX «КОБАЛЬТ» 1.0	нет данных	
ОС «Синергия»	нет данных	

Обновления для Windows выходят второй вторник каждого месяца – очевидный потенциал для роста у отечественных ОС.

Выводы

1. Пока ещё рано говорить о том, что переход на импортозамещающие технологии близок к завершению.
2. Встроенных в ОС сертифицированных защитных механизмов пока еще не достаточно для обеспечения защиты информации.
3. Требуется время, чтобы на рынке сертифицированных СЗИ появились соответствующие решения.

Спасибо за внимание!

https://dallaslock.ru