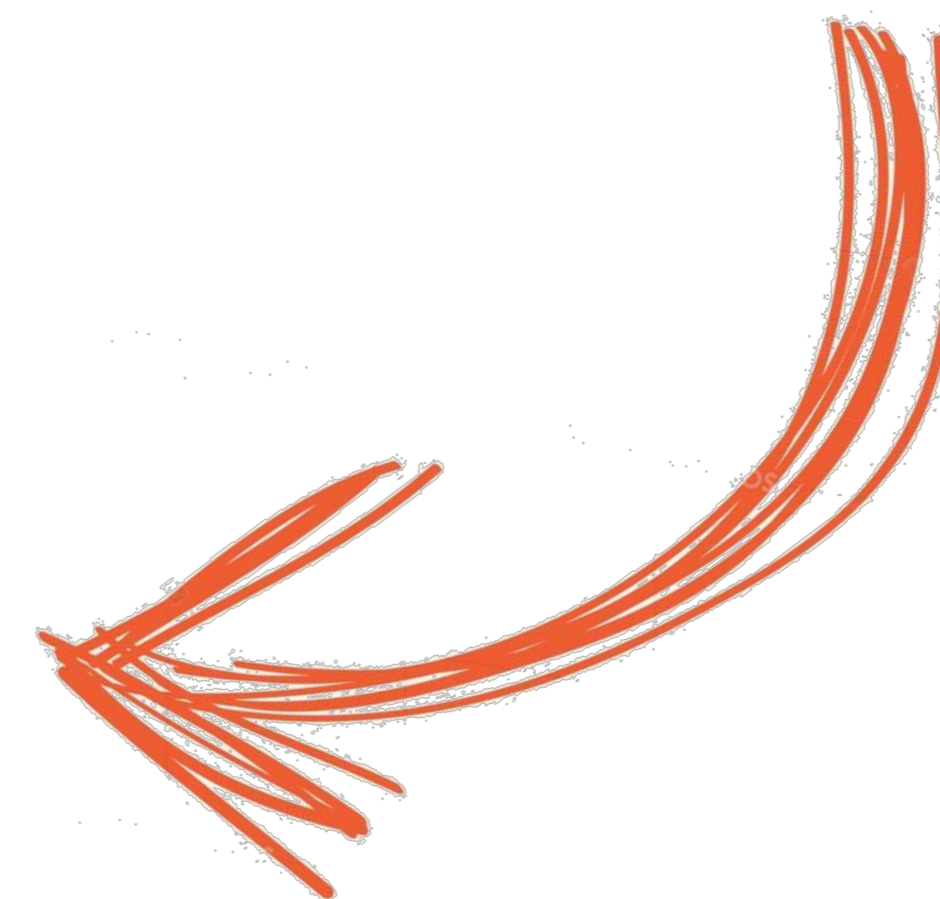
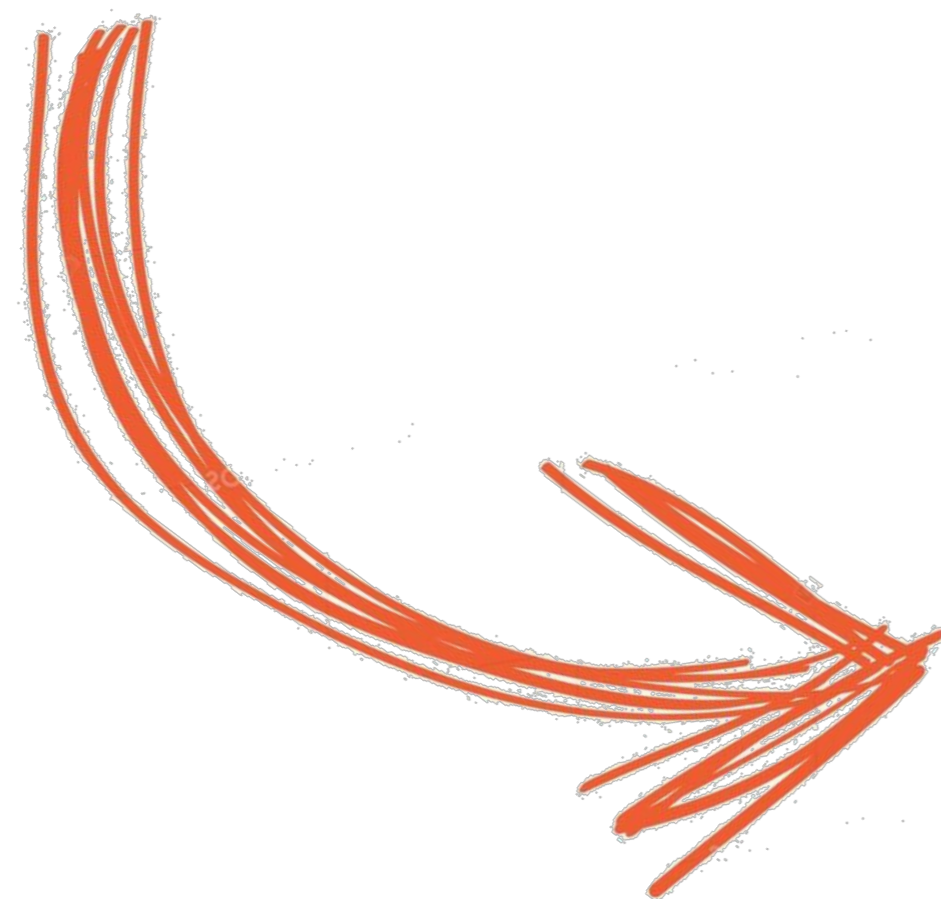




Необходимо обеспечить защиту информации в ГИС и/или в значимом объекте КИИ

Требования по защите информации

Требования по импортозамещению



149-ФЗ «Об информации, информационных технологиях и о защите информации»

Постановление
Правительства № 676

Приказ ФСТЭК России № 17 + «Методичка»

Классификация ГИС

Разработка модели угроз
безопасности информации

Выбор базовых мер
защиты

Адаптация, уточнение, дополнение
+ компенсирующие меры

**Выбор СЗИ
нужного класса**

Требования к системе защиты
информации

187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

Постановление
Правительства № 127

Приказ ФСТЭК России № 239 + «...»

Категорирование
объекта КИИ

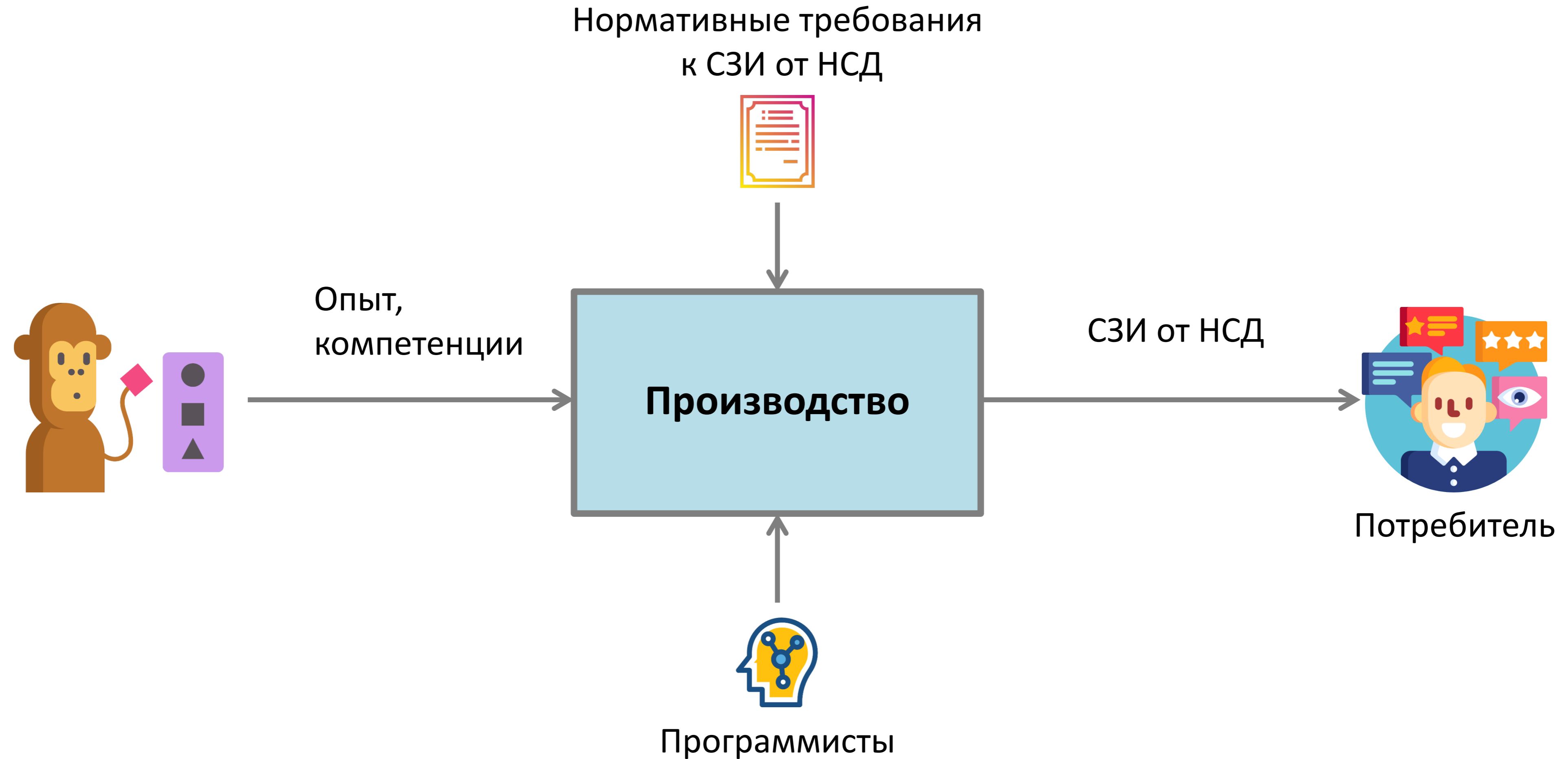
Разработка модели угроз
безопасности информации

Выбор базовых мер
защиты

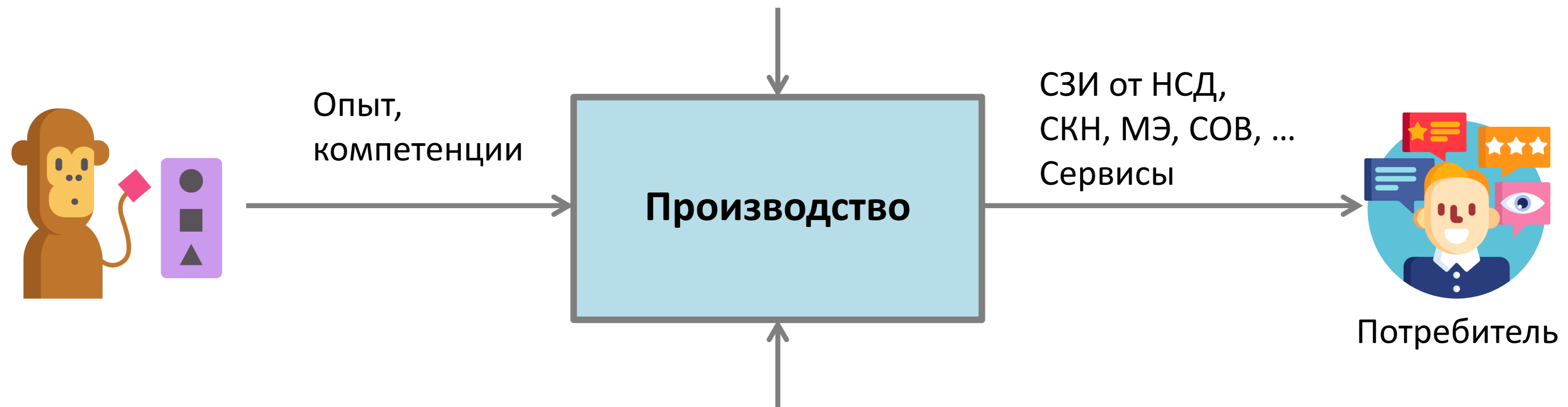
Адаптация, уточнение, дополнение
+ компенсирующие меры

**Выбор СЗИ
нужного класса**

Требования к системе защиты
информации



- Нормативные требования: СЗИ от НСД, СКН, МЭ, СОВ, СДЗ, САВЗ, ОС, ...
- Требования системы сертификации, включая техническую поддержку.
- Функциональные требования рынка.
- Требования по надёжности, производительности и т.п.



- Программисты, аналитики, тестировщики, специалисты поддержки, ...
- Стендовая база и средства (безопасной) разработки и тестирования.
- Инфраструктура для оказания круглосуточной технической поддержки.
- Привлечение испытательной лаборатории и органа по сертификации.

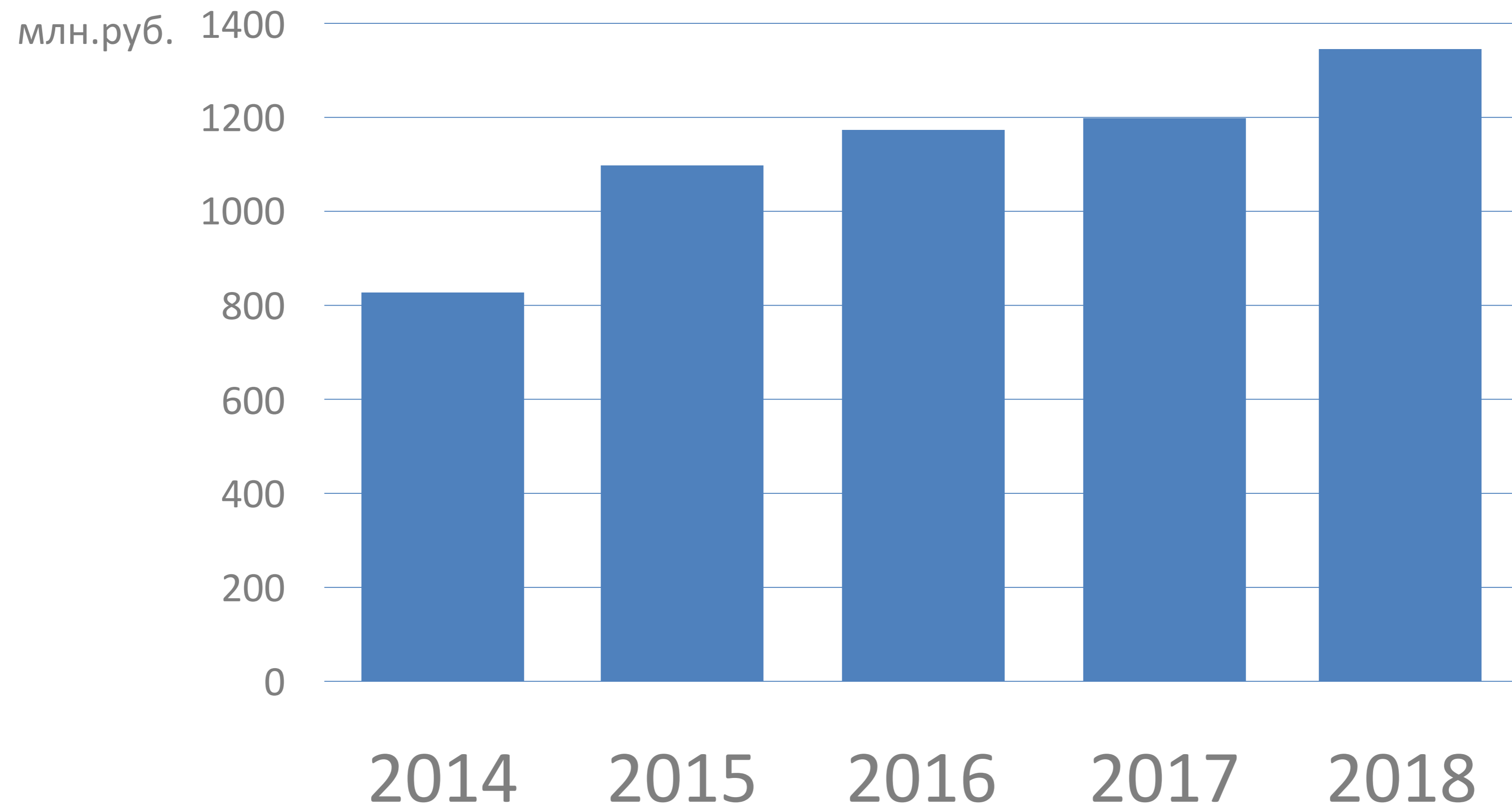


СЗИ от НСД отличаются

УРОВЕНЬ ЗРЕЛОСТИ СЗИ

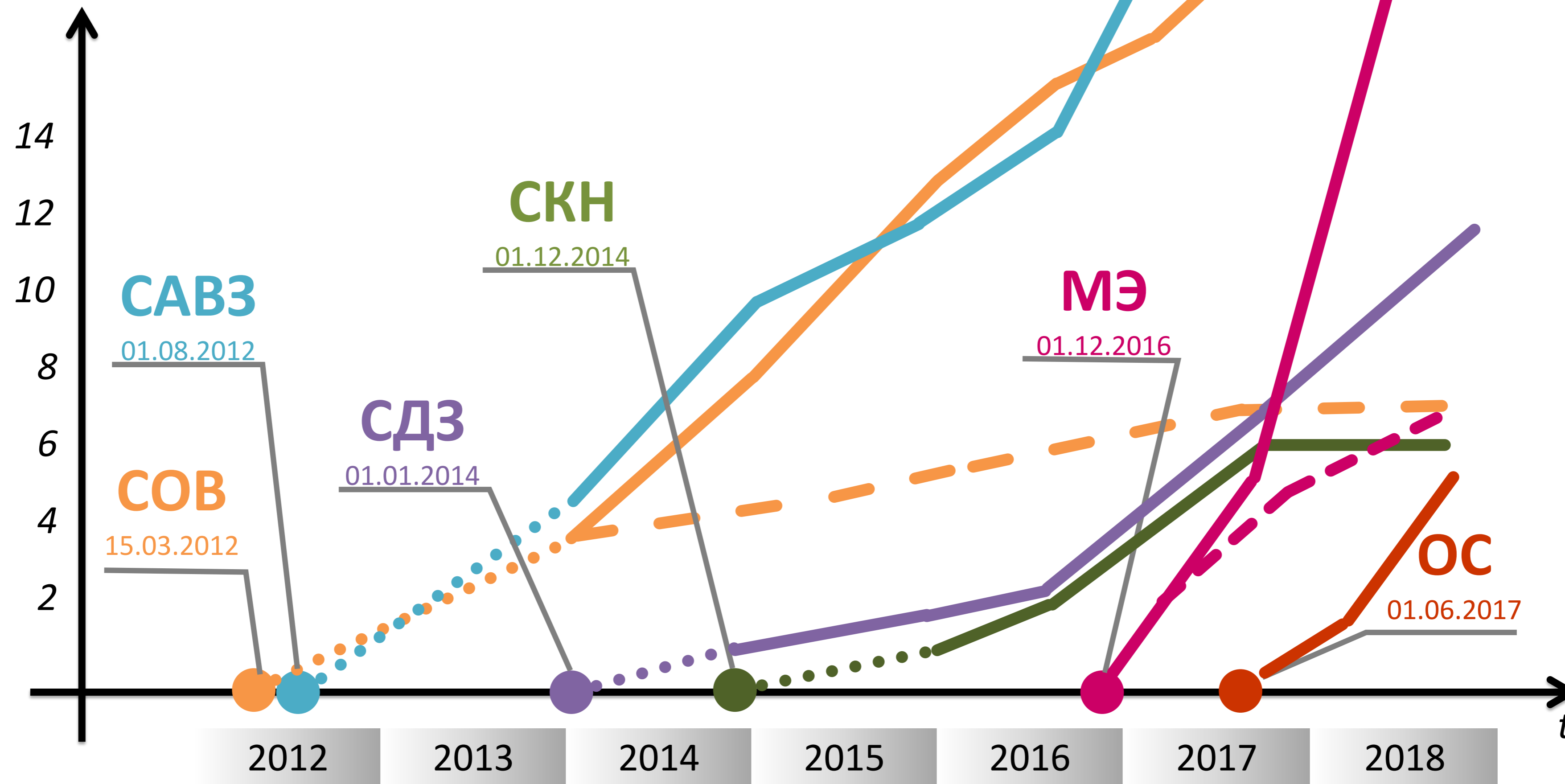
низкий ← → *высокий*

Базовые функции защиты информации от несанкционированного доступа				
Централизованное управление, включая развёртывание				
Наличие сертифицированных модулей в составе системы защиты: СКН, МЭ, СОВ, ...				
Развитые сервисы производителя, включая круглосуточную техническую поддержку				
Дополнительные функции, не входящие в «базовый» набор мер				



Объём рынка СЗИ от НСД, включая модули СКН, МЭ, СОВ
(стоимость лицензий и сервисов в ценах конечных пользователей)

Количество сертифицированных СЗИ





Распоряжение Правительства РФ от 17.12.2010 г. № 2299-р «План перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения».



Постановление Правительства РФ от 16.11.2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».



Письмо Минкомсвязи России от 15.03.2016 НН-П11-4736 «О необходимости соблюдения государственными заказчиками требований о защите информации».



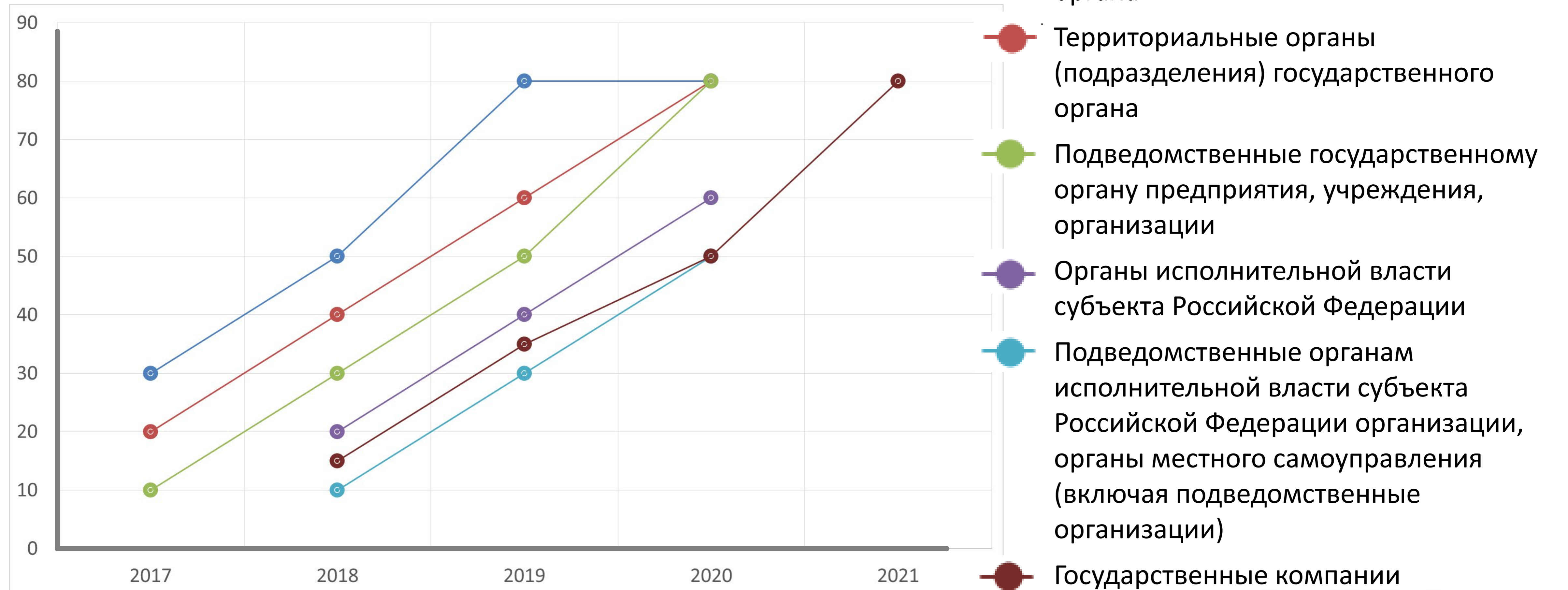
Распоряжение Правительства РФ от 26.07.2016 г. № 1588-р «План перехода в 2016 – 2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения».



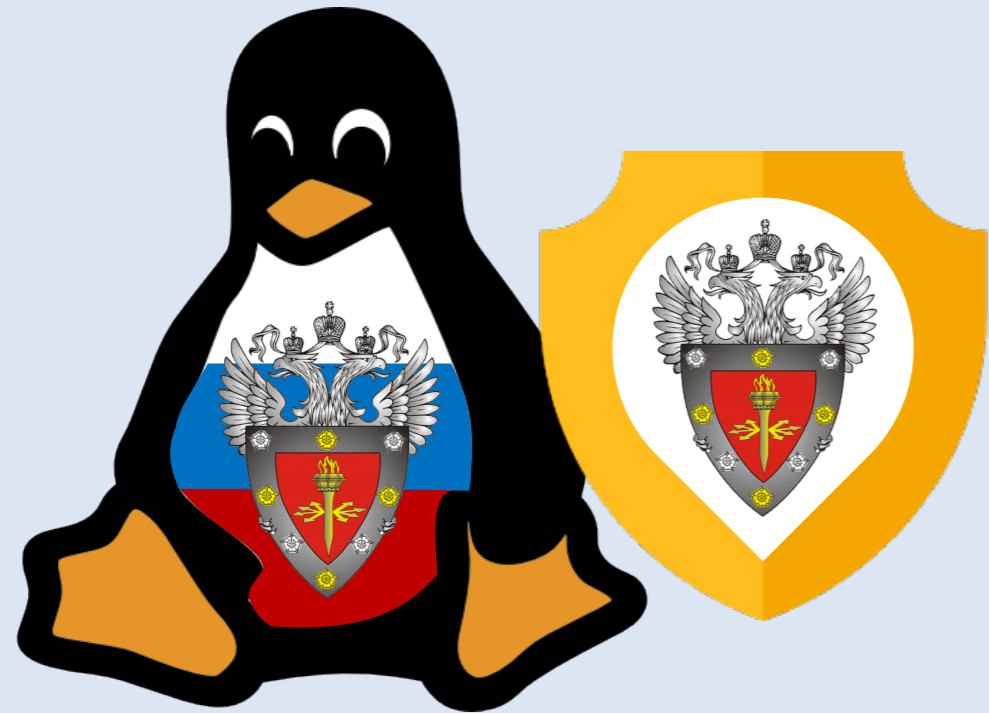
Приказы Минкомсвязи России: методические рекомендации по переходу на использование отечественного офисного программного обеспечения в том числе закупленного ранее офисного программного обеспечения.

Требования по импортозамещению ОС

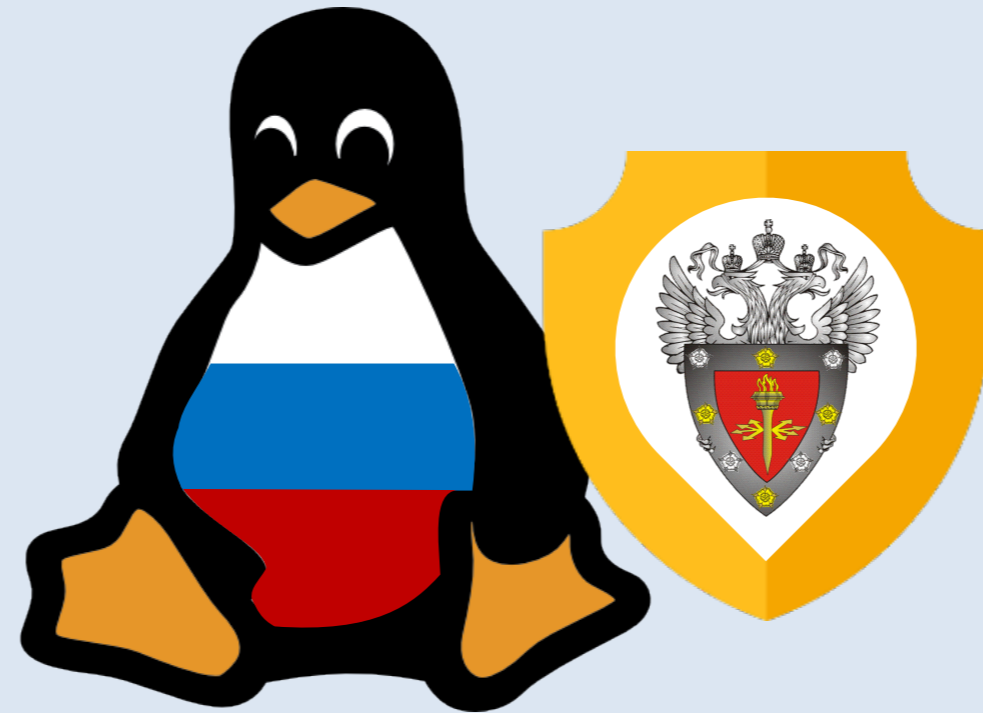
Доля отечественных ОС, %



Какая должна быть ИТ-инфраструктура заказчиков в результате импортозамещения

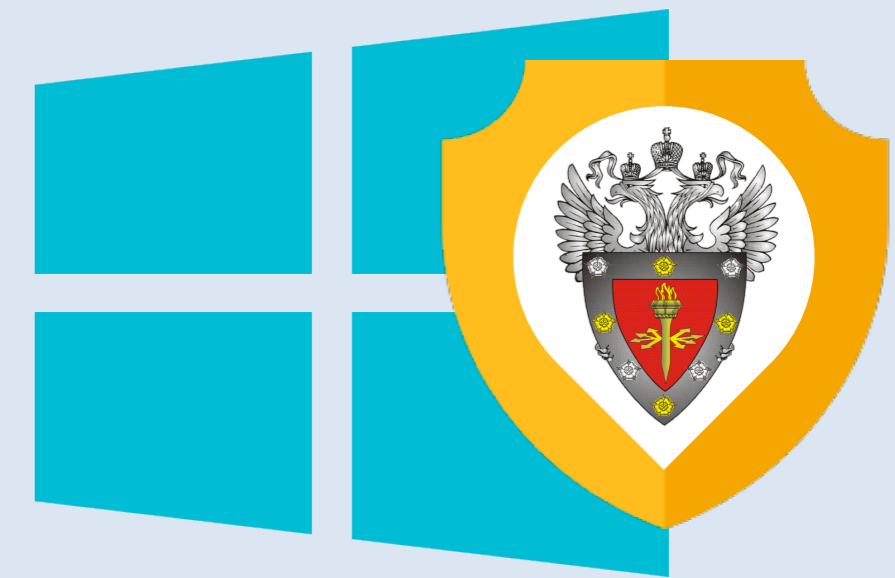


*Сертифицированные
отечественные ОС +
накладные СЗИ*



*Не сертифицированные
отечественные ОС +
накладные СЗИ*

и/или



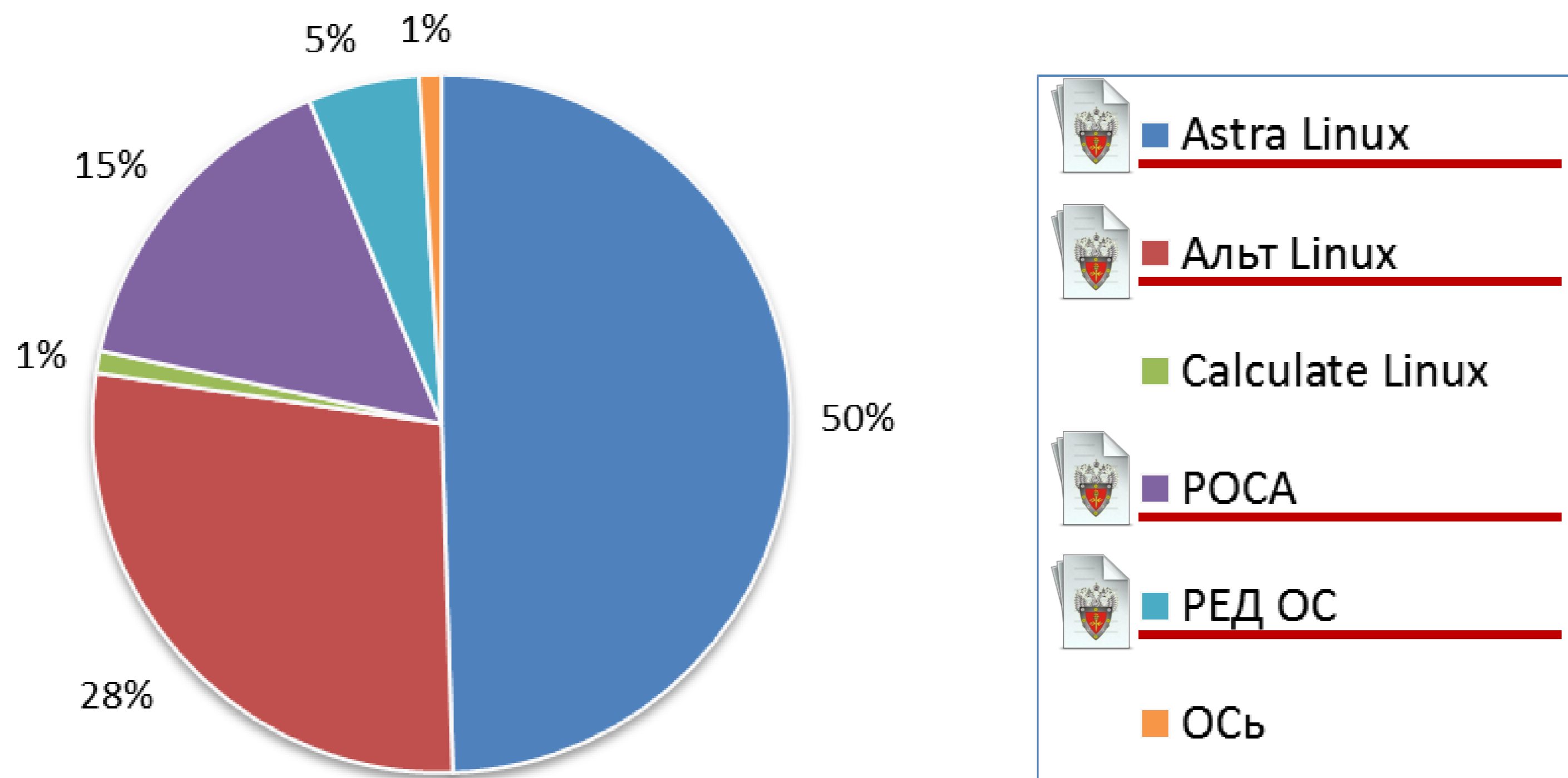
*ОС Windows +
накладные СЗИ*

Количество российских ОС на рынке

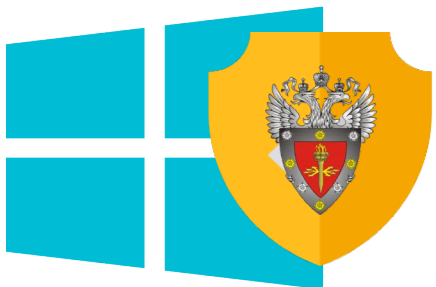
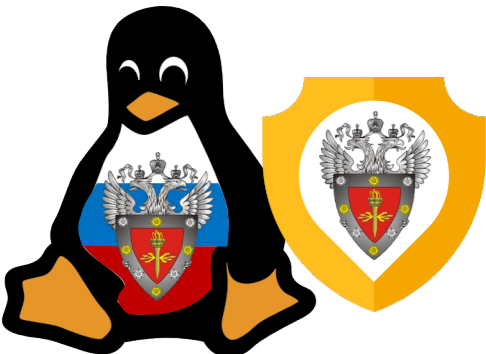
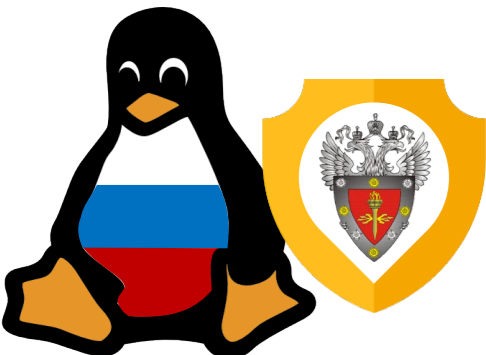


Наиболее популярные российские ОС по данным опроса пользователей

Наиболее популярные настольные российские ОС 2018 г. по мнению пользователей портала DallasLock.ru



Какие у нас есть варианты?

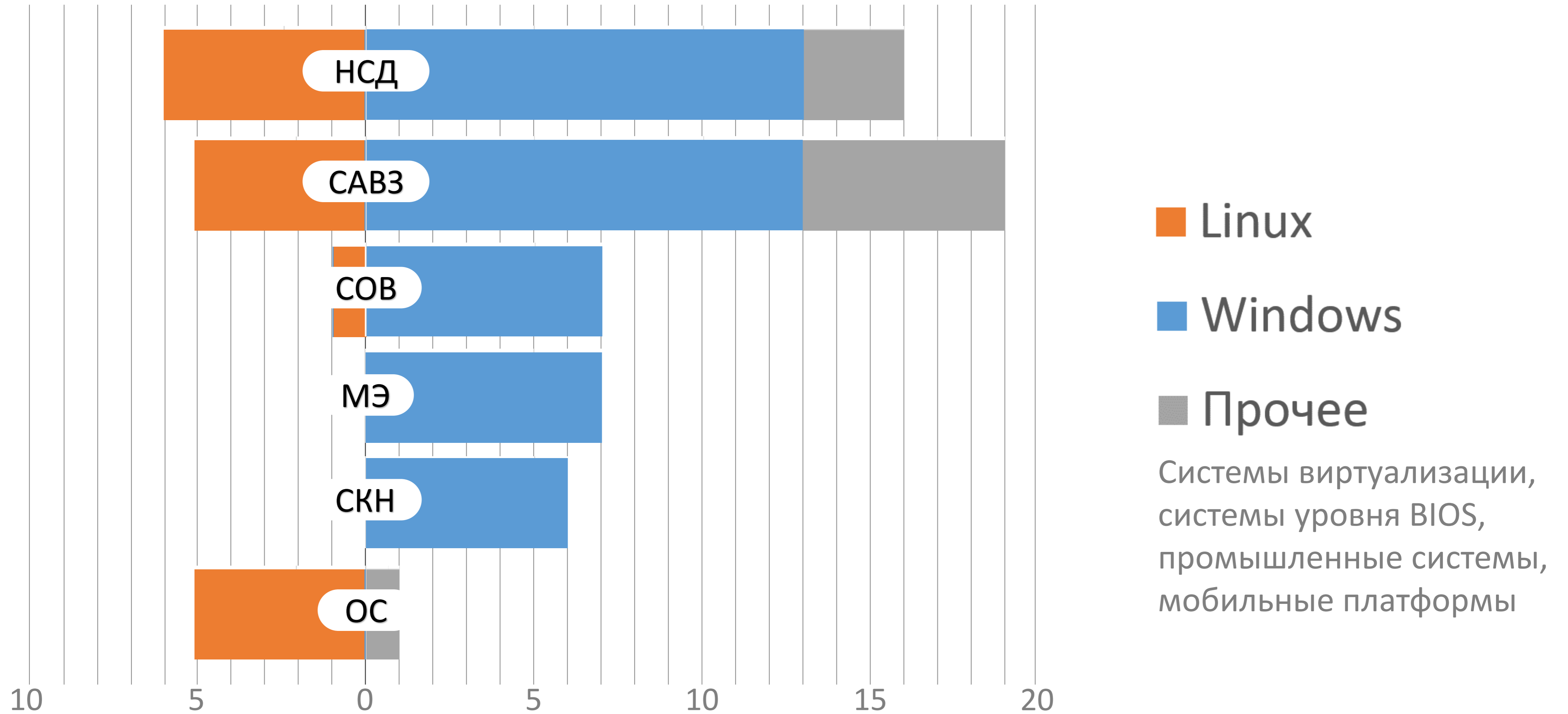
	НСД	МЭ	СОВ	САВЗ	СДЗ	СКН	ОС
 ОС Windows + накладные СЗИ	●	●	●	●	●	●	
 Сертифицированные отечественные ОС + накладные СЗИ	●	✗	●	●	●	✗	●
 Не сертифицированные отечественные ОС + накладные СЗИ	●	✗	✗	●	●	✗	

✗ нет решений

● почти нет решений

● есть решения

Количество сертифицированных решений уровня узла



1

Почему на рынке не появилось в достаточном количестве СЗИ под ОС Linux?

2

Как скоро они появятся и появятся ли вообще?

Сроки появления СЗИ уровня узла



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

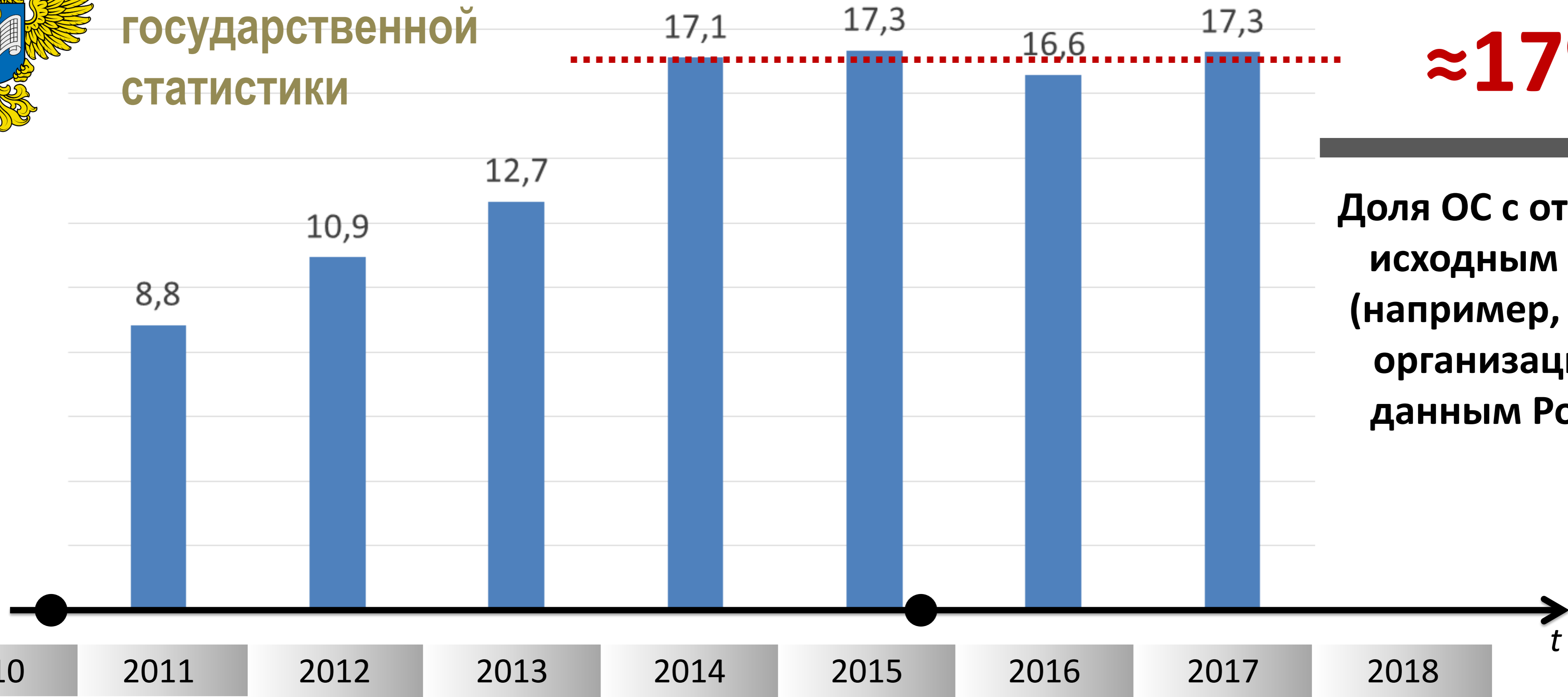
Постановление Правительства РФ от 16 ноября 2015 г. № 1236

2010 2011 2012 2013 2014 2015 2016 2017 2018 t

Доля ОС Linux в организациях по данным Росстата



Федеральная служба
государственной
статистики

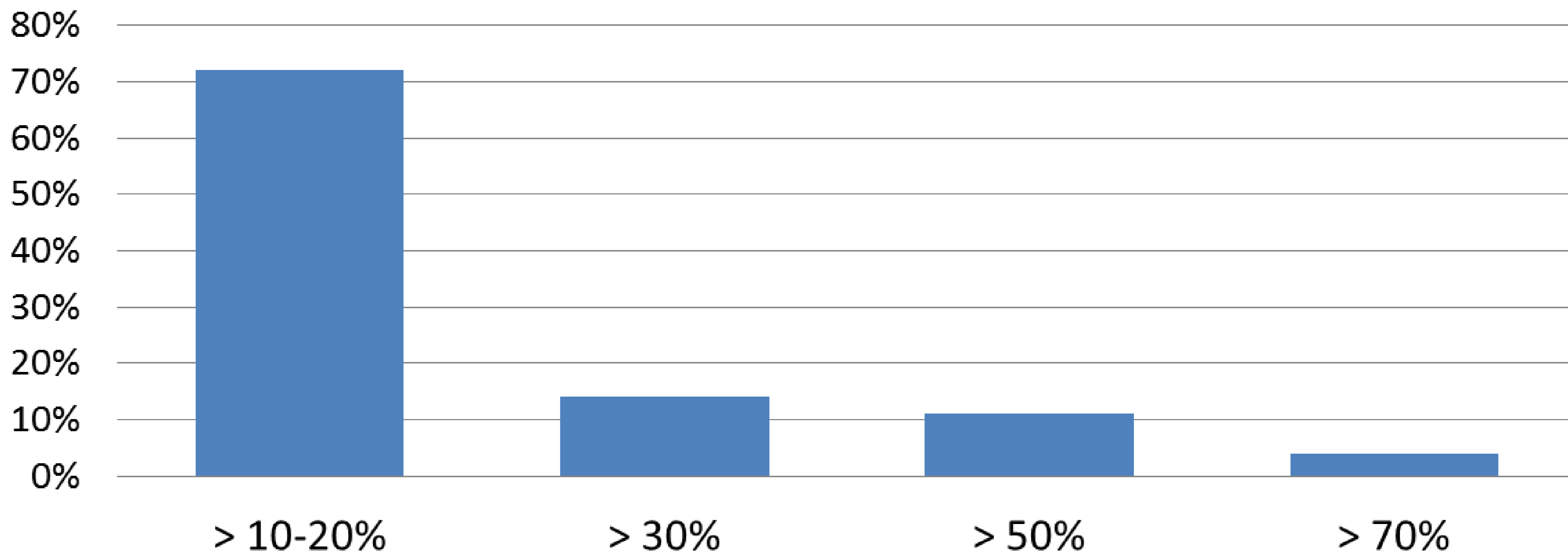


≈17%

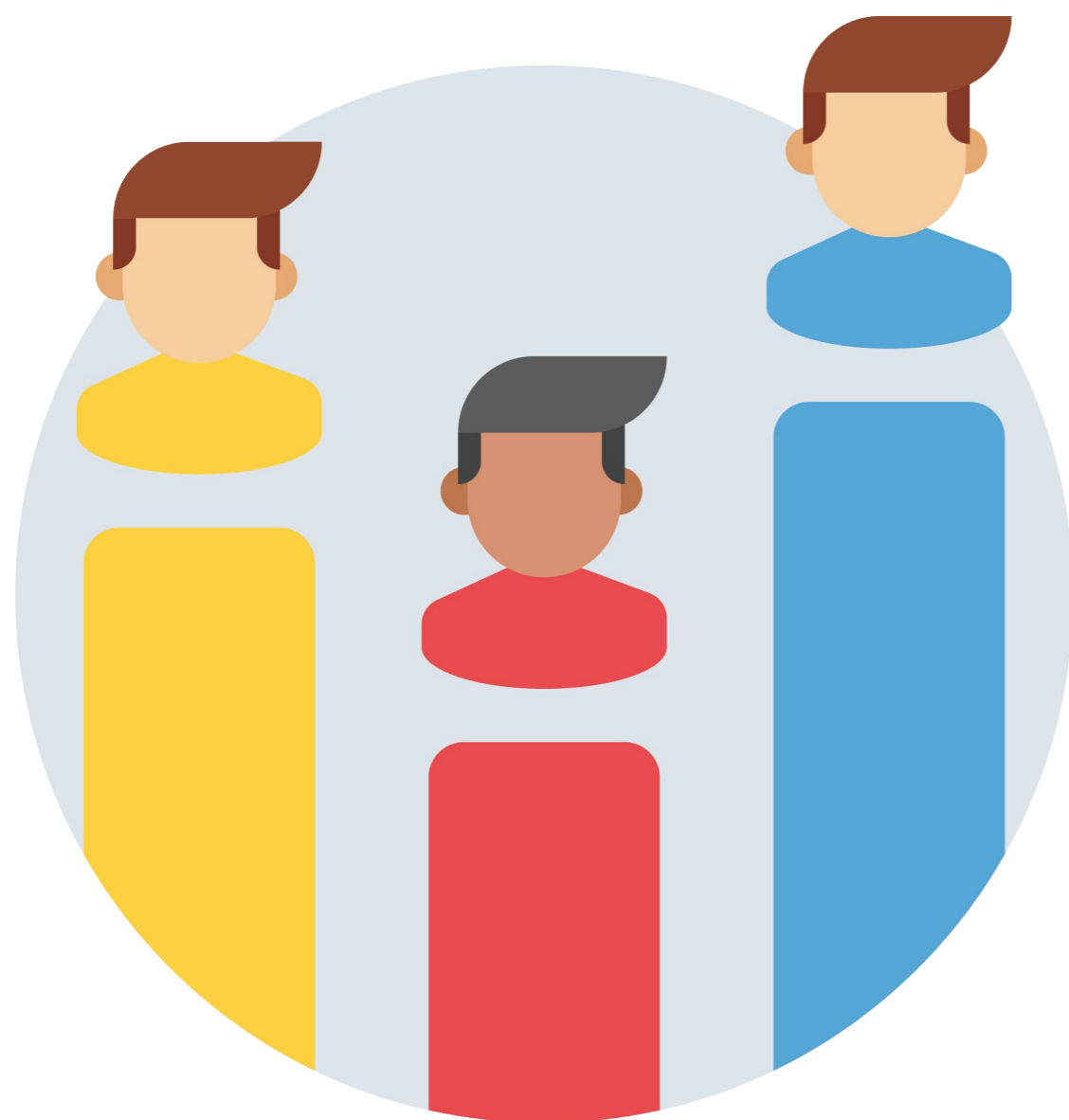
Доля ОС с открытым
исходным кодом
(например, Linux) в
организациях по
данным Росстата

Доля российских ОС в инфраструктуре заказчиков по данным опроса пользователей

Доля российских ОС в инфраструктуре государственных заказчиков на конец 2018 г. по мнению пользователей портала DallasLock.ru



Доля российских ОС в инфраструктуре заказчиков по данным опроса пользователей



Опросы показывают, что доля российских ОС на текущий момент не превышает 10%-20%

Объём госзакупок российских ОС для рабочих станций

млн.руб. 1400



Доля российских ОС в ИТ-инфраструктуре заказчиков



Росстат

≈17%



Опросы

10-20%



Госзакупки

15-20%

**Доля российских ОС в ИТ-инфраструктуре
заказчиков не превышает 20%**



№ 1 (253) | 2019

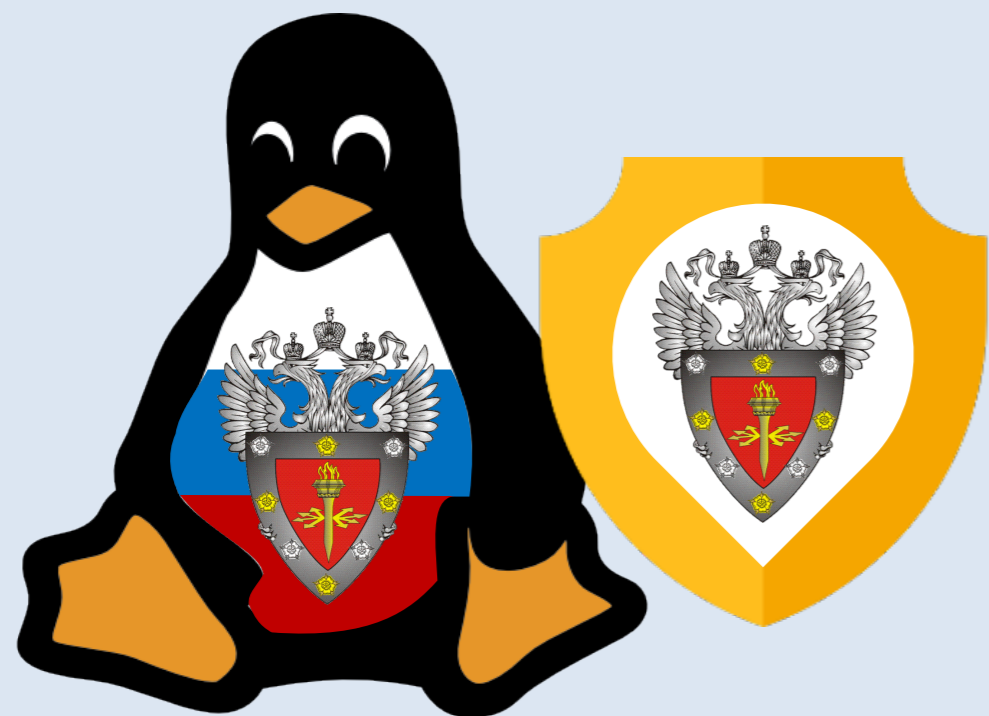
БЮЛЛЕТЕНЬ

Отчет о результатах экспертно-аналитического мероприятия «Мониторинг и оценка эффективности мер по импортозамещению в части осуществления закупок программного обеспечения для государственных и муниципальных нужд за истекший период 2018 года»

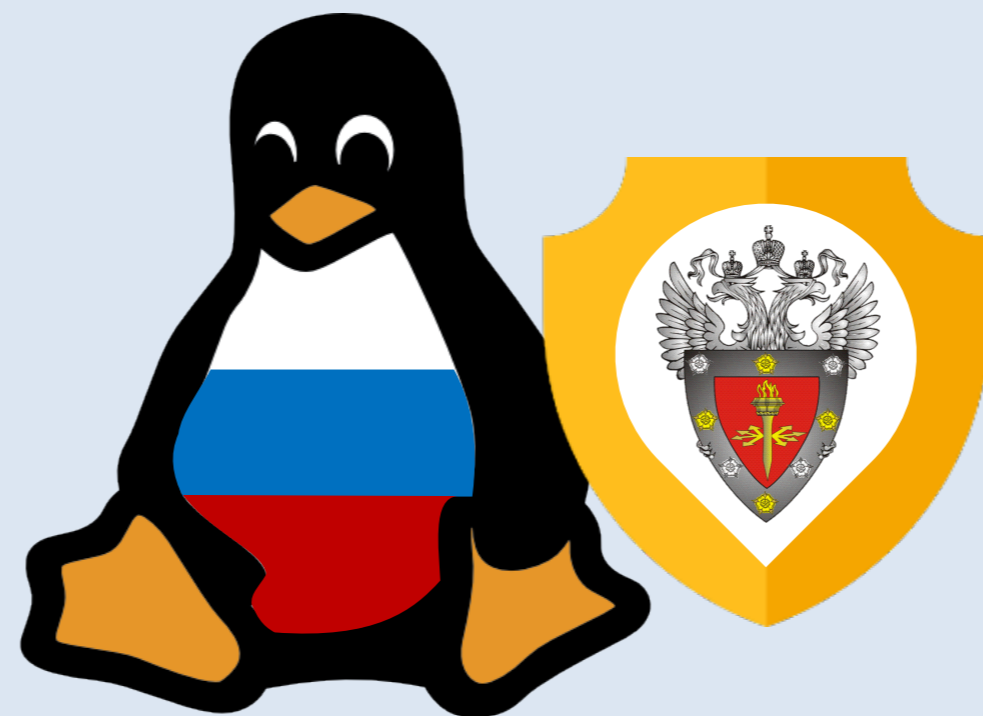
<http://audit.gov.ru/activities/bulleten/937/35754/>

«Реализация планов перехода на отечественное офисное программное обеспечение фактически не осуществляется»

Какая должна быть ИТ-инфраструктура заказчиков в результате импортозамещения

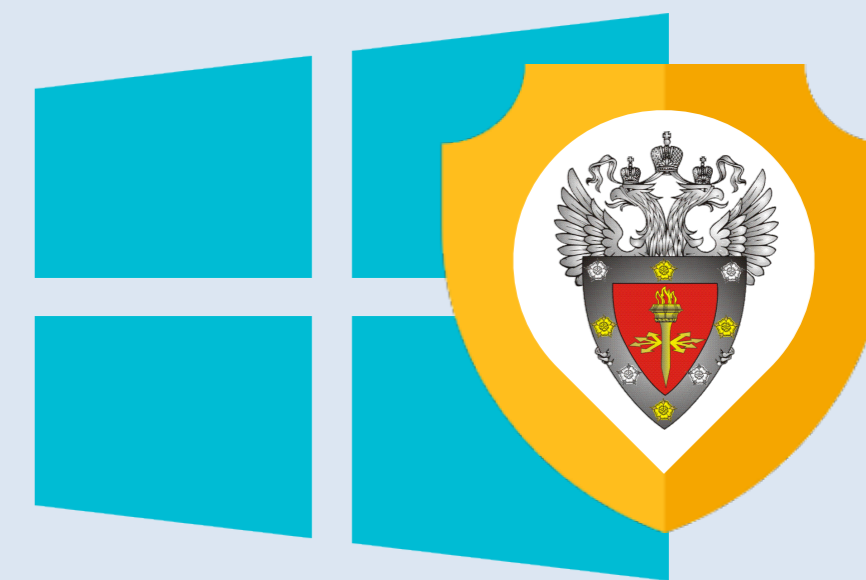


*Сертифицированные
отечественные ОС +
накладные СЗИ*



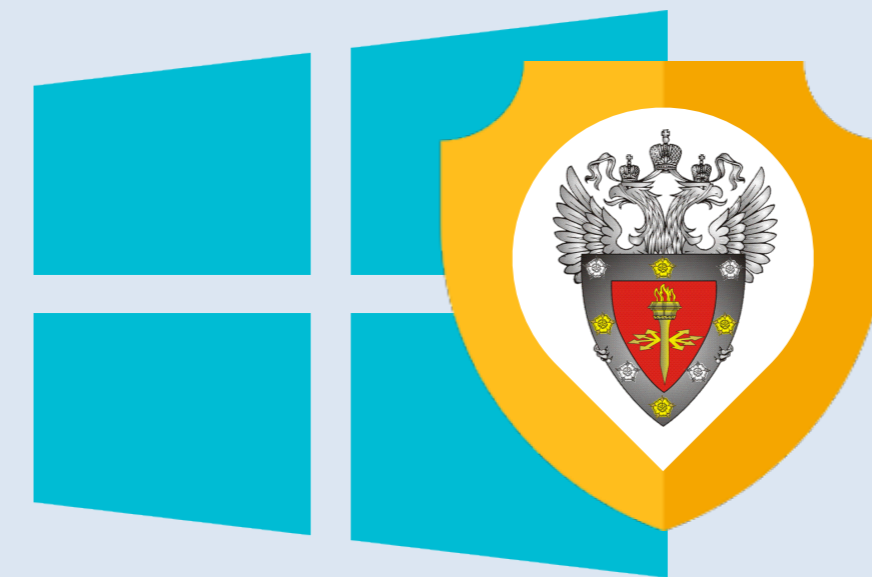
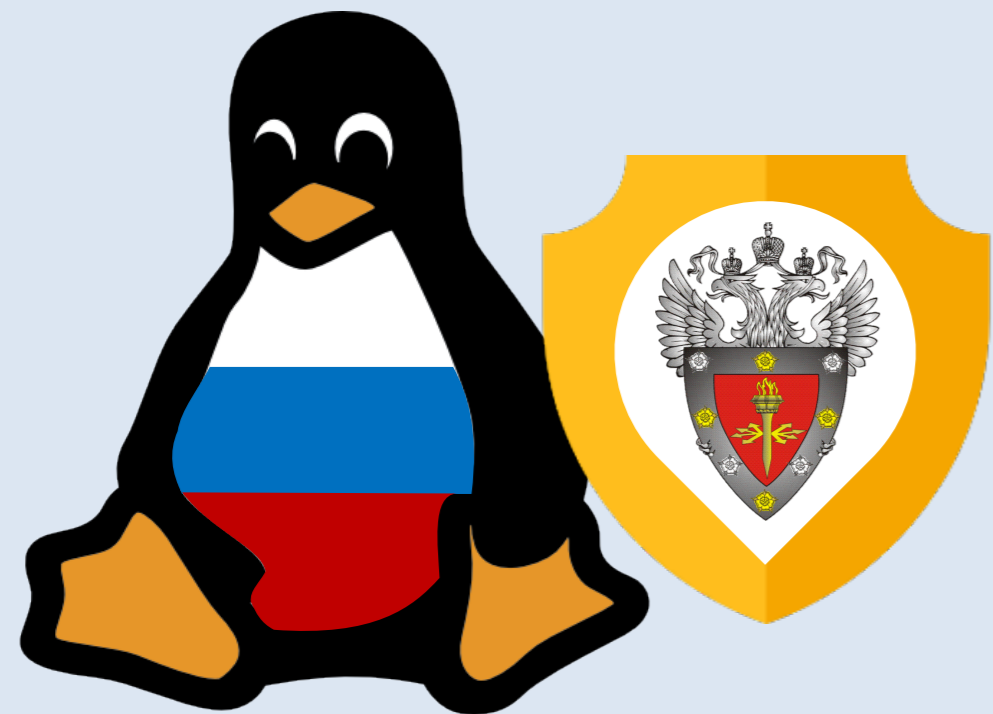
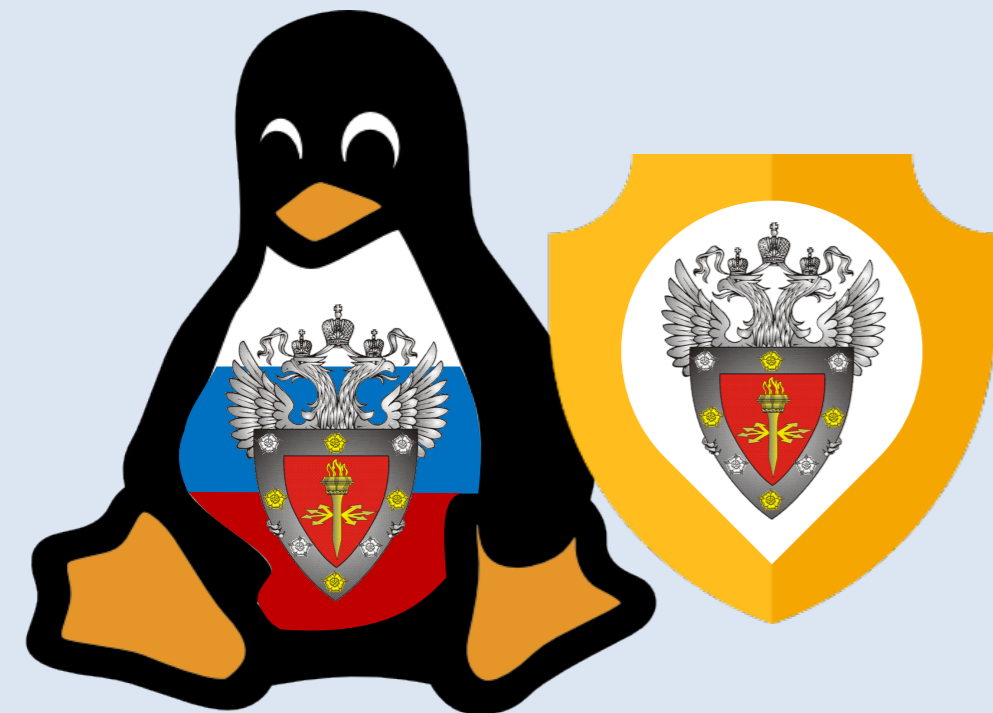
*Не сертифицированные
отечественные ОС +
накладные СЗИ*

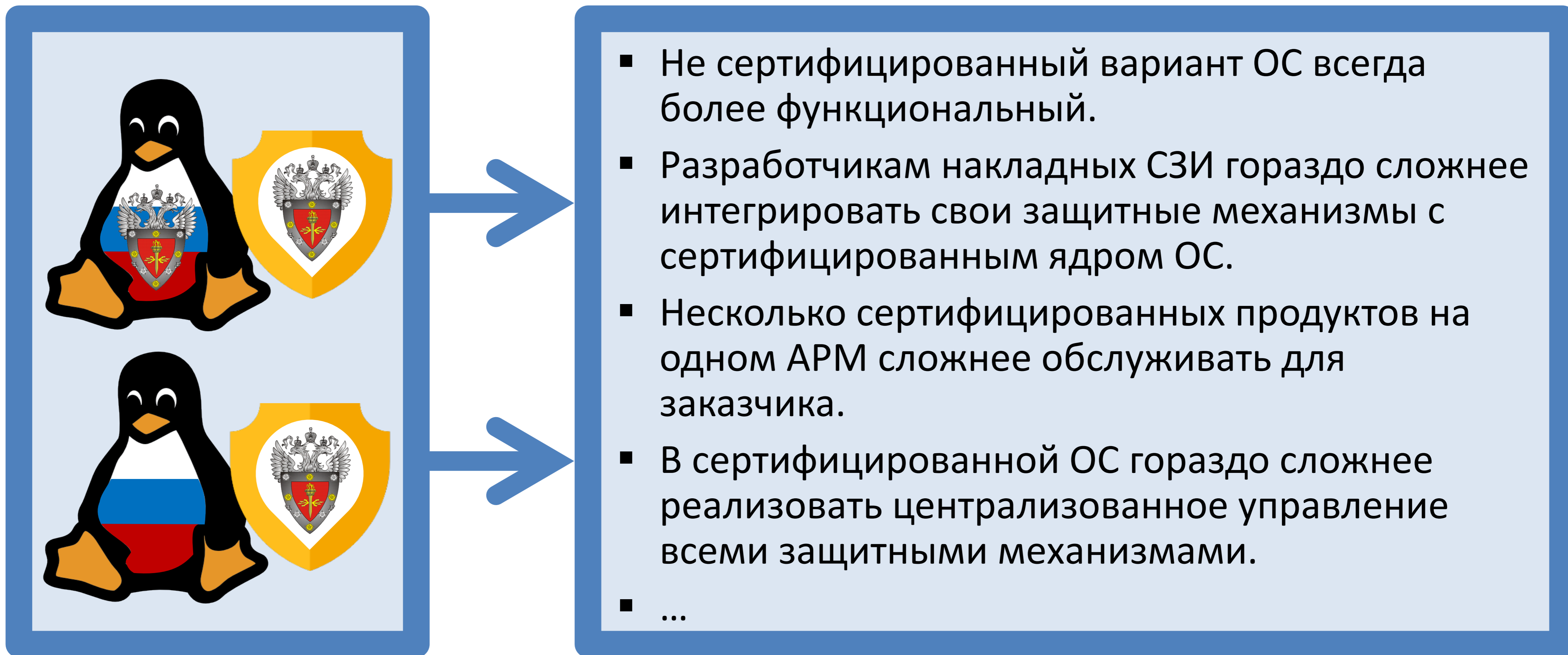
и/или



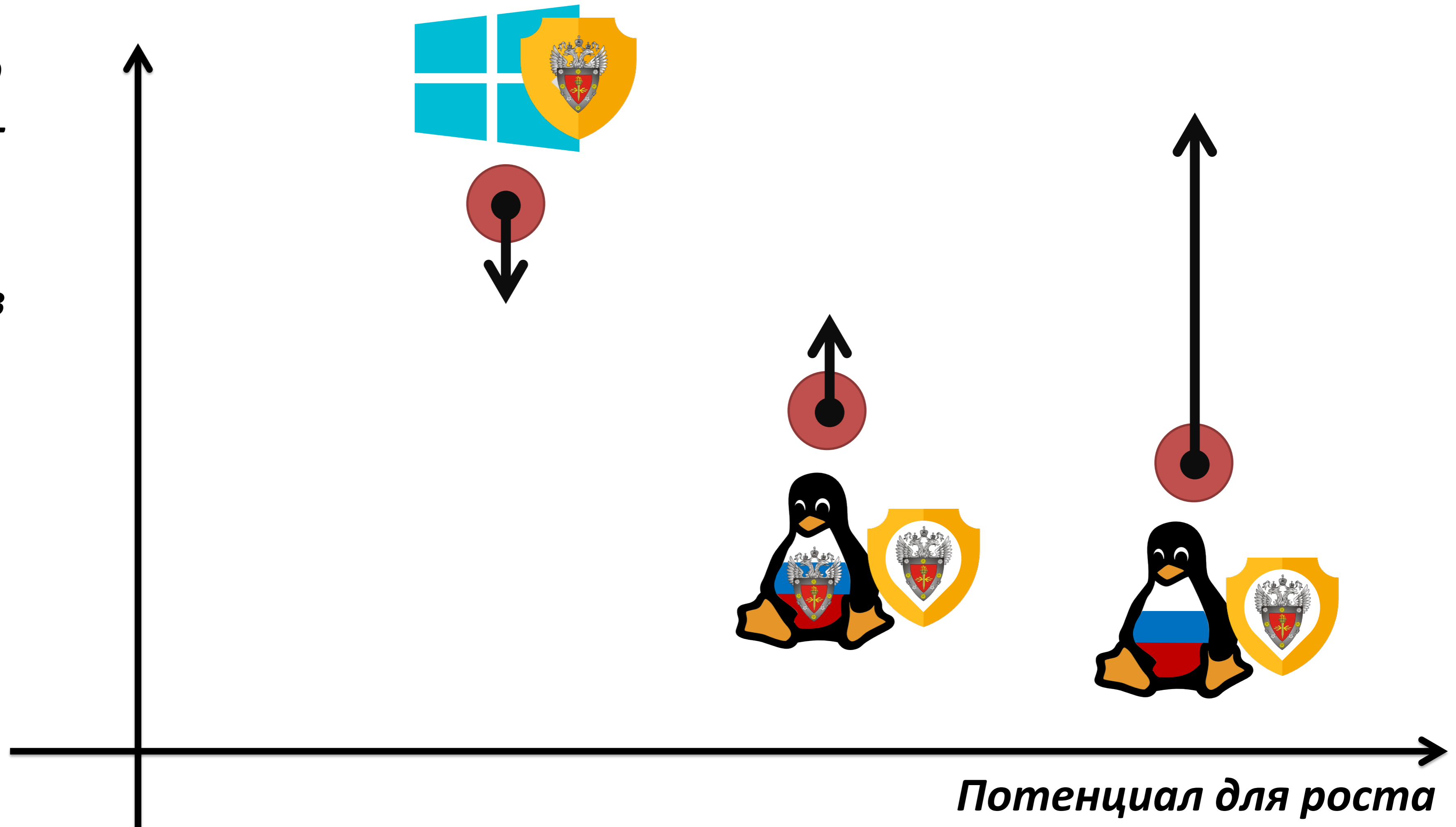
*ОС Windows +
накладные СЗИ*

ИТ-инфраструктура заказчиков на текущий момент





*Количество
сертифици-
рованных
защитных
механизмов*





Смогут ли разработчики сертифицированных ОС самостоятельно разработать все необходимые защитные механизмы?

[Главная](#) \ [Пресс-центр](#) \ [Новости](#)

Новости

Поиск подходящей платформы для импортозамещения продолжается

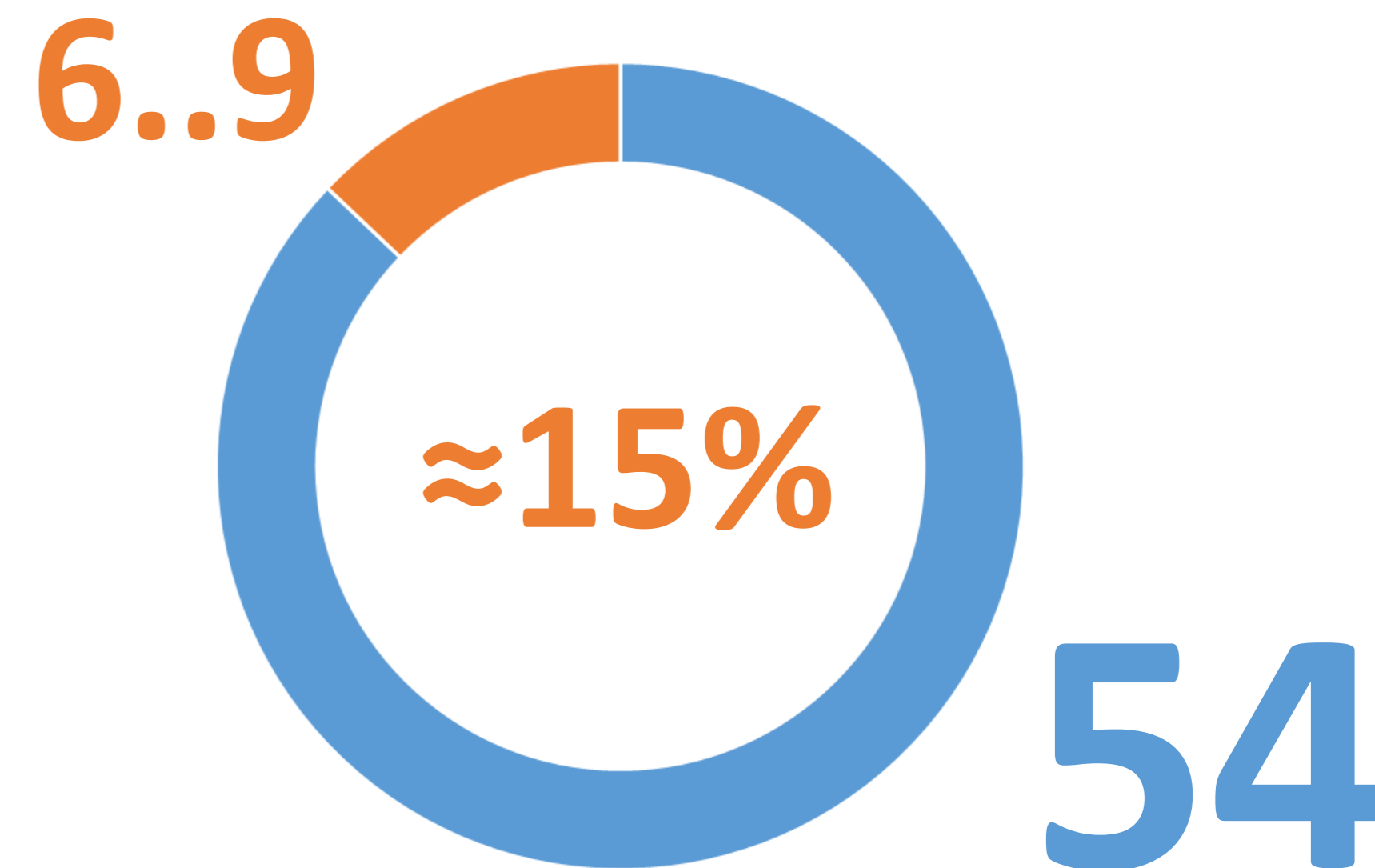
17 Декабря 2018  154  4 

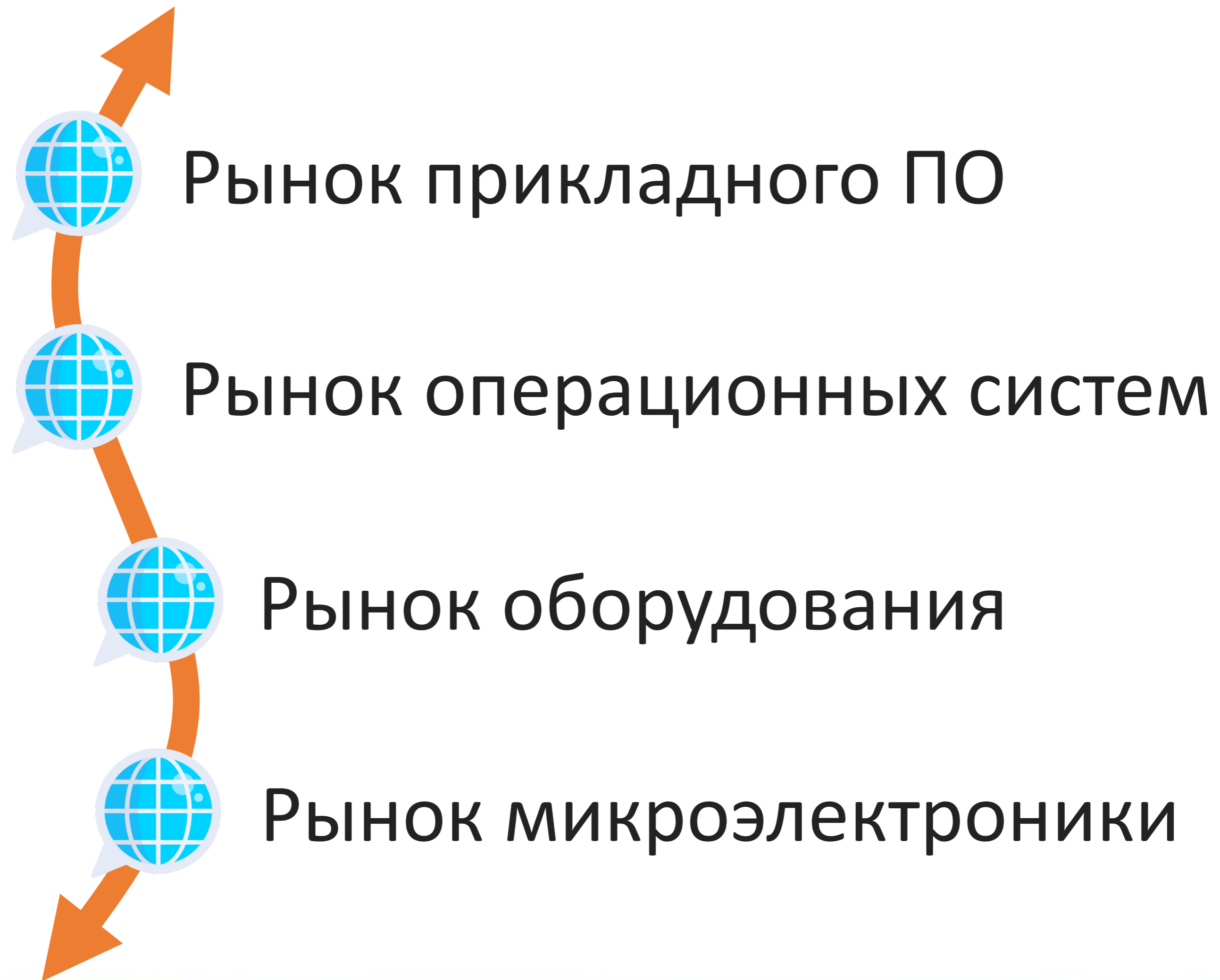
В минувшую пятницу в департаменте информационных технологий и связи было организовано [совещание](#) по выбору отечественной платформы (операционной системы) для реализации перехода исполнительных органов государственной власти Ямало-Ненецкого автономного округа и их подведомственных организаций на использование отечественного офисного программного обеспечения. В рамках совещания была сформирована комиссия по выбору отечественной платформы (Комиссия), в состав которой вошли представители исполнительных органов государственной власти Ямало-Ненецкого автономного округа и представители компаний-разработчиков, возглавил работу Комиссии директор департамента информационных технологий и связи автономного округа - Албычев Кирилл Сергеевич.

«было выявлено, что на сегодняшний день ни одна из представленных платформ не позволяет в полной мере работать с действующими региональными информационными системами»

<https://ditis.yanao.ru/presscenter/news/6551/>

Из 54-х критичных региональных информационных систем на ведущих отечественных платформах удалось успешно запустить от 6 до 9 информационных систем







Windows Vista™

Отзывы пользователей были плохими. Производители периферийного оборудования не поверили в то, что Windows Vista «взлетит», хотя в улучшение подсистемы безопасности было вложено порядка \$100 млн.

Ситуация с драйверами для принтеров оказалась плачевной. Их попросту не было. Никто кроме «них» не смог разработать драйверы. Проблема начала разрешаться только после того, как по всему миру было продано около полутора сотен миллионов лицензий.

И всё равно не взлетела... Windows Vista заняла первое место в конкурсе «Most Epic FAIL», проводимом *Pwnie Award*.

Некоторые ошибки являются уязвимостями

Статистика уязвимостей отечественного программного обеспечения

Распределение по производителям



Распределение уязвимостей по уровням опасности



Слайд из презентации
Заместителя начальника
отдела управления
ФСТЭК России
**Гефнер Ирины
Сергеевны.**

Конференция
**«Актуальные вопросы
защиты информации»**,
г. Москва,
13 февраля 2019 г.

«...нельзя абсолютизировать импортозамещение. Нельзя, чтобы импортозамещение у нас привело к какому-то критическому снижению эффективности других процессов»

<https://minsvyaz.ru/ru/events/38534/>



Носков Константин Юрьевич

Министр цифрового развития,
связи и массовых коммуникаций
Российской Федерации

Рынок российских ОС ещё только формируется. Его зрелости пока не хватает для появления большого количества накладных средств защиты информации под эти ОС.

2017-2019 годы посвящены пилотным проектам по импортозамещению. Текущие проблемы связаны с работоспособностью информационных систем и совместимостью ОС с периферийным оборудованием.

Ресурсов разработчиков ОС не хватает для создания полного набора сертифицированных защитных механизмов для удовлетворения потребностей рынка.

1

Проверяйте работоспособность своих систем.

2

Применяйте накладные решения. Это перспективно.

Что у нас есть на текущий момент



Dallas Lock Linux

сертифицированная система защиты информации накладного типа для защиты конфиденциальной информации.



Red Hat
Enterprise
Linux Server 7



CentOS 7



Fedora
20, 24*



Debian
7.8, 7.11*



OpenSUSE
12.3, 42*



Ubuntu
16.04*



Alt Linux
8*



Astra Linux
Common Edition Орёл*



Лотос
2.1*

Поддерживаются
наиболее популярные
Linux-дистрибутивы

Поддерживаются
русские ОС

* Реализовано и работает. Доступно после окончания процедуры инспекционного контроля.



Спасибо за внимание!

ЕВГЕНИЙ МАРДЫКО

Заместитель коммерческого директора
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

www.dallaslock.ru