ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
УЧРЕЖДЕНИЕ ТУЛЬСКОЙ ОБЛАСТИ
«ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Перспективы применения TLS-ГОСТ для защиты подключения к информационным системам

Худолей Ярослав Олегович

начальник отдела «Удостоверяющий центр»

государственного автономного учреждения Тульской области

«Центр информационных технологий»

ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

С 2012 года мы обеспечиваем работу и информационную безопасность сети правительства Тульской области и поддерживаем все ведомственные системы.

OPENREGION71.RU

РИС3

АИС КОНТИНГЕНТ

РСЭП

ГОСУСЛУГИ

РСЭД

Задачи организации доступа к ресурсам сети

Конфиденциальность
защита передаваемых сведений

Целостность
подтверждение подлинности информационного ресурса

Разграничение доступа
Полномочный доступ

Масштаб

РИСЗ

12 000

АИС КОНТИНГЕНТ

44 000

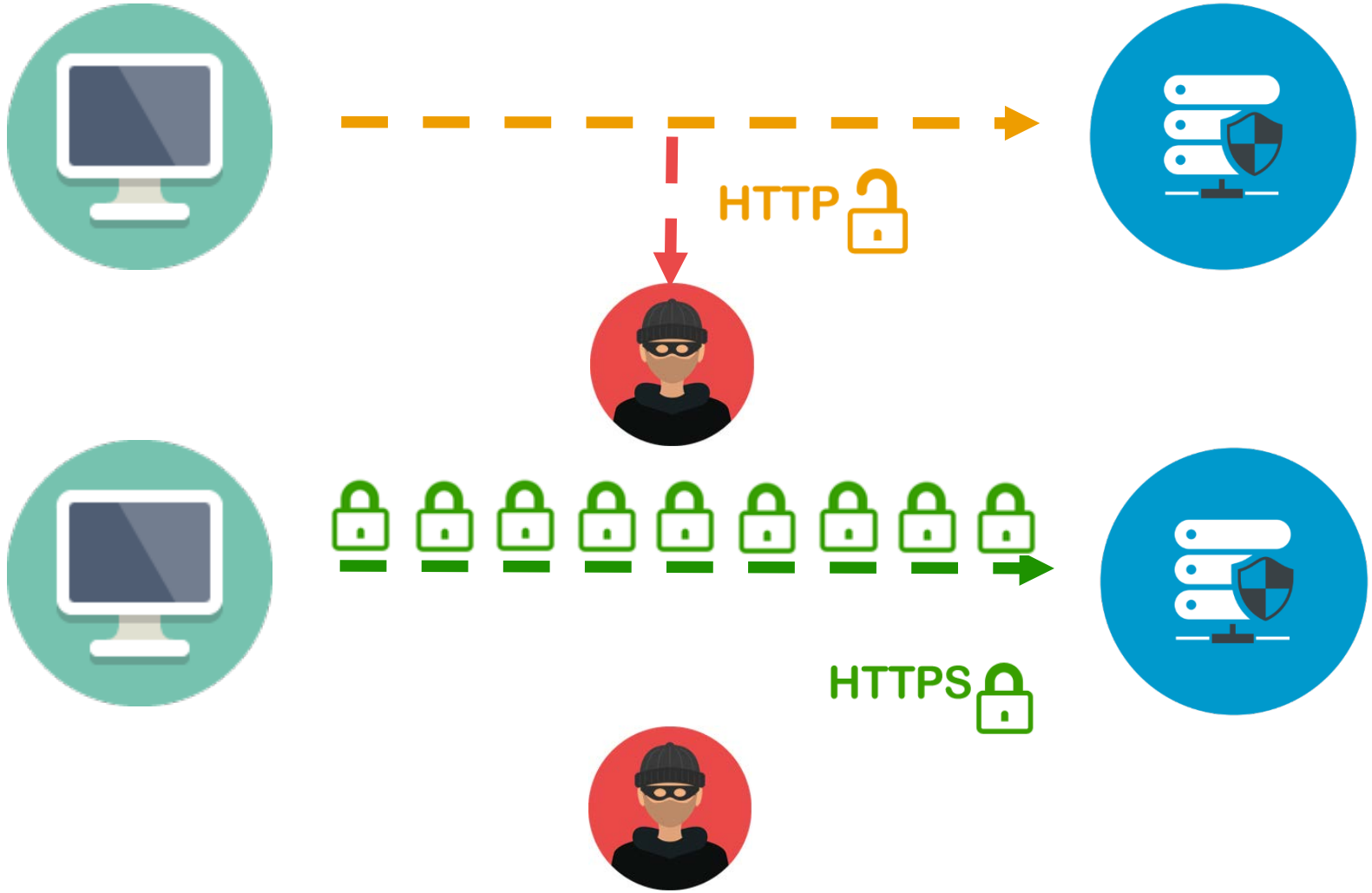
РСЭП

3 000

РСЭД

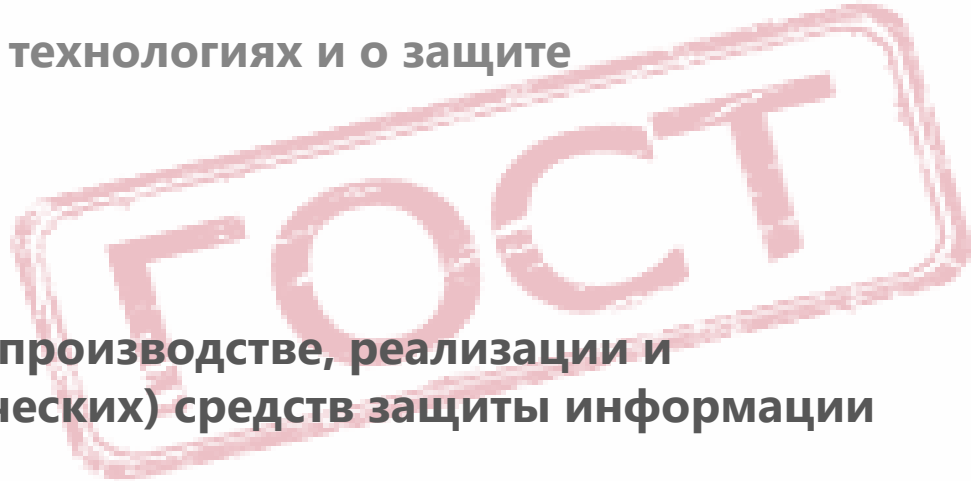
2 500

SSL/TLS



Требования

- **Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования**
- **149-ФЗ «Об информации, информационных технологиях и о защите информации»**
- **Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»**

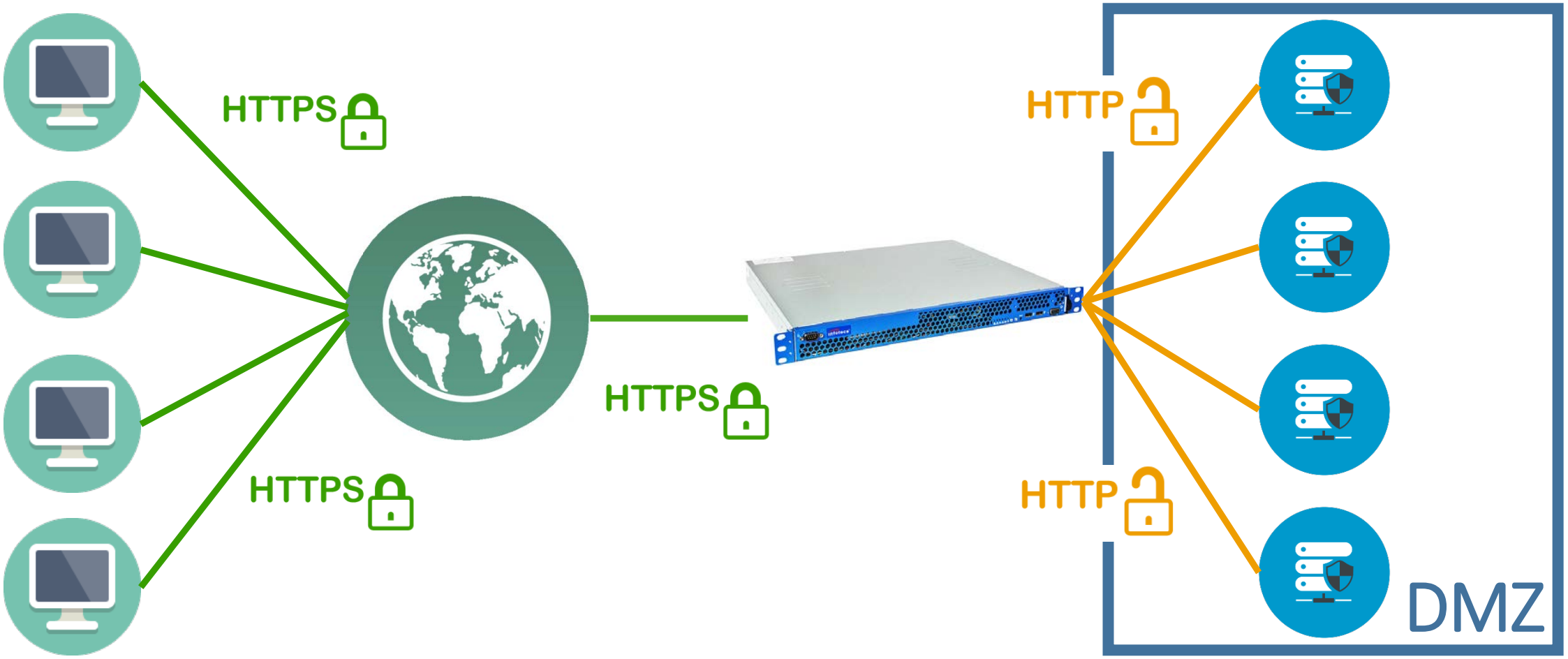


Встраивание СКЗИ в ИС

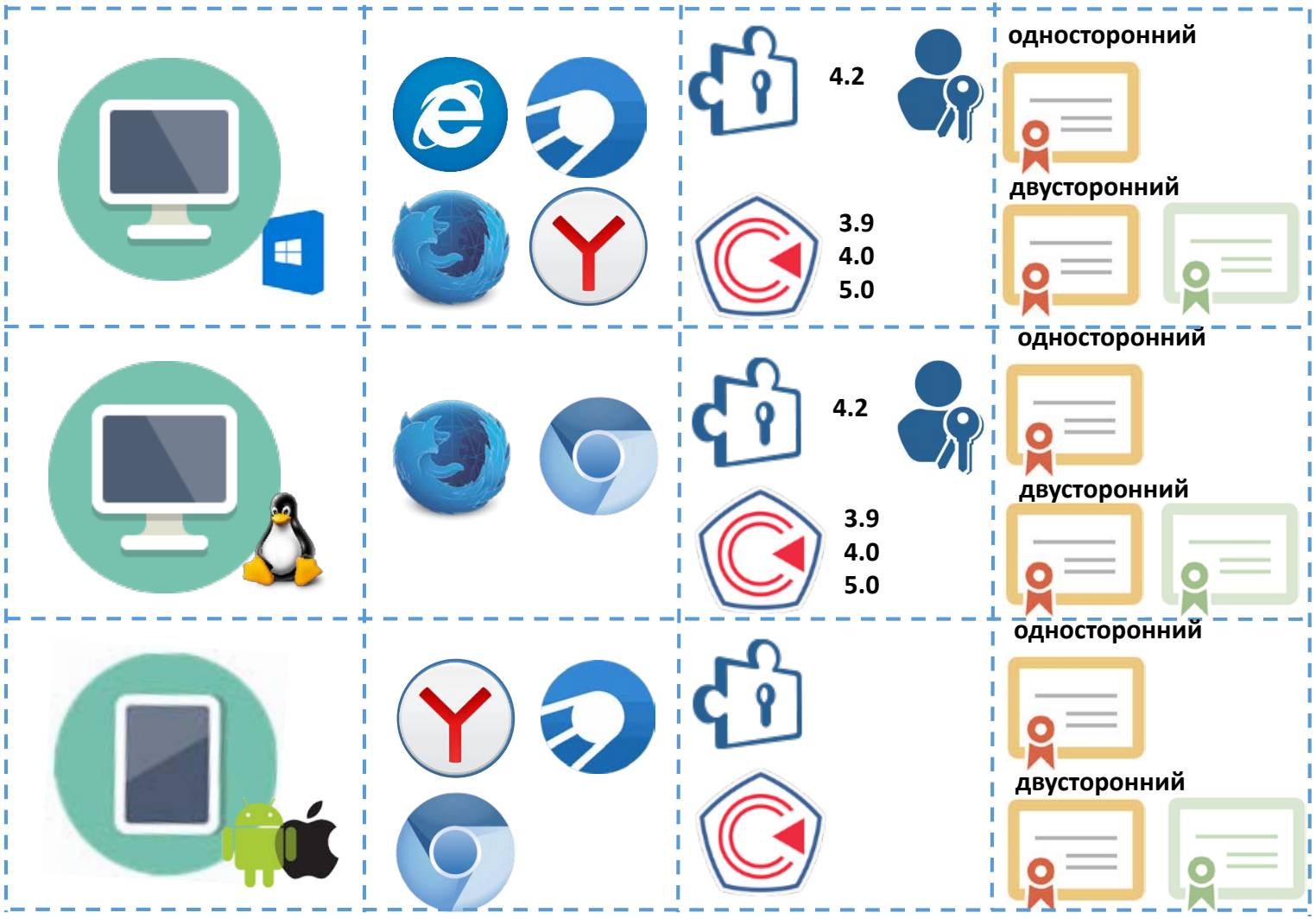
1. **Криптопровайдер ГОСТ**
2. **Выполнение требований эксплуатации СКЗИ**
3. **Доработка функционала ИС**
4. **Контроль встраивания**

- Дорого
- Долго
- Сложно администрировать

Криптошлюз



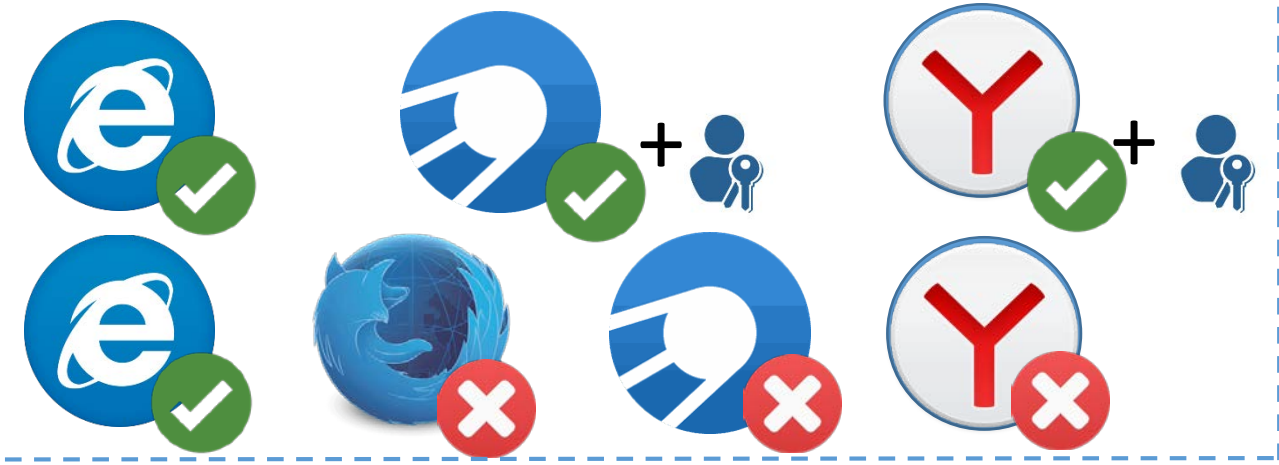
Кейсы

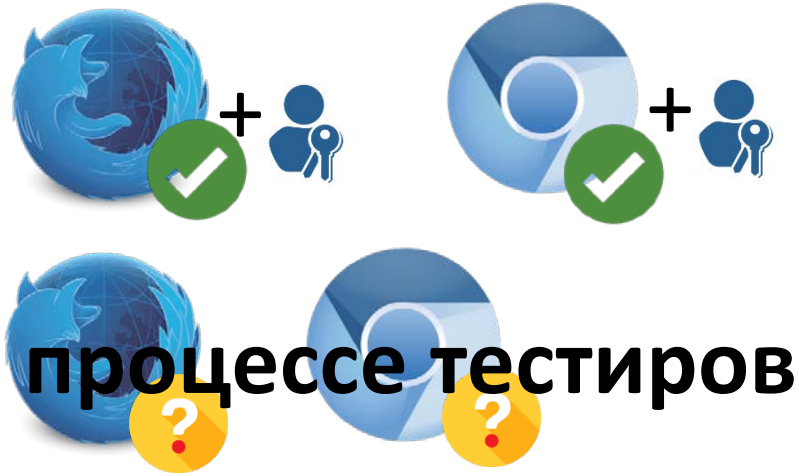

4.2
3.9
4.0
5.0
односторонний
двусторонний
4.2
3.9
4.0
5.0
односторонний
двусторонний
односторонний
двусторонний

TLS GATEWAY

Название исполнения	TLS 1000
Форм-фактор	ПАК (19” Rack 1U)
Предельная пропускная способность в режиме обратного HTTPS-прокси (Мбит/с)	до 680
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси	до 8900
Максимальное число внешних клиентов (сертификатов)	до 5000
Интерфейсы	4x Ethernet 10/100/1000

Результаты тестирования TLS Gateway





В процессе тестирования

Плюсы

- Интерфейс пользователя и администратора
- Автоматическая загрузка CRL доверенных УЦ
- Одновременная возможность работы с ГОСТ Р.34.10-2012 и Р.34.10-2001
- Сертификация (КС1,КС3)
- Возможность работы со сторонними браузерами с помощью PKI Client
- Отсутствие единого интерфейса управления кластером
- В настоящий момент отсутствует сертифицированный CSP для LINUX с функционалом TLS.

Предложения

- Централизованное управление
- Готовое решение для отечественных ОС
- Решение для мобильных ОС

— Вопросы?

— Спасибо за внимание!