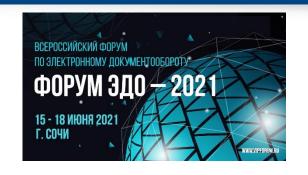




Ключевое слово в защите информации



«Развитие электронного документооборота. Тренды. Регулирование. Практика»

«Средства ЭП и защиты информации для применения в системах ЭДО»

Маслов Юрий Геннадьевич

Коммерческий директор

maslov@cryptopro.ru





Локальное средство ЭП

Традиционный сценарий

Сценарий коллективного рабочего места

Терминальный доступ

Криптосервер

Распределённое средство ЭП

Сервер формирования ЭП

Сервер создания электронной подписи







Локальное средство ЭП





Рабочее место пользователя





КриптоПро CSP











Привычно операторам и регуляторам

Риски работы с ключом создания ЭП перекладываются на пользователя

Использование средства ЭП и как средство шифрования



Квалификация пользователей

Зависимость от среды функционирования

Затратное обновление средств ЭП и ключевых носителей





Коллективное рабочее место



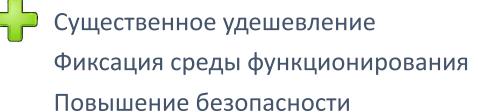


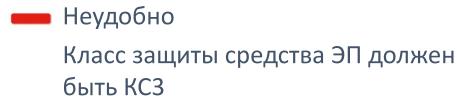








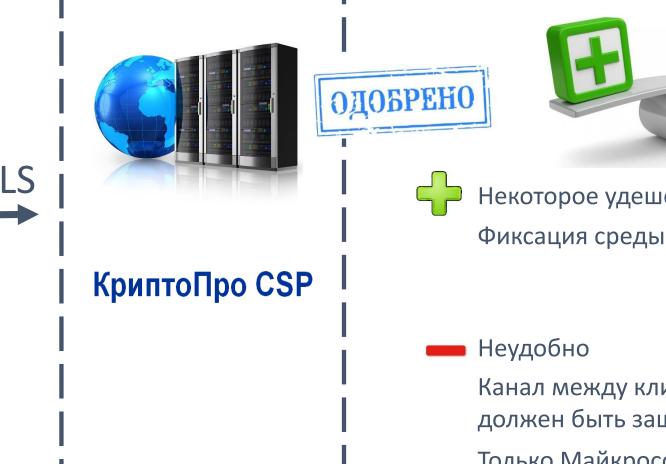








Тер<u>минальный се</u>рвер





Некоторое удешевление Фиксация среды функционирования

Канал между клиентом и сервером должен быть защищён по ГОСТ Только Майкрософт











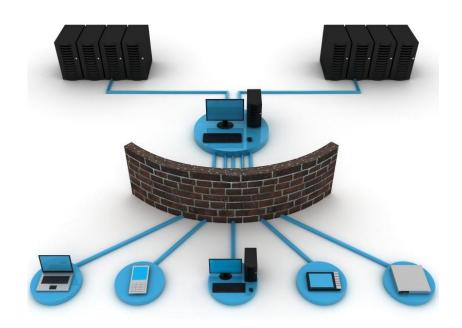


Грубое нарушение условий эксплуатации средств ЭП Нарушение конфиденциальности ключей создания ЭП









Распределённое средство ЭП















Сервер формирования ЭП КриптоПро DSS Lite





Почти любые среды функционирования

Любые браузеры Единая точка поддержки форматов

Передача больших документов в мобильные устройства
Невозможность подписания на изолированном устройстве









электронной подписи









Экономичность для больших систем (более 10 тысяч) Любая платформа и браузер Единая точка поддержки форматов

Аккуратное внедрение и позиционирование

Для КЭП только мобильная аутентификация



НЕТ решений, отвечающих требованиям, которые обеспечивают выполнение ч. 2) п.3.1 статьи 16 63-Ф3 «Об ЭП» (средств дистанционной (удалённой) ЭП для аккредитованных УЦ.







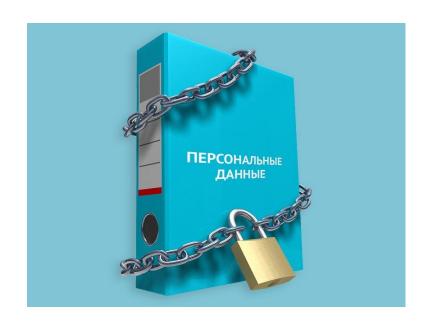
поэтому НЕВОЗМОЖНА аккредитация УЦ по пункту 3.1 статьи 16 63-Ф3







Ещё одно требование к ЭДО – шифрование информации, передаваемой по каналу связи







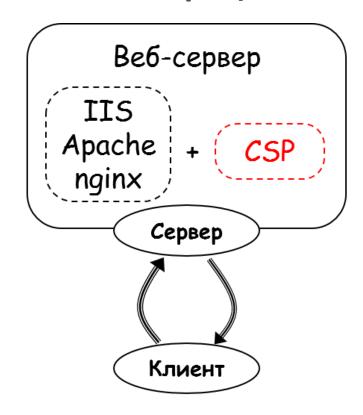
ГОСТ TLS – самая распространённая технология



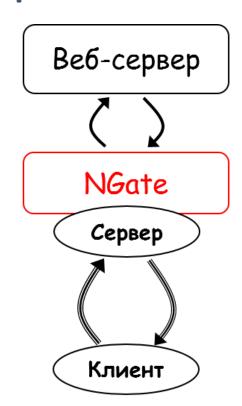




Вариант 1: Интеграция СКЗИ Вариант 2: Наложение СКЗИ



Криптография встроена в ПО

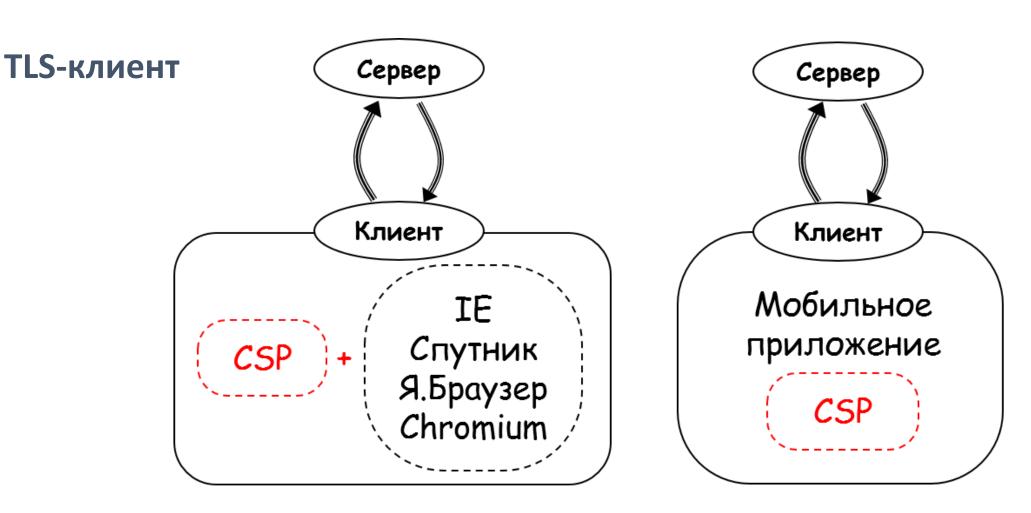


Криптография вынесена на отдельную аппаратную или виртуальную платформу









Ставим и пользуемся

Необходимо встраивание



В отличии от ЭП для защиты информации важен класс защиты СКЗИ

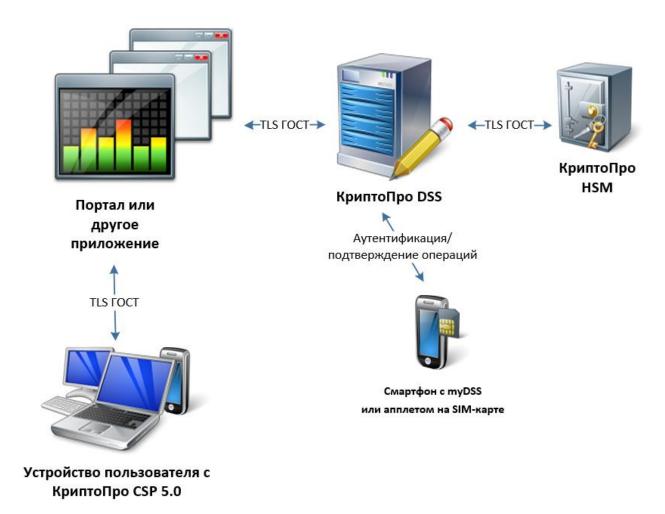
Решение	Платформа	Сертификация	Класс защиты
CSP + IIS	Windows	любая поддерживаемая версия CSP	KC1, KC2*, KC3*
CSP + Apache	Linux	начиная с CSP 5.0 R2	KC1, KC2*, KC3**
CSP + nginx	Linux	начиная с CSP 5.0 R2	KC1, KC2*, KC3**
NGate	Усиленная ОС на базе Linux Debian	самостоятельное СКЗИ	KC1, KC2, KC3

^{* –} требуются дополнительные настройки и технические средства защиты ** – КСЗ только под Astra Linux





В случае применения средства ЭП с централизованным созданием ЭП





Ключевое слово в защите информации



СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18

Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru



Общие вопросы: info@cryptopro.ru Контрактный отдел: kpo@cryptopro.ru Для дилеров: dealer@cryptopro.ru

