# Программно-аппаратные средства Web

## HTTPS, ЭЦП и ЭДО

Сергей Геннадьевич Синица

КубГУ, 2020

sin@kubsu.ru

# HTTPS

Transport Layer Security (TLS), Secure Sockets Layer (SSL)

RSA и AES, GOST2001, Кузнечник, Стрибог

Сертификат

Доверенная цепочка

Самоподписанный сертификат

Сертификационный центр

Клиентский сертификат

# ЭЦП

Ст.4 ФЗ “Об ЭЦП”: равнозначна собственноручной подписи в документе на бумажном носителе при условии, что сертификат ключа подписи этой ЭЦП не утратил силу на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписния.

Откреплённая или внедренная в документ

Простая (ПЭП) не позволяет проверить неизменность документа, только авторство подписи, в отличии от квалифицированной (КЭП) и неквалифицированной (НЭП)

Усовершенствованная (штамп времени)

# Использование ЭЦП

Электронные торги

Электронный документооборот (ЭДО)

Электронная отчетность

# Законы ЭЦП

Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (редакция 28.06.2014 с изм. и доп. вступ. в силу с 1.04.2015)

*Заменяет N 1-ФЗ от 10.01.2002*

Вводит понятие квалифицированной ЭЦП, в частности ее сертификат содержит СНИЛС, а использованное ПО сертифицированно на совместимость с ФЗ и ГОСТ.

# Законы ЭДО

Акты, накладные, договоры с 2002 г.

Приказ Минфина РФ от 25.04.2011 № 50н «Об утверждении порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи» – оператор ЭДО

Приказ ФНС России от 5 марта 2012 года № ММВ-7-6/* – форматы электронных счетов-фактур, книг покупок и продаж и журнала учета выставленных и полученных счетов-фактур

# ГОСТы

Алгоритм подписи:

- ГОСТ Р 34.10-94
- ГОСТ Р 34.10-2001 (+криптостойкость)
- ГОСТ Р 34.10-2012 (+криптостойкость, новый хеш)

Алгоритм хеширования:

- ГОСТ Р 34.11-94
- ГОСТ Р 34.11-2012

Алгоритм шифрования:

- ГОСТ Р 28147-89

# Криптография

(ввоз, применение, разработка, деятельность, вывоз)

Использовать “для себя” (юр. и физ. лицу) СКЗИ можно свободно.

Коммерческая деятельность требует лицензирования, а криптосредства – сертификации ФСБ.

Особый порядок ввоза криптостойких средств шифрования на территорию РФ требует лицензию Минпромторга (56 бит симметричное, 512 ассиметричное).

Постановление Правительства Российской Федерации от 16 апреля 2012 г. N 313 г. Москва требует лицензирования коммерческой деятельности в ФСБ в зависимости от криптостойкости.

Приказ ФСБ России от 9 февраля 2005 г. N 66 регулирует разработку и эксплуатацию криптосредств государством и дает рекомендации остальным.