Криптография для общества. Проблемы защиты с точки зрения обычных пользователей

Автор доклада: Дмитрий Малинкин,
Руководитель разработки браузера «Спутник»

Представляет: С.В. Смышляев, к.ф.-м.н.,
Директор по информационной безопасности ООО «КРИПТО-ПРО»

2018

Роль криптографии в жизни пользователей

Спутник

Криптография везде, но мало кто на это обращает внимания …

- *HTTPS:// (весь интернет)*
- *Telegram/Whatsapp/Viber/Skype …*
- *Opera VPN, Tor и т.п.*
- *А … ну да … теперь это еще и деньги (+ магия BlockChain)*

Что это все??? Какие протоколы, технологии, кто контролирует, кто гарантирует? – Никто?

Вернемся с старому доброму http://

Спутник

- **Есть стандарты**
- **Есть комитеты, которые эти стандарты утверждают**
- **Есть корпорации, которые эти стандарты внедряют**
  …
- **НО!**

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

ISO

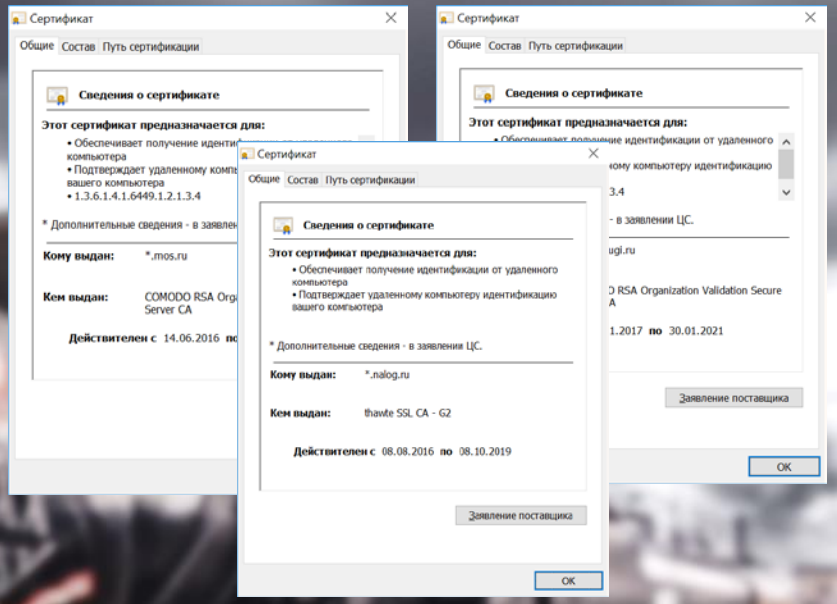
Спасибо Mr. Snowden !!!!!

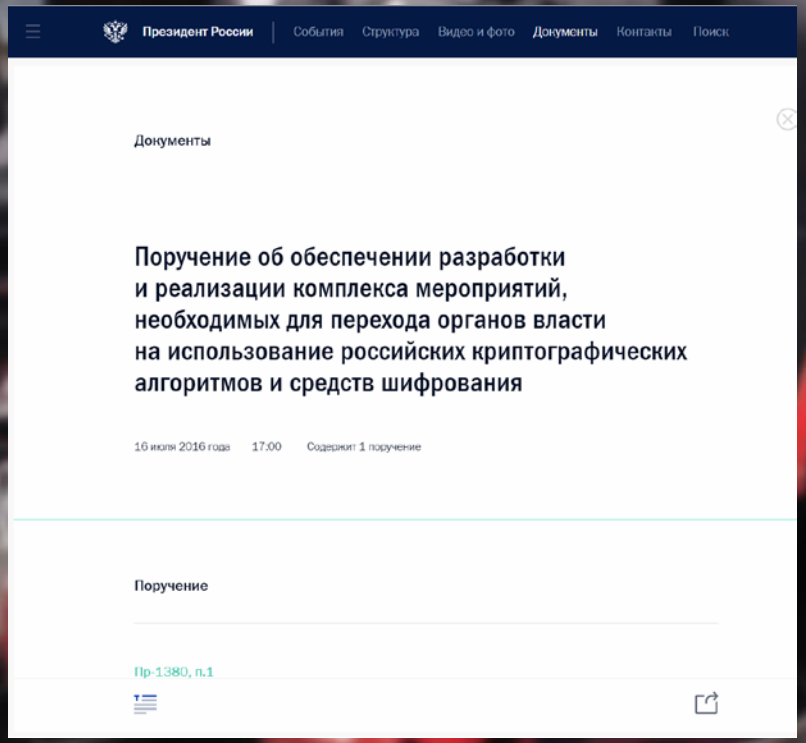
Как отмечает The New York Times, полученные от Сноудена документы свидетельствуют о том, что АНБ считает возможность расшифровывать информацию одним из своих приоритетов и «соперничает в этой области со спецслужбами Китая, России и других стран». «В будущем сверхдержавы будут появляться и приходить в упадок в зависимости от того, насколько сильными будут их криптоаналитические программы. Это цена, которую должны заплатить США чтобы удержать неограниченный доступ к использованию киберпространства», — цитирует газета документ АНБ от 2007 года.

Что делать то?

Спутник

- *А именно: зачем вообще что-то делать?*
- *И кто должен что-то делать?*



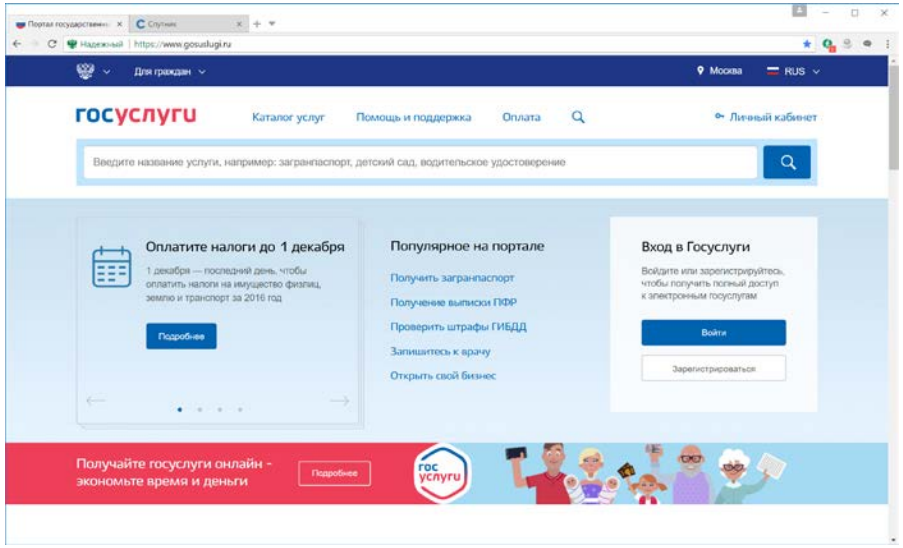


А если конкретно?

- *Внедрить поддержку отечественной криптографии на государственных ресурсах, обеспечивающих оказание государственных и муниципальных услуг*
- *Создать и распространить продукты, удобные и понятные пользователям*
- *Упростить получение технологии пользователями*
- *Стимулировать к использованию (в том числе и материально)*

Ну на самом деле уже кое-что делается …

- ***Разработан план мероприятий*** *(«дорожная карта») перехода в 2018 – 2019 годах федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления на использование российских криптографических алгоритмов и средств шифрования при электронном взаимодействии с гражданами и организациями*
- ***Проведен пилот на ЕПГУ***



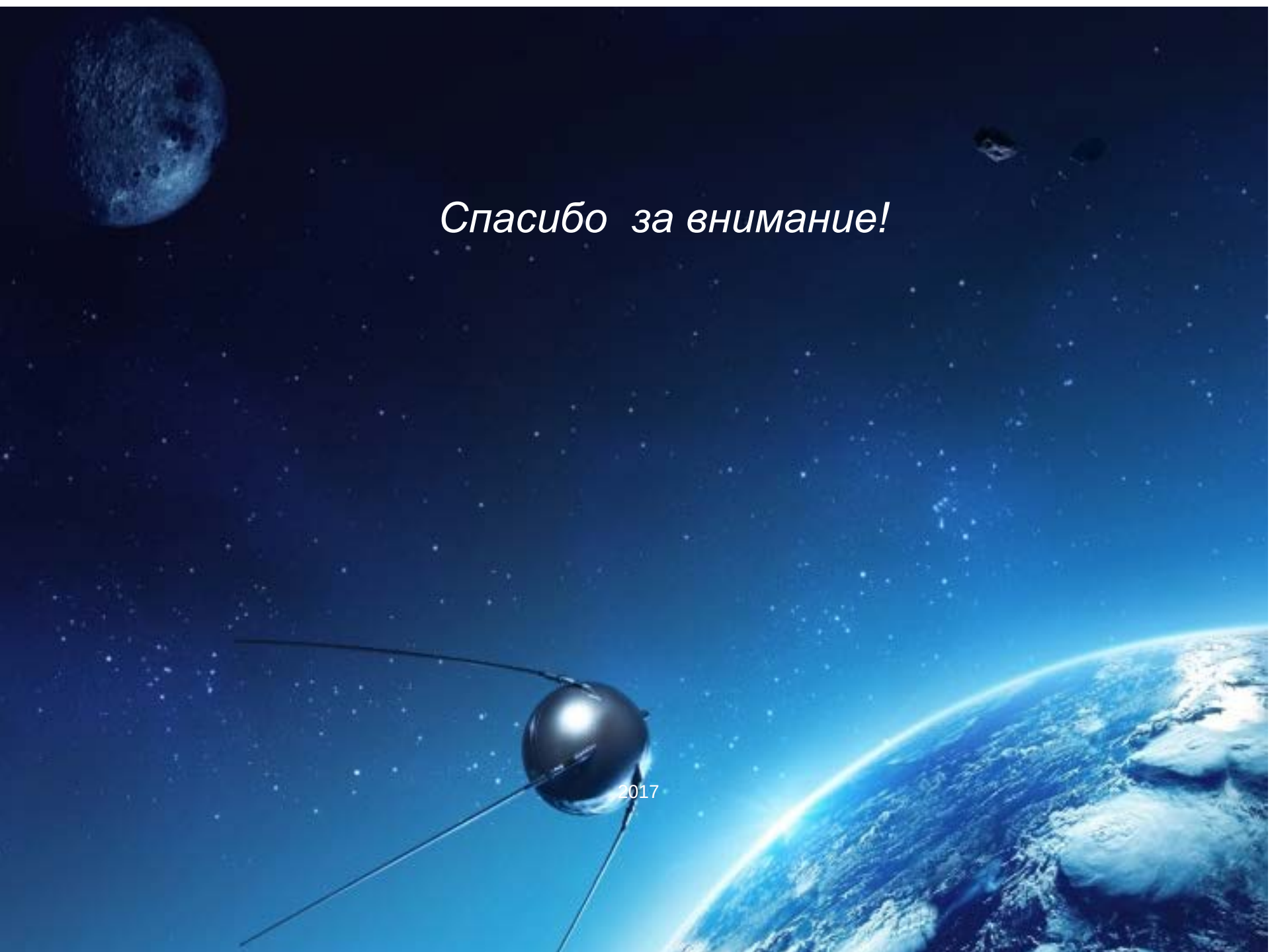
А как делать?

Спутник

«… нежно и ласково» (с)

- Принять простые и понятные правила (законодательства), в том числе определить правила для оборота ГОСТ-TLS сертификатов.
- Обязать гос. порталы, работающие с населением реализовать вариативность доступа.
- Предоставлять гос. сервисы для юридических лиц только и использованием доступа по ГОСТ.

- Дать гражданам удобные и понятные для них инструменты, которые бы вносили минимальное влияние в их повседневную жизнь
- Проводить массовую разъяснительную и агитационную политику
- Стимулировать использование именно российских средств, в том числе материально


Спасибо за внимание!
2017