Ассоциация РусКрипто

РусКрипто 2019

Ассоциация РусКрипто

Развитие информационных технологий

Ассоциация РусКрипто

Развитие информационных технологий

Ассоциация РусКрипто

Киберпреступность

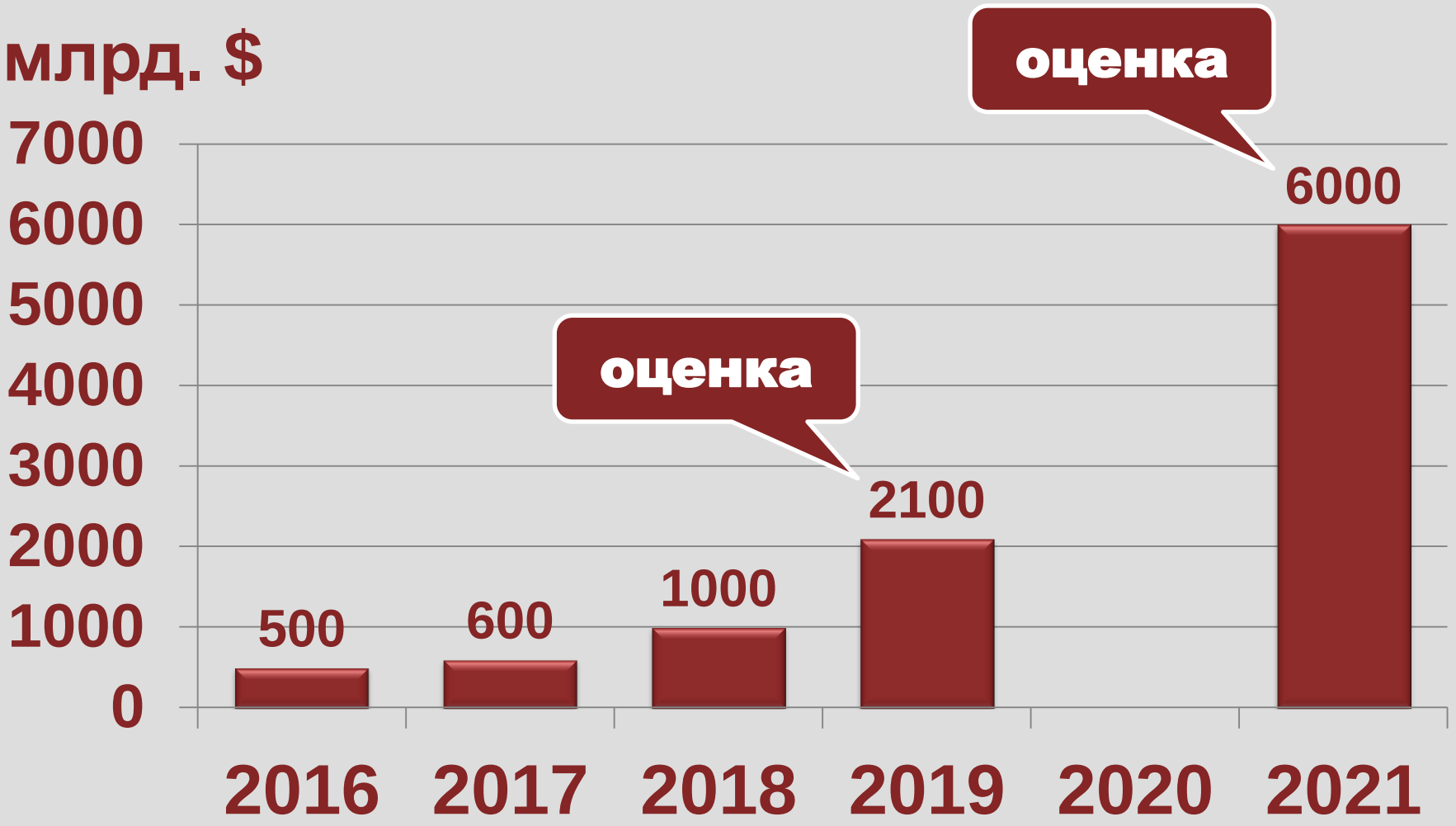
- Каждые 39 секунд в мире происходит кибератака.

- В 2016 г. по числу ***объявленных*** преступлений – киберпреступления были на 2-м месте.

Ассоциация РусКрипто

Потери от киберпреступности в мире

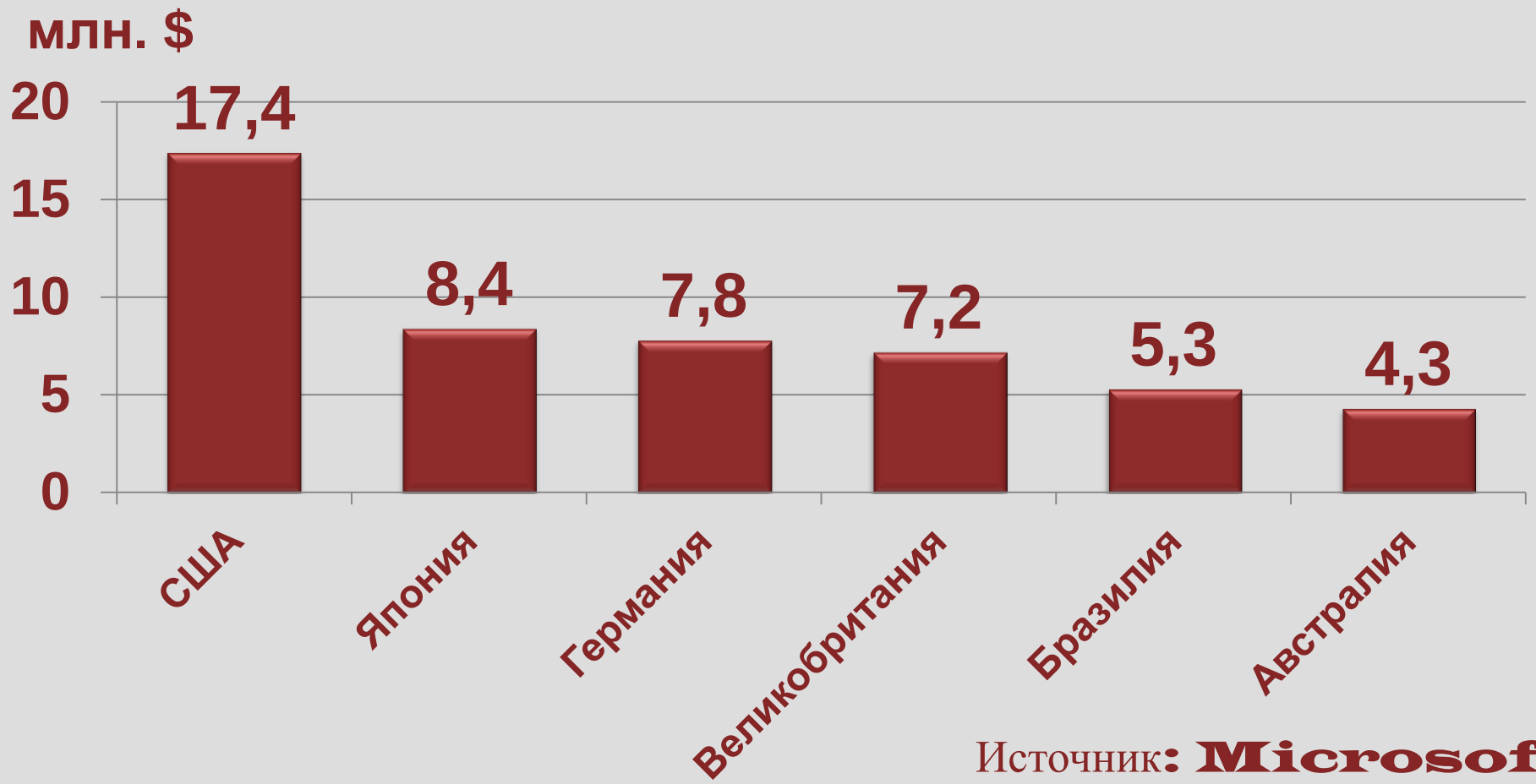
Источник: Microsoft



Ассоциация РусКрипто

Средние потери от одной кибератаки

$3.8 млн. – средние потери от одной кибератаки для бизнеса (2018).



Источник: Microsoft

Ассоциация РусКрипто

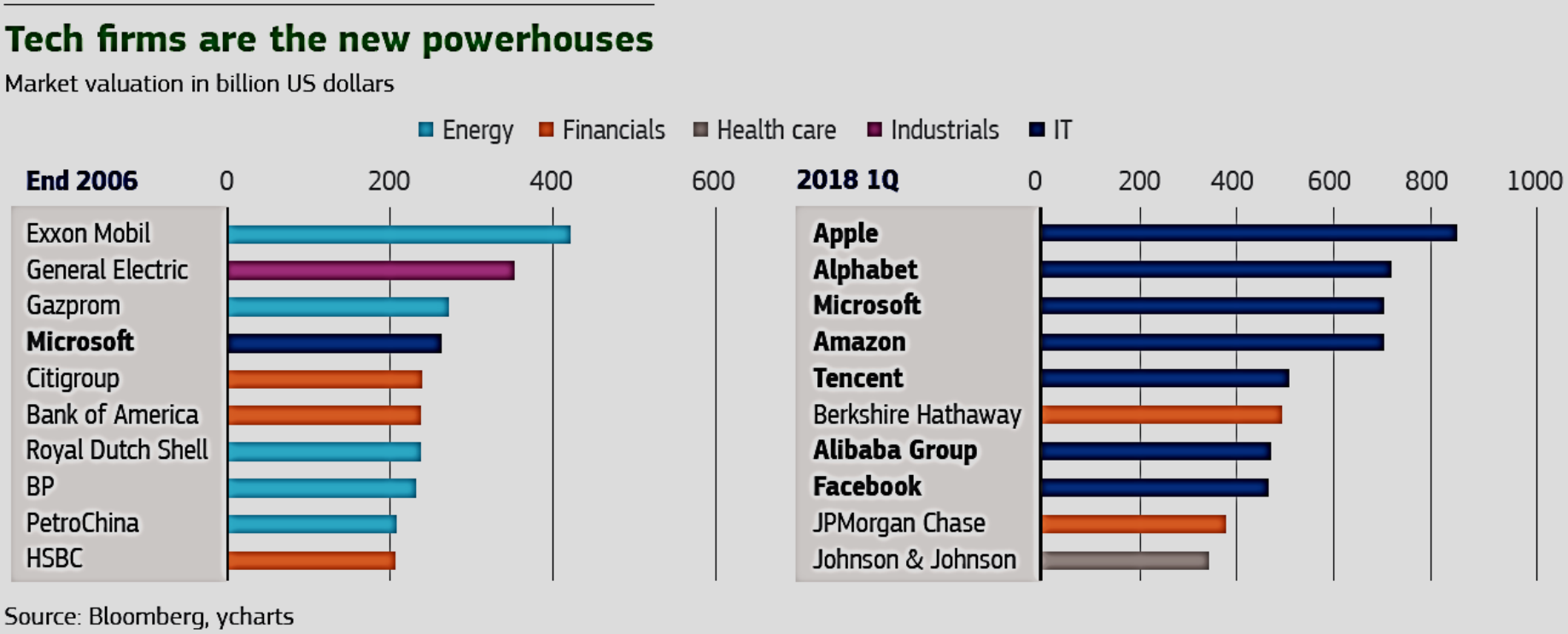
Киберпреступность

- **$3.8 млн. – средние потери от одной кибератаки для бизнеса в 2018 г.**
- **$150 млн. – оценка средних потерь от одной кибератаки для бизнеса в 2020 г.**
- **$530 млн. – потери от самой дорогостоящей на сегодняшний день кибератаки – январь 2018 г. (*Time Money*)**

При этом бóльшая часть компаний предпочитает не сообщать о своих потерях.

Ассоциация РусКрипто

Развитие информационных технологий



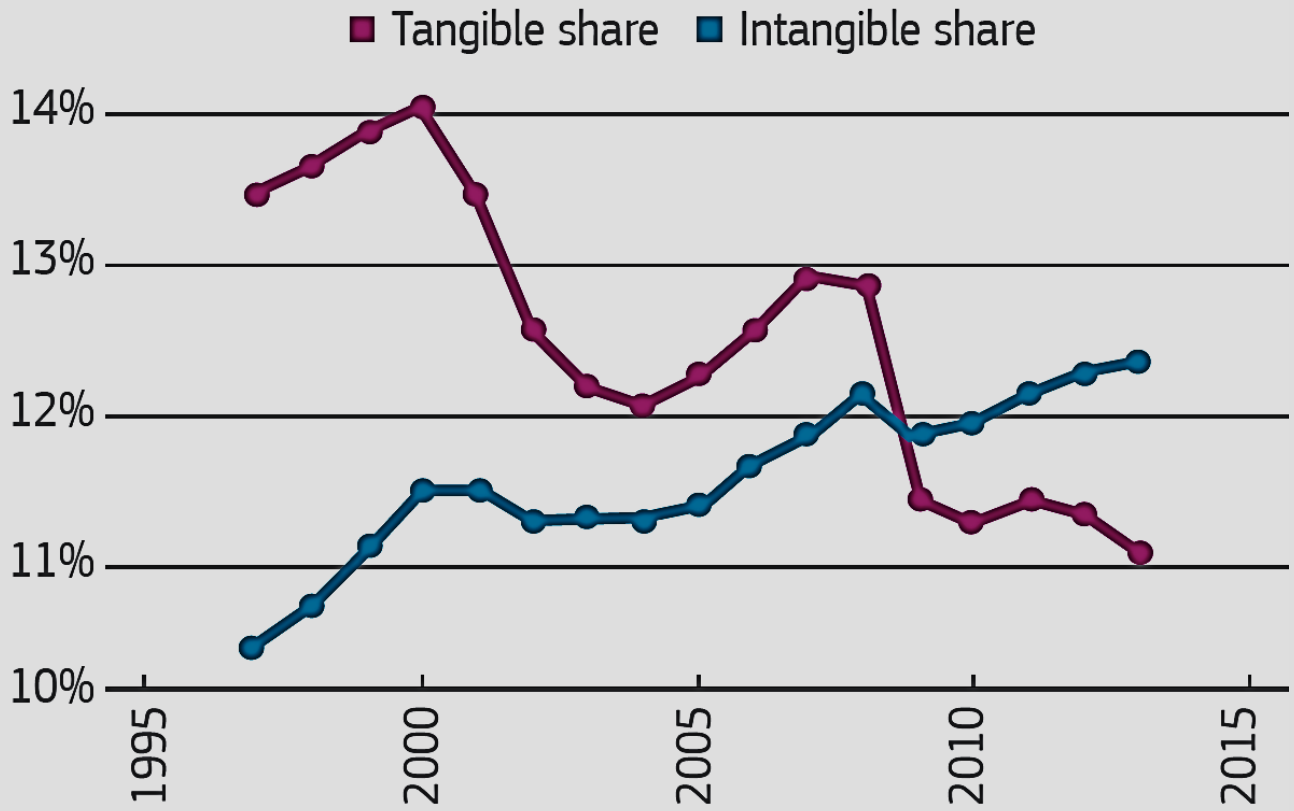
Источник: Bloomberg

Ассоциация РусКрипто

Развитие информационных технологий

Intangible investments have overtaken tangibles

Share of GDP, US+EU11, whole economy

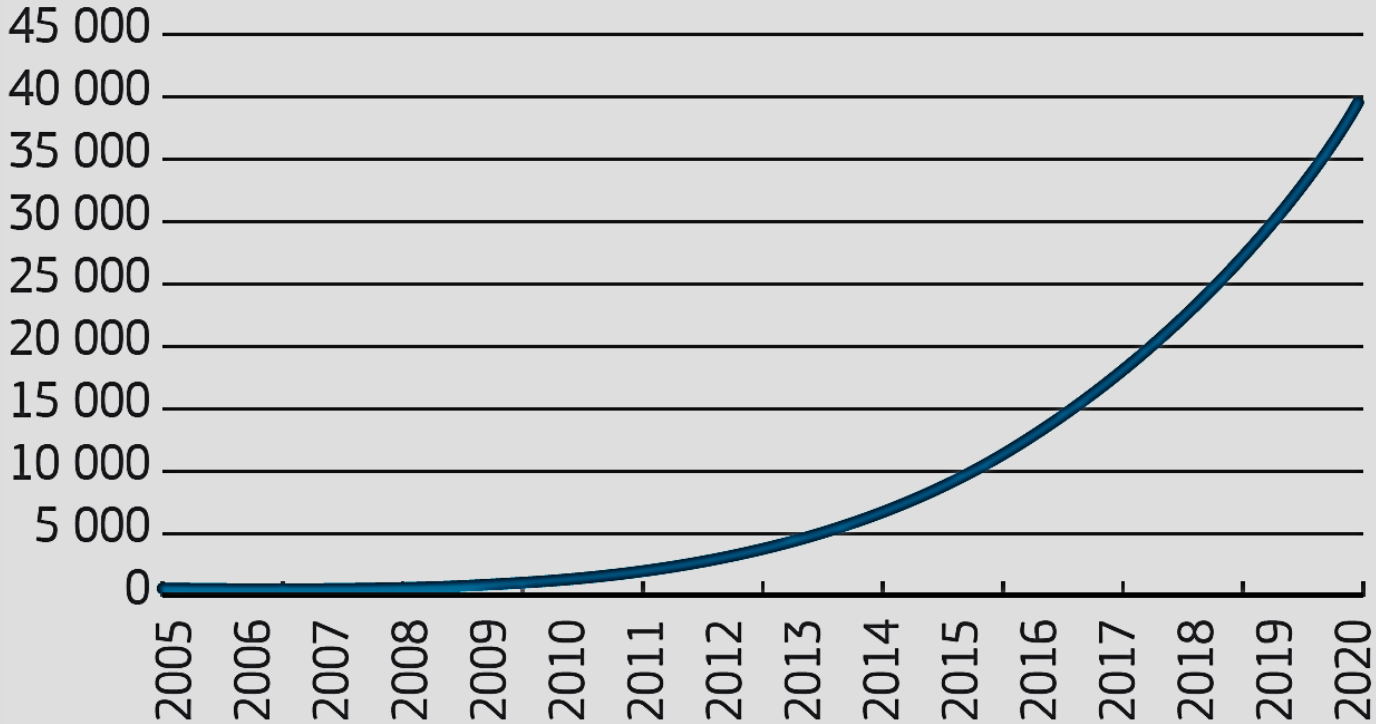


Ассоциация РусКрипто

Развитие информационных технологий

Global explosion of data fuels new innovation paradigm

Worldwide data storage in exabytes (=2^{60} – миллиард Гб.)



Source: Internation Data Corporation Digital Universe Study

Ассоциация РусКрипто

Киберпреступность

- За 2015 г. было похищено более 500 млн. персональных данных.
- В среднем за день похищается 3,809,448 персональных данных:
  - 158,727 в час
  - 2,645 в минуту
  - 44 в секунду

Cybersecurity Ventures

Ассоциация РусКрипто

Развитие информационных технологий

JAN 2018

DIGITAL AROUND THE WORLD IN 2018

KEY STATISTICAL INDICATORS FOR THE WORLD'S INTERNET, MOBILE, AND SOCIAL MEDIA USERS

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
7.593 BILLION	4.021 BILLION	3.196 BILLION	5.135 BILLION	2.958 BILLION
URBANISATION: 55%	PENETRATION: 53%	PENETRATION: 42%	PENETRATION: 68%	PENETRATION: 39%

we are social

we are social

SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. **NOTE:** PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).

Hootsuite™

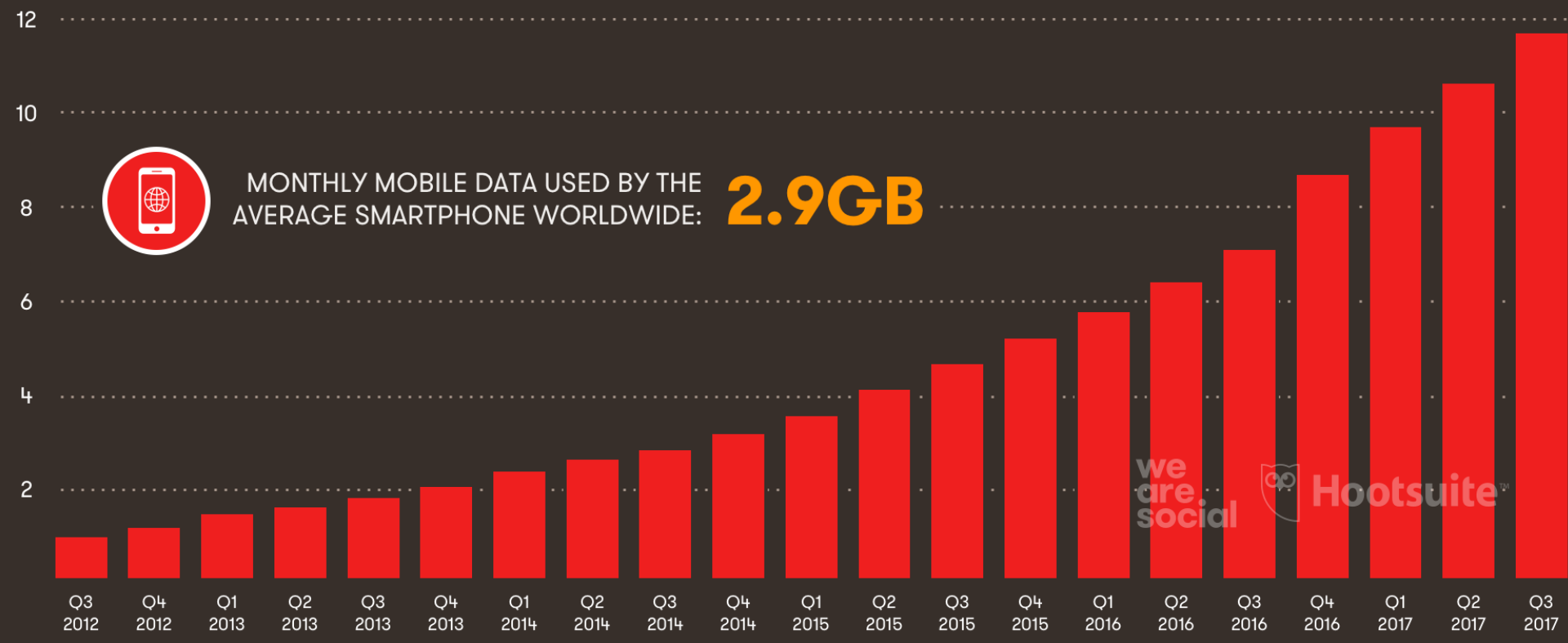
Ассоциация РусКрипто

Развитие информационных технологий

JAN 2018

GLOBAL MOBILE DATA GROWTH

TOTAL MONTHLY GLOBAL MOBILE DATA TRAFFIC (UPLOAD & DOWNLOAD), IN EXABYTES (BILLIONS OF GIGABYTES)



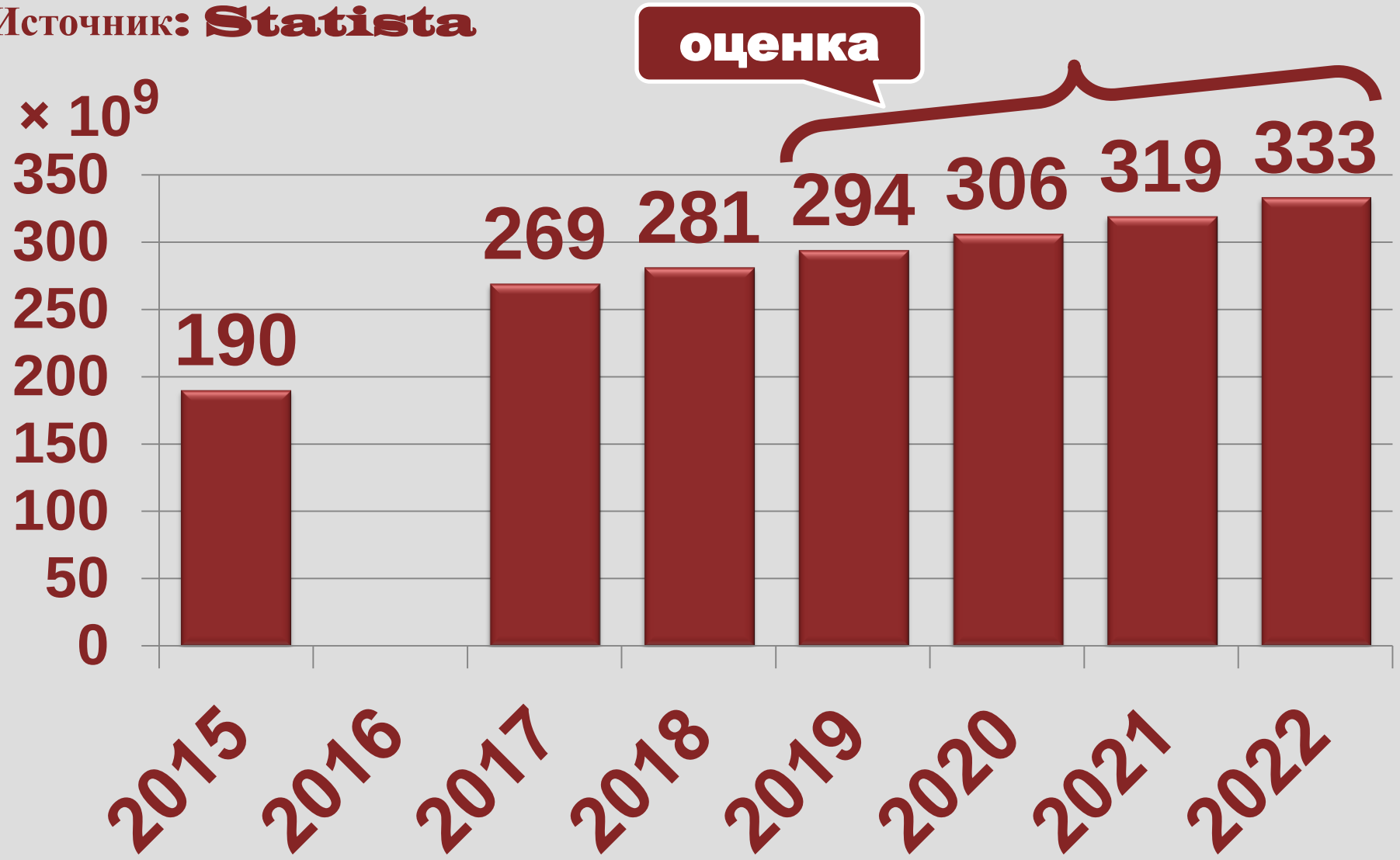
SOURCE: ERICSSON MOBILITY REPORT, NOVEMBER 2017.

Hootsuite™

Ассоциация РусКрипто

Количество электронных писем, отправляемых в 1 день

Источник: Statista



Ассоциация РусКрипто

E-mail Traffic

По оценке Statista 2,3% электронных писем содержат вредоносные вложения.

Ассоциация РусКрипто

Смартфоны и мобильные устройства

JAN 2018

SHARE OF WEB TRAFFIC BY DEVICE

BASED ON EACH DEVICE'S SHARE OF ALL WEB PAGES SERVED TO WEB BROWSERS

LAPTOPS & DESKTOPS	MOBILE PHONES	TABLET DEVICES	OTHER DEVICES
43%	52%	4%	0.14%
YEAR-ON-YEAR CHANGE: -3%	YEAR-ON-YEAR CHANGE: +4%	YEAR-ON-YEAR CHANGE: -13%	YEAR-ON-YEAR CHANGE: +17%

SOURCE: STATCOUNTER, JANUARY 2018 AND JANUARY 2017.

Hootsuite™

Ассоциация РусКрипто

Смартфоны и мобильные устройства

- По оценкам Ericsson, к концу 2020 г. будет 6.4 млрд. пользователей смартфонов – практически все население Земли (в 2018 г. – 5.1 млрд. – 68%).
- Вычислительные возможности современного смартфона превосходят вычислительные возможности всего оборудования Space Shuttle.

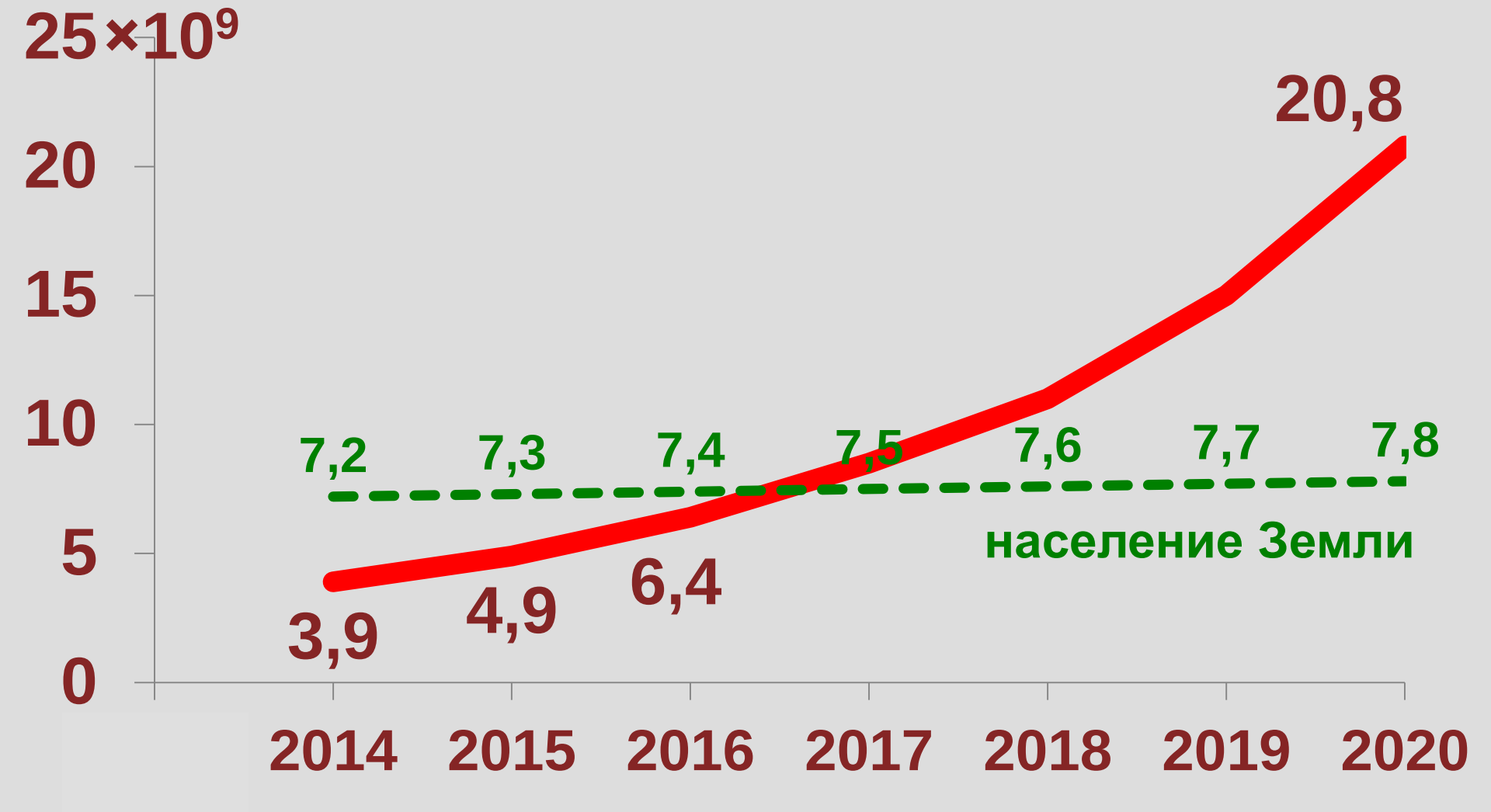
Приложения Apple Pay, Samsung Pay и Android Pay делают смартфоны весьма привлекательным объектом для кибератак.

Ассоциация РусКрипто

Internet-of-Things

Ассоциация РусКрипто

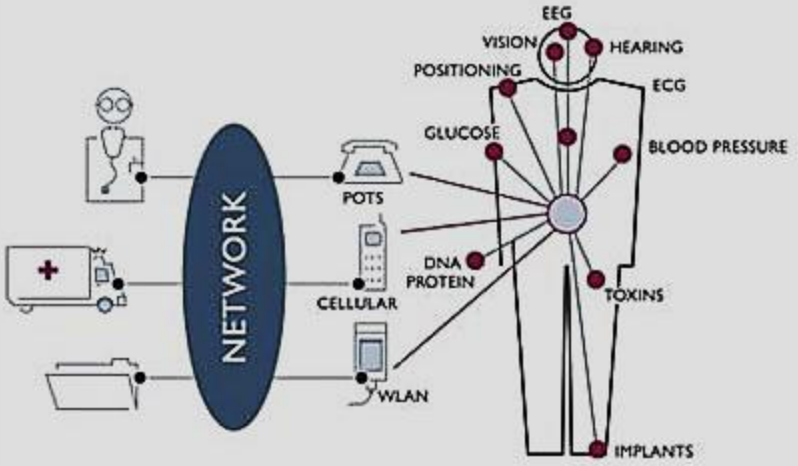
Internet-connected Things



Ассоциация РусКрипто

Киберпреступность

- С 2016 по 2017 г.г. число кибератак через IoT-устройства выросло в 6 раз.
  - Cars.
  - Smart home devices.
  - Medical devices.
  - Smart TVs.
  - Embedded devices.



- По оценке Gartner к 2020 г. 25% кибератак будут производиться через IoT-устройства

Ассоциация РусКрипто

Global eCommerce

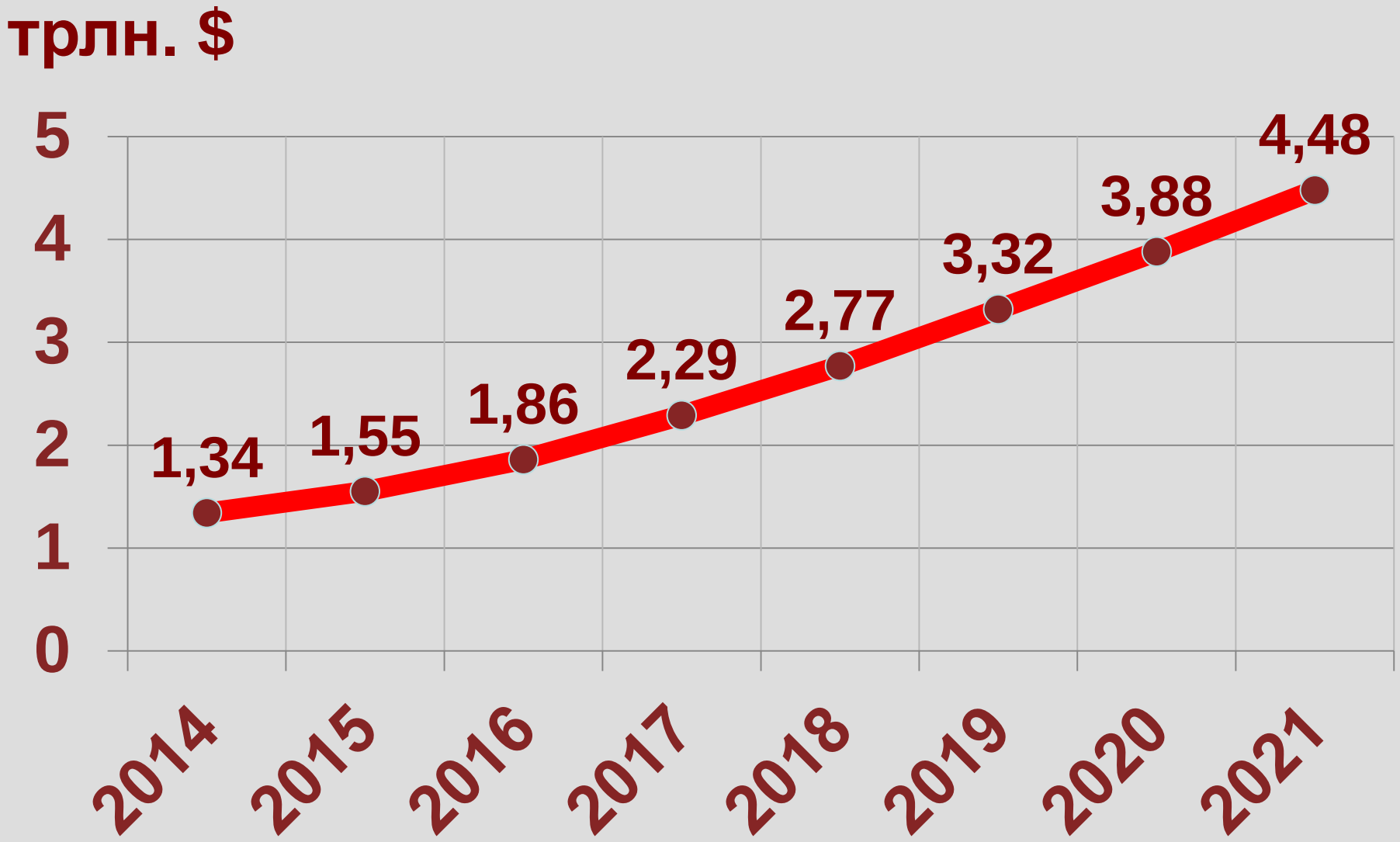
2018 Global Ecommerce Report

Ecommerce FOUNDATION

AWIN SAP Teleperformance each interaction matters Safe.Shop

Ассоциация РусКрипто

Global retail eCommerce



Ассоциация РусКрипто

Борьба с киберпреступностью

Ассоциация РусКрипто

Борьба с киберпреступностью

В 2018 г. Мировой Экономический Форум (WEF) включил киберпреступность в список глобальных угроз человечеству, поместив ее на 3-е место.

Ассоциация РусКрипто

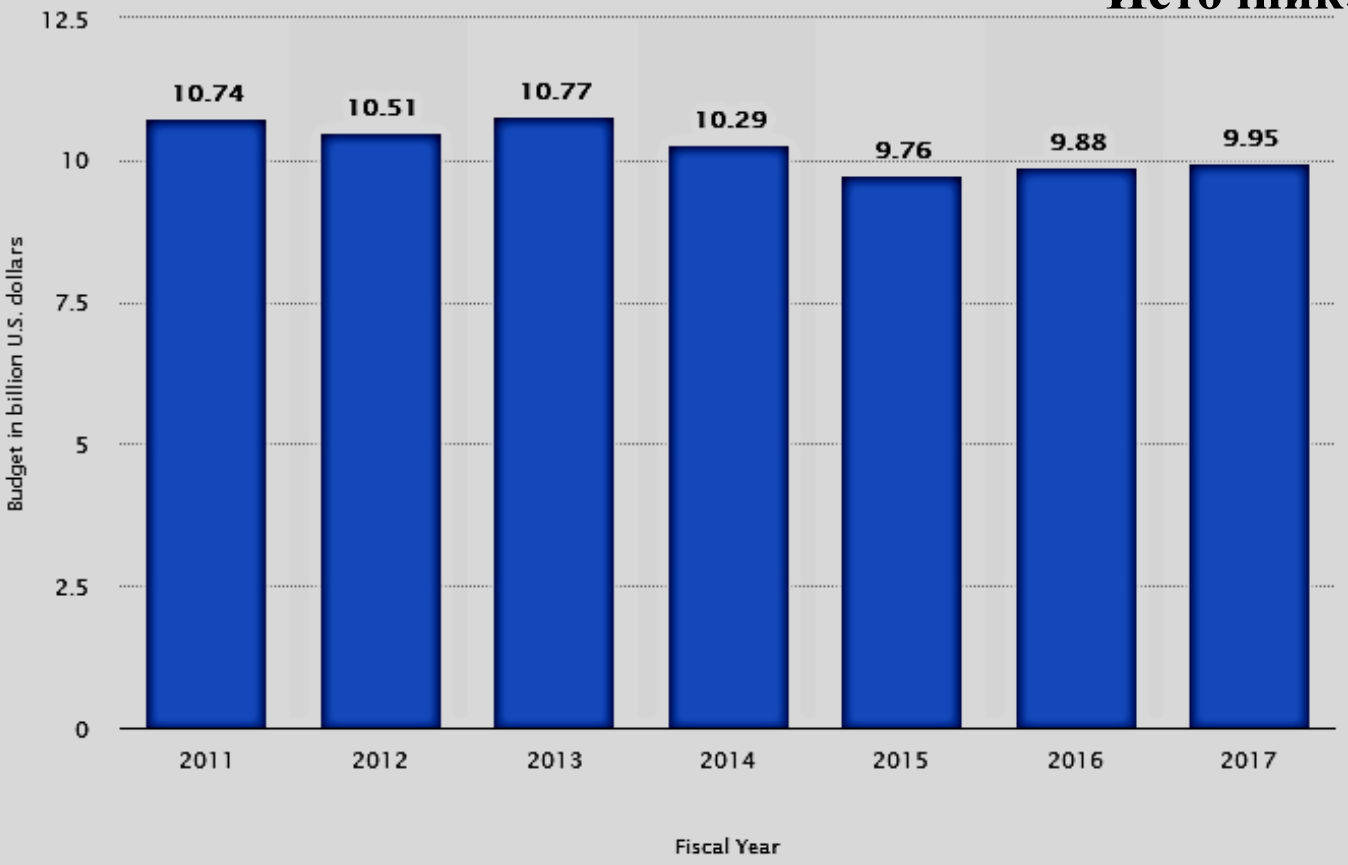
Борьба с киберпреступностью

- Ряд экспертов рассматривает киберпреступность как бóльшую опасность, чем ядерное оружие.
- Правительство США рассматривает возможность применения ядерного оружия в ответ на кибератаку.

New York Times

Budget of the U.S. National Security Agency in line with the U.S. National Intelligence Program for fiscal years 2011 to 2017 (in billion U.S. dollars)

Источник: The Washington Post



В 2017 г. затраты правительства США на кибер-безопасность составили $14 млрд.

Chief Information Officer

В «Consolidated Cryptologic Program» США задействовано более 35,000 специалистов.

Ассоциация РусКрипто

Гранты и фонды

- Если в период с 2000 по 2010 г.г. менее 15% работ, представленных учеными США на криптографических конференциях, финансировались силовыми структурами, то в 2011 г. их число возросло до 25%, а с 2012 до 2015 г.г. – до 65%

Phillip Rogaway

«The Moral Character of Cryptographic Work»

Ассоциация РусКрипто

Борьба с киберугрозами

Ассоциация РусКрипто

Crypto in 2018

Ассоциация РусКрипто

Crypto in 2018

2018 г. – более 60 конференций по криптографии и информационной безопасности, более 1600 докладов

Crypto in 2018

CRYPTO

EUROCRYPT

ASIACRYPT

AFRICACRYPT

INDOCRYPT

CHES

CT-RSA

FC

FSE

LightSec

PKC

SAC

TCC

ACNS

C2SI

ICISC

IMACC

Inscrypt

SPACE

QCrypt

PQCrypto

Crypto in 2018

ACISP
ATCI
ATIS
CRiSIS
CSS
CTCIS
DBSec
ESORICS
Euro-CYBERSEC

FDSE
FNSS
FPS
GameSec
ICCCS
ICICS
ICISS
ICISSP
ICITS

IOSec
ISC
ISDDC
ISPEC
ISSA
IWSEC
MMM-ACNS
NSS
ProvSec

RFIDSec
SAFECOMP
Security Protocols
SpaCCS
WAIFI
WISA
WISE
WISTP

Crypto in 2018

CRYPTO	Santa Barbara, CA, USA, August 19–23, 2018	Part I LNCS v. 10991 Part II LNCS v. 10992 Part III LNCS v. 10993
EUROCRYPT	Tel Aviv, Israel, April 29 – May 3, 2018	Part I LNCS v. 10820 Part II LNCS v. 10821 Part III LNCS v. 10822
ASIACRYPT	Brisbane, QLD, Australia, December 2–6, 2018	Part I LNCS v. 11272 Part II LNCS v. 11273 Part III LNCS v. 11274
AFRICACRYPT	Marrakesh, Morocco, May 7–9, 2018	LNCS v. 10831
INDOCRYPT	New Delhi, India, December 9–12, 2018	LNCS v. 11356

Crypto in 2018

CHES *Cryptographic Hardware and Embedded Systems*	Amsterdam, The Netherlands, September 9–12, 2018	
CT-RSA *The Cryptographers' Track at the RSA Conference*	San Francisco, CA, USA, April 16–20, 2018	LNCS v. 10808
FC *Financial Cryptography and Data Security*	Nieuwpoort, Curaçao, March 2, 2018	LNCS v. 10958
FSE *Fast Software Encryption*	Bruges, Belgium, March 5-7, 2018.	IACR Transactions on Symmetric Cryptology

Crypto in 2018

LightSec *Lightweight Cryptography for Security and Privacy*	Cardiff, Wales, United Kingdom, September 10-12, 2018	
PKC *Public-Key Cryptography*	Rio de Janeiro, Brazil, March 25–29, 2018	LNCS v. 10769 LNCS v. 10770
QCrypt *Quantum Cryptography*	Shanghai, China, August 27–31, 2018	
PQCrypto *Post-Quantum Cryptography*	Fort Lauderdale, FL, USA, April 9–11, 2018	LNCS v. 10786
TCC *Theory of Cryptography*	Panaji, India, November 11–14, 2018	LNCS v. 11239 LNCS v. 11240

Crypto in 2018

ACNS *Applied Cryptography and Network Security*	Leuven, Belgium, July 2–4, 2018	LNCS v. 10892
C2SI *Codes, Cryptology and Information Security*	Rabat, Morocco, April 10–12, 2017	LNCS v. 10194
ICISC *Information Security and Cryptology*	Seoul, South Korea, November 28–30, 2018	LNCS v. 11396
SAC *Selected Areas in Cryptography*	Calgary, AB, Canada, August 15–17, 2018	LNCS v. 11349

Crypto in 2018

Inscrypt *Information Security and Cryptology*	Beijing, China, November 4–6, 2016	LNCS v. 10143
SPACE *Security, Privacy, and Applied Cryptography Engineering*	Kanpur, India, December 15–19, 2018	LNCS v. 11348
IMACC *IMA International Conference Cryptography and Coding*	Oxford, UK, December 12–14, 2017	LNCS v. 10655

Crypto in 2018

ACISP	Australasian Conference Information Security and Privacy
ATCI	International Conference on Applications and Techniques in Cyber Security and Intelligence
ATIS	Applications and Techniques in Information Security
CRiSIS	Risks and Security of Internet and Systems
CSS	Cyberspace Safety and Security
CTCIS	Chinese Conference Trusted Computing and Information Security
DBSec	Data and Applications Security and Privacy
ESORICS	European Symposium on Research in Computer Security
Euro-CYBERSEC	*International ISCIS Security Workshop* Security in Computer and Information Sciences

Ассоциация РусКрипто

Crypto in 2018

FDSE	Future Data and Security Engineering
FNSS	Future Network Systems and Security
FPS	Foundations and Practice of Security
GameSec	Decision and Game Theory for Security
ICCCS	International Conference on Cloud Computing and Security
ICICS	International Conference on Information and Communications Security
ICISS	International Conference on Information Systems Security
ICISSP	International Conference on Information Systems Security and Privacy
ICITS	International Conference on Information Theoretic Security

Crypto in 2018

IOSec	Information and Operational Technology Security Systems
ISC	Information Security International Conference
ISDDC	Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments
ISPEC	Information Security Practice and Experience International Conference
ISSA	Information Security International Conference
IWSEC	International Workshop on Security
MMM-ACNS	International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security
NSS	Network and System Security International Conference
ProvSec	Provable Security International Conference

Crypto in 2018

RFIDSec	Radio Frequency Identification and IoT Security
SAFECOMP	Computer Safety, Reliability, and Security
Security Protocols	International Workshop on Security Protocols
SpaCCS	Security, Privacy, and Anonymity in Computation, Communication, and Storage
WAIFI	International Workshop on Arithmetic of Finite Fields
WISA	International Workshop on Information Security Applications
WISE	International Workshop on Information Security Education
WISTP	International Workshop on Information Security Theory and Practice

Ассоциация РусКрипто

Research in Cryptography

- Theoretical Foundations
- New Methods in Cryptanalysis
- Homomorphic Encryption
- Cloud Computing Security
- Key Exchange Protocols
- Leakage Resilient Cryptography
- Deniability and Anonymity
- Password-Based Cryptography
- Secure Multiparty Computation
- Authenticated Encryption
- Light Weight Cryptography
- Hash functions

Ассоциация РусКрипто

New Directions of Modern Cryptography

- authorized cryptography (proxy cryptography, proxy re-cryptography)
- attribute-based cryptography (identity-based cryptography, spatial cryptography, functional cryptography)
- post-quantum cryptography (noncommutative cryptography, lattice-based cryptography)
- bigkey cryptography
- biologic cryptography (DNA cryptography, biometric feature based cryptography).

Ассоциация РусКрипто

Crypto in 2018

Исследовательские проекты и процессы стандартизации

Big Data

Ассоциация РусКрипто

Big Data Analytics and Applications

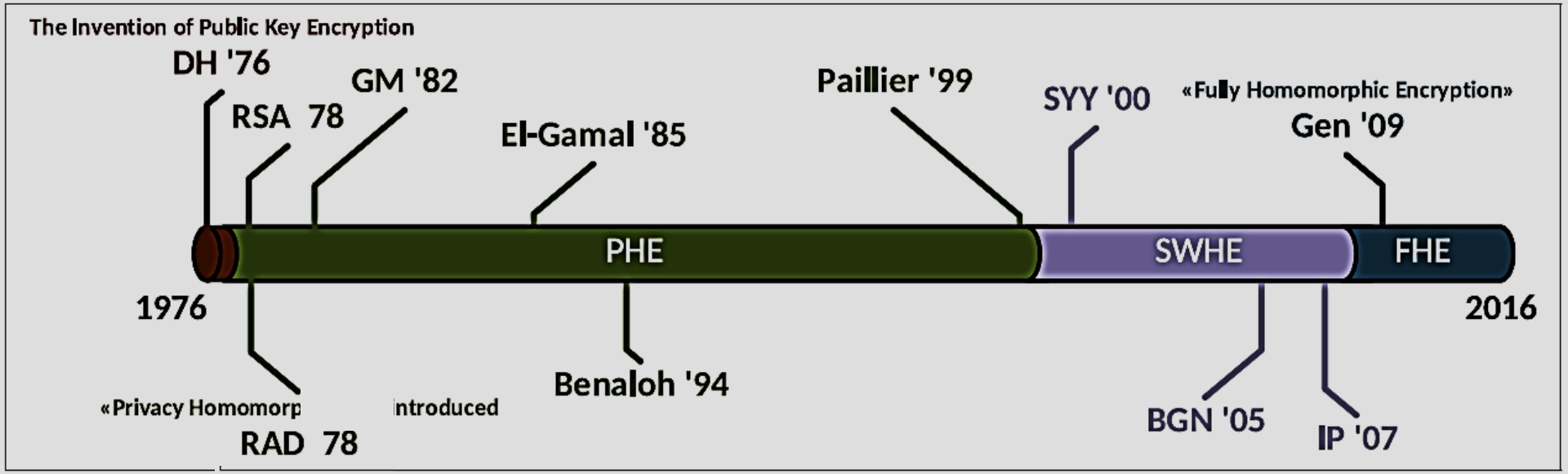
- International Workshop on Security in Big Data (SECBD-2017)
- The 8th International Workshop on Trust, Security and Privacy for Big Data (TrustData 2017)
- The 3rd International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2017)
- The 2017 International Symposium on Big Data and Machine Learning in Information Security, Privacy and Anonymity (SPBD 2017)

Homomorphic Encryption

Ассоциация РусКрипто

Homomorphic Encryption

Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation* 4, 11 (1978), 169–180.



Timeline of HE schemes until Gentry's first FHE scheme.

Ассоциация РусКрипто

The HEAT Project

Homomorphic Encryption: Application & Technology

- Project funded by EU in Horizon 2020.
- Starting date 1st January 2015

Ассоциация РусКрипто

Fully Homomorphic Encryption

The HEAT proposal brings together Europe's leading researchers on homomorphic cryptography

- **KU Leuven, Belgium (Co-ordinator)**
- **University of Bristol, UK**
- **University of Luxemburg, Luxemburg**
- **Université Pierre et Marie Curie, France**

and three industrial partners with existing interests in the field

- **CryptoExperts, France**
- **NXP Semiconductors, Belgium**
- **Thales UK, UK**

Ассоциация РусКрипто

The HEAT Project

Homomorphic Encryption: Application & Technology

- The proposed outputs of HEAT are an **open source software library** to support applications that wish to use homomorphic cryptography.

https://heat-project.eu

Quantum Cryptography

Ассоциация РусКрипто

Quantum Cryptography

- В 2004 г. в рамках «Quantum Network project» продвигавшегося US Defense Advanced Research Projects Agency (DARPA) была продемонстрирована первая в мире QKD-линия длиной около 10 км., соединившая 3 пункта связи, расположенные в районе Бостона.
- США анонсировали планы построить QKD-линию, соединяющую Бостон и Вашингтон (634 км.).

Ассоциация РусКрипто

Quantum Cryptography

- В 2008 г. в рамках проекта Евросоюза SECOQC (Secure Communication based on Quantum Cryptography) была открыта QKD-сеть длиной 30 км., с пропускной способностью 1 кб/с, соединившая 6 пунктов связи в Вене.

  Сеть использовалась в том числе и для шифрования телефонных переговоров.

Ассоциация РусКрипто

Quantum Cryptography

- В 2010 г. в Японии силами Министерства внутренних дел и коммуникаций и National Institute of Information and Communications Technology (NICT) реализована QKD-сеть с пропускной способностью 100 кб/с. На ее базе впервые было продемонстрирована передача QKD-зашифрованной видеотрансляции.

В настоящее время вполне реальным считается построение QKD-линии длиной 50 км. с пропускной способностью 1 Мб/с.

Процесс стандартизации криптографических алгоритмов

Ассоциация РусКрипто

Стандартизация криптографических алгоритмов

«If the industrial age was marked by standardisation, the digital era is about customisation. The consumer and user is ever more central to innovation, by virtue of being more active and responsive, hence shaping the value chain and leading the way towards more tailor-made, personalised, on-demand products and services.»

The European Political Strategy Centre (EPSC)
«10 Trends Shaping in the Digital Age Innovation»

Ассоциация РусКрипто

Quantum Cryptography Standardization

QKD-стандартизацией занимаются

- International Organization for Standardization (ISO/IEC)
- Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T)
- ISG-QKD (Industrial Specification Group of QKD devices), входящая в ETSI (European Telecommunications Standards Institute) – в рамках европейской программы SECOQC

Post-Quantum Cryptography

Ассоциация РусКрипто

International efforts to standardize PQC

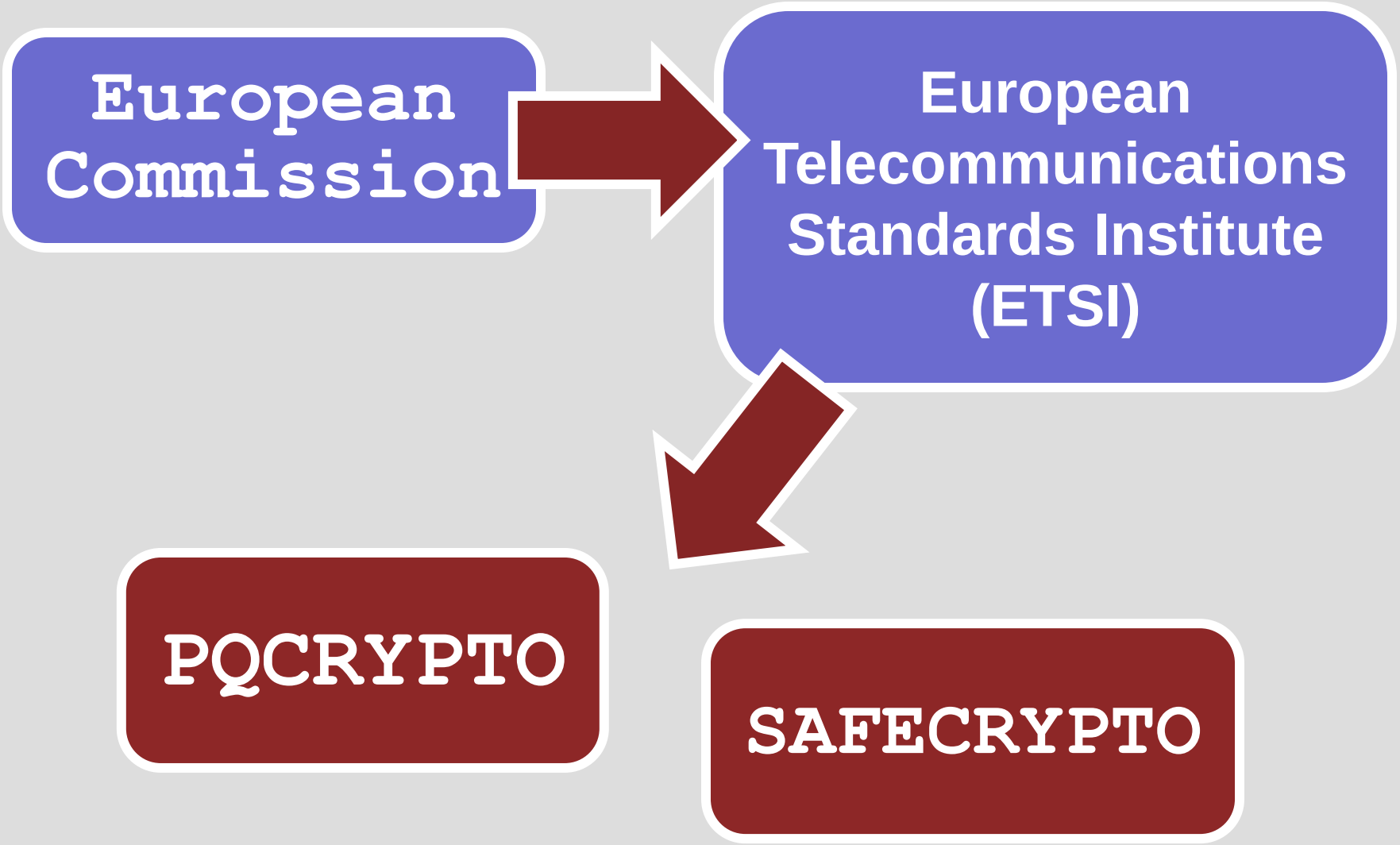
European Commission

Japanese Society for the Promotion of Science

U.S. National Institute of Standards and Technology (NIST)

Ассоциация РусКрипто

European efforts to standardize PQC



Ассоциация РусКрипто

International efforts to standardize PQC

Organization for Standardization (ISO)

International Electrotechnical Commission (IEC)

Ассоциация РусКрипто

PQC standardization trends in Japan

Ministry of Internal Affairs and Communications

National Institute of Information and Communications Technology (NICT)

Ministry of Economy, Trade and Industry

Information-technology Promotion Agency (IPA)

CRYPTREC (Cryptography Research and Evaluation Committees) project

Ассоциация РусКрипто

NIST PQC standartization

28.04.2016
NISTIR 8105
release

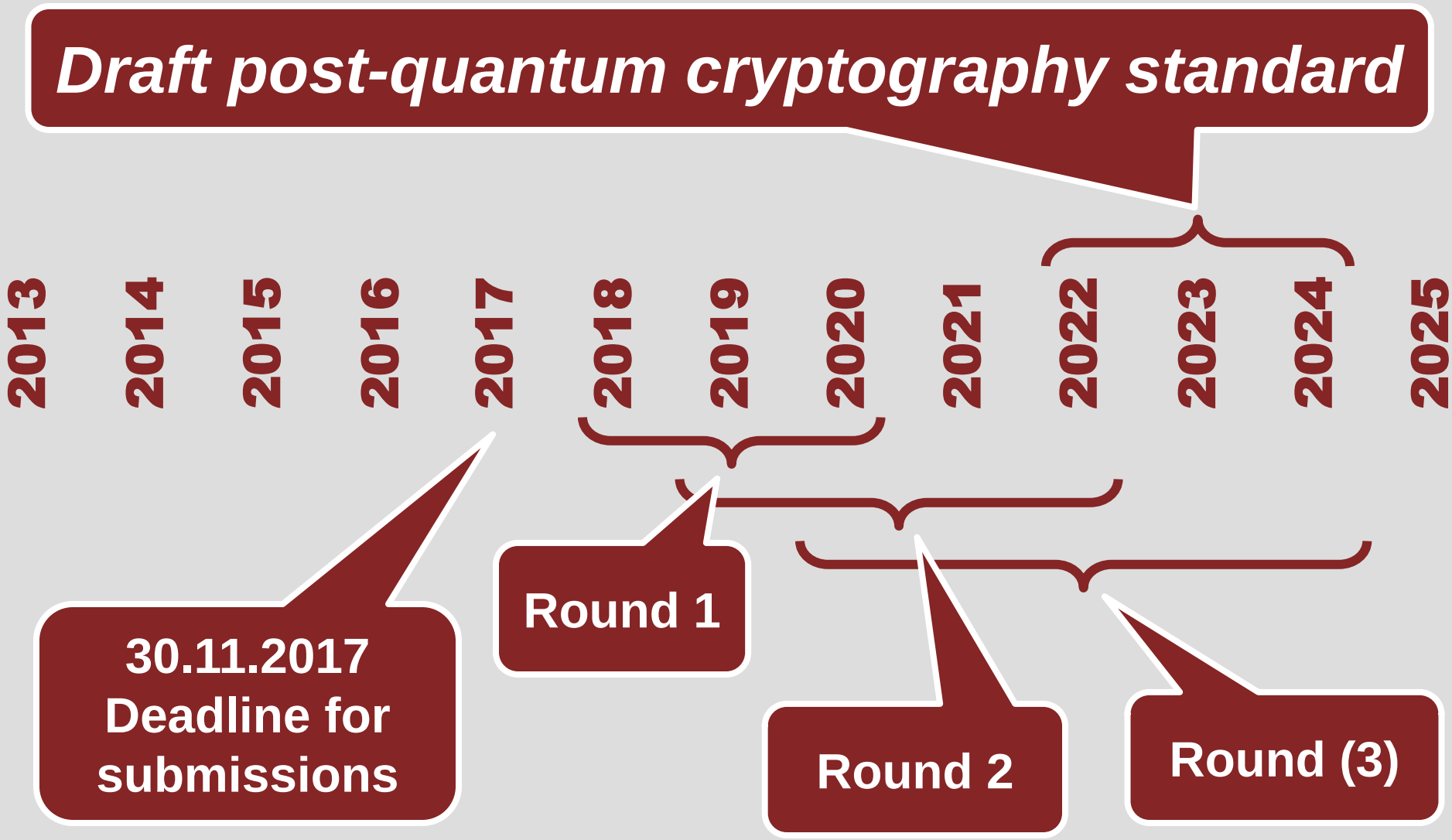
20.12.2016
Call for submissions

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025

30.11.2017
Deadline for
submissions

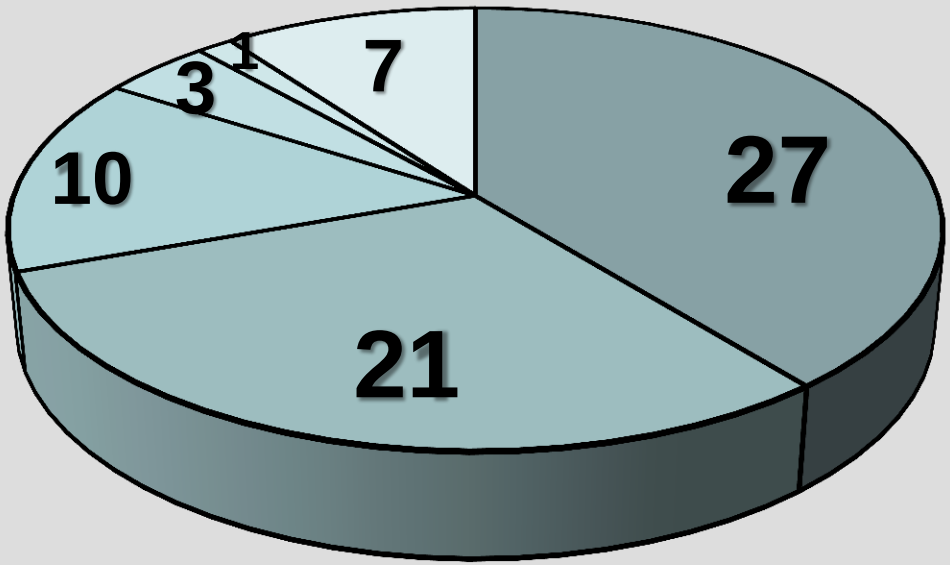
Ассоциация РусКрипто

NIST PQC standartization



Ассоциация РусКрипто

NIST PQC standartization



- Lattice-based – 27
- Code-based – 21
- Multivariate – 10
- Hash-based – 3
- Isogeny-based – 1
- Other – 7

Authenticated Encryption

Ассоциация РусКрипто

CAESAR

- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- 2014 – ~~2017~~ ~~2018~~ 2019?
- Goal: “Identify a portfolio of authenticated ciphers that offer advantages over AES-GCM (the current de-facto standard) and are suitable for widespread adoption.”

http://competitions.cr.yp.to/caesar.html

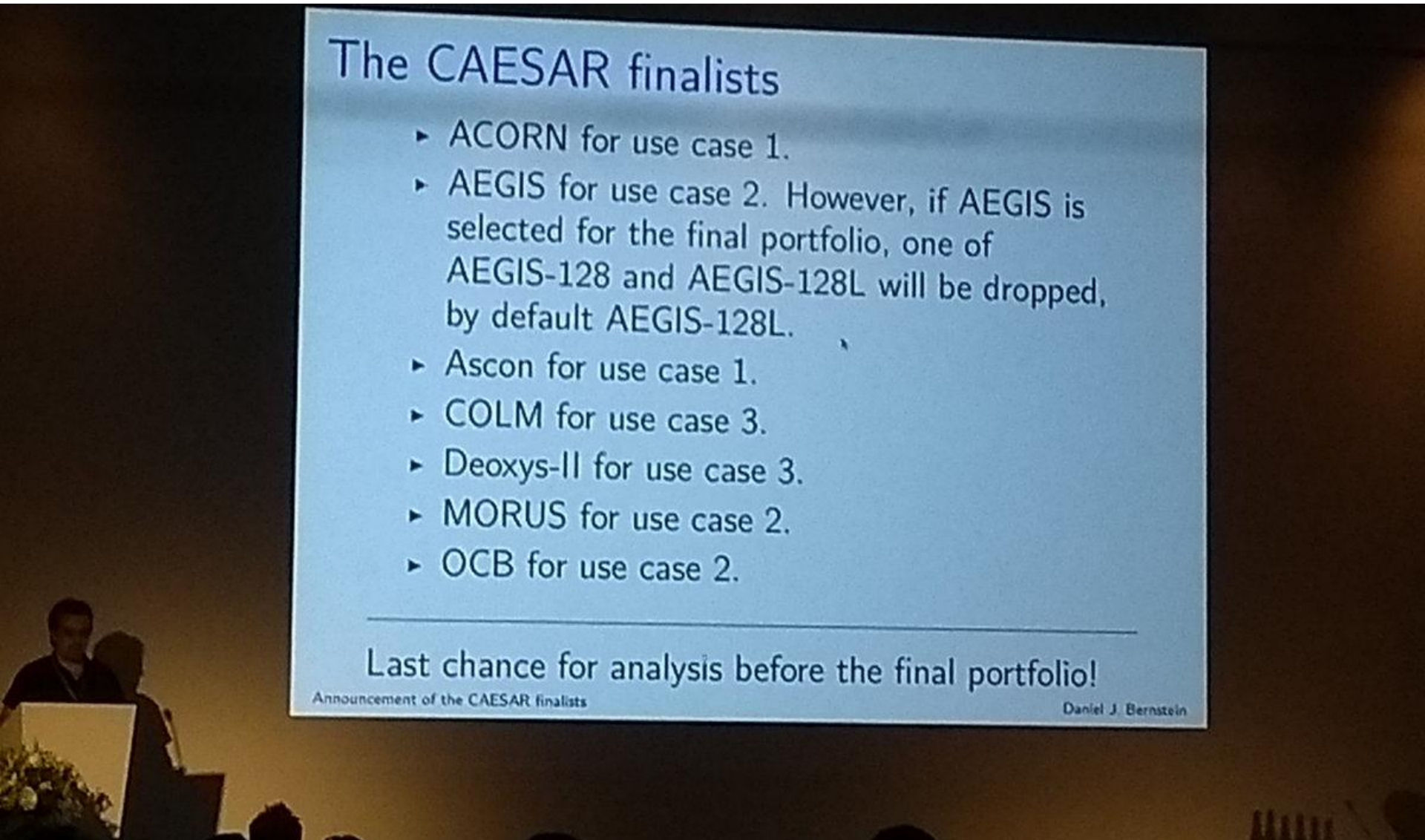
Ассоциация РусКрипто

CAESAR

Timeline planned in 2012	
2013.01: Announce “tentative schedule”.	2013.01.15: Competition announced
2014.01: Deadline for first-round submissions.	2014.03.15: Deadline for first-round submissions.
2015.01: Announce second-round candidates.	2015.07.07: Announcement of second-round candidates.
2016.01: Announce third-round candidates.	2016.08.15: Announcement of third-round candidates.
2017.01: Announce finalists	2018.03.06: Announcement of finalists.
2018.01: Announce final portfolio.	2019.02.20: Announcement of final portfolio.

Ассоциация РусКрипто

CAESAR Finalists Announced on 6 Mar 2018



Lightweight Cryptography

Ассоциация РусКрипто

Lightweight Cryptography

- **ISO/IEC FDIS 29192-1 – 29192-5**

  Information technology – Security techniques – Lightweight cryptography (2011-2015)

  - **Part 1: General.**
  - **Part 2: Block ciphers.**
  - **Part 3: Stream ciphers.**
  - **Part 4: Mechanisms using asymmetric techniques.**
  - **Part 5: Lightweight hash functions**

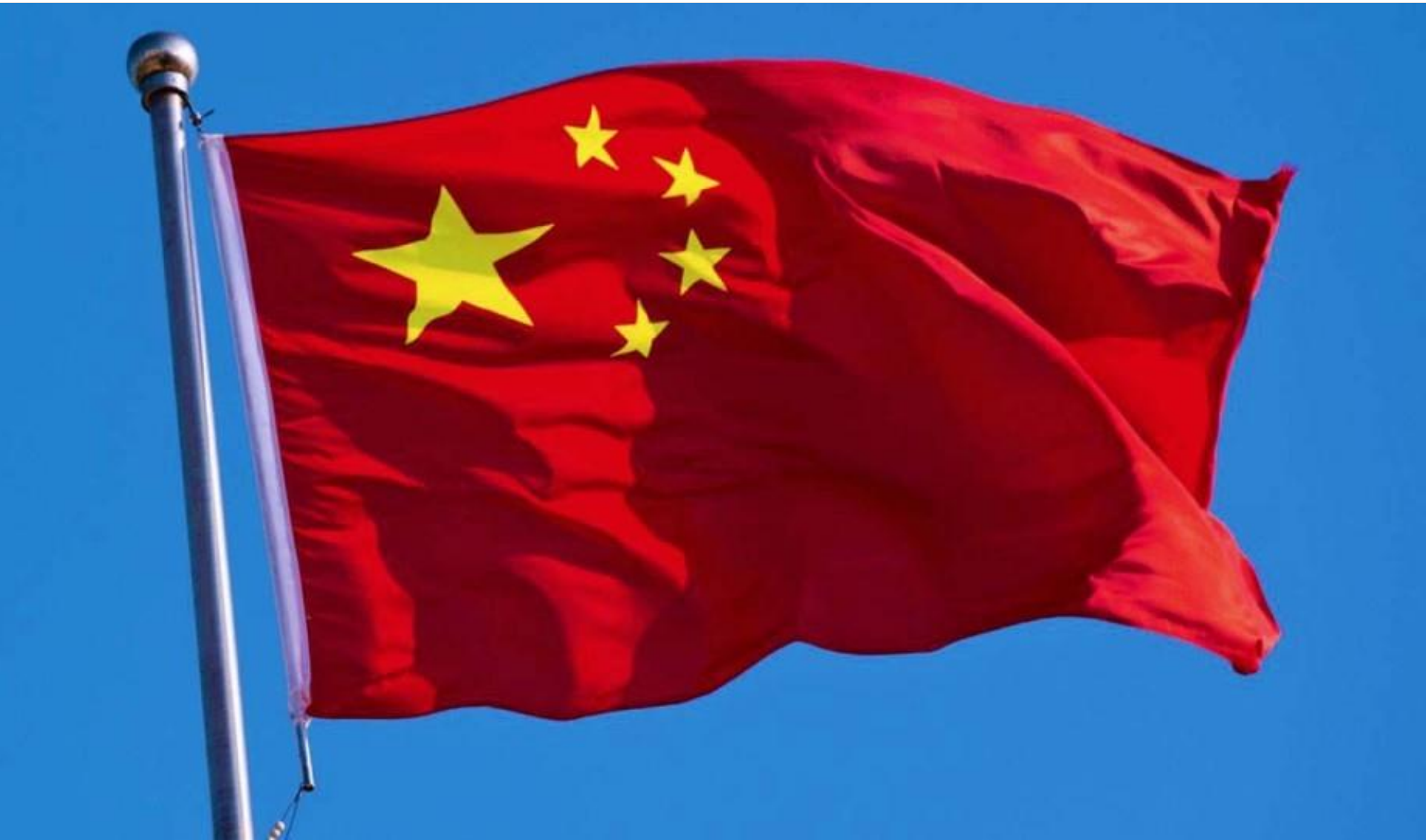
Lightweight Cryptography

National Institute of Standards and Technology:

Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process (Aug 2018)

https://csrc.nist.gov/Projects/Lightweight-Cryptography

中国

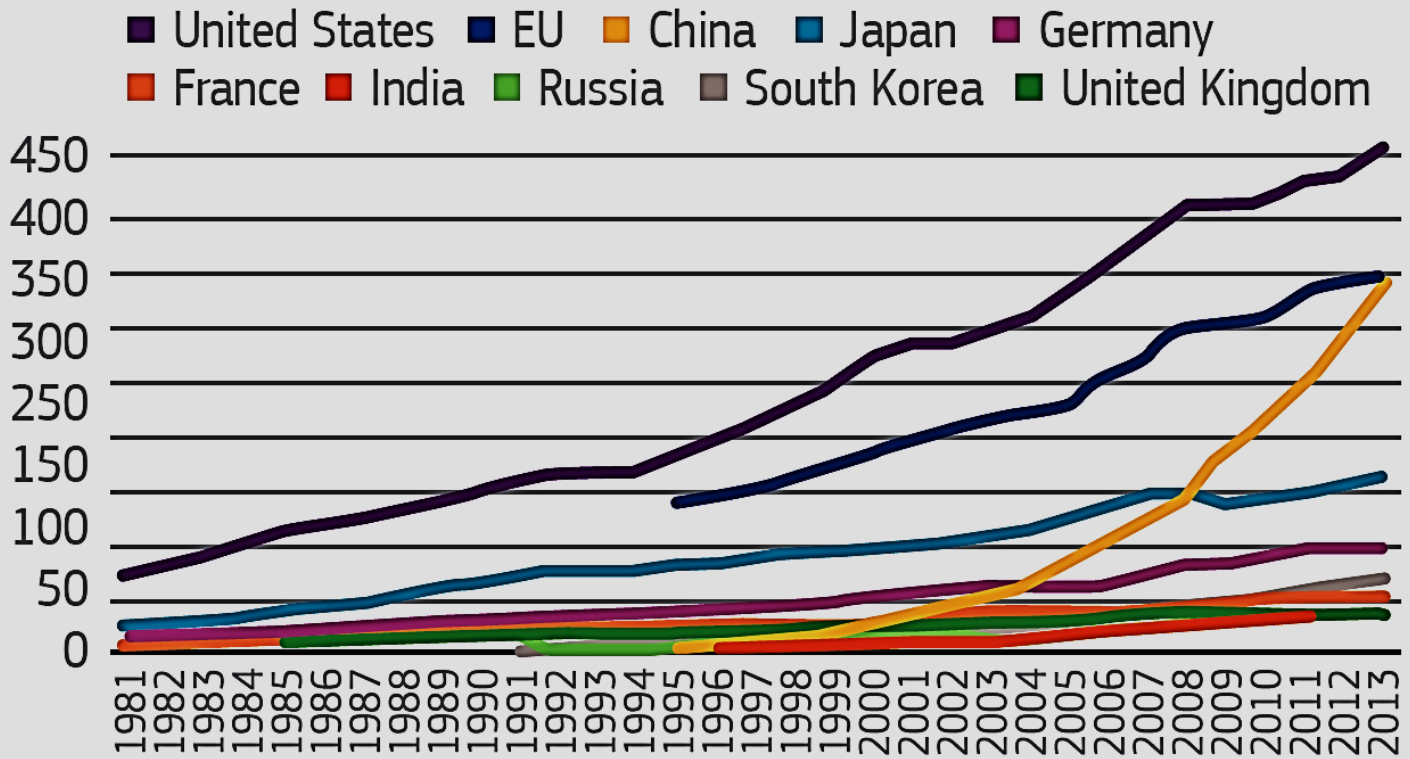


Ассоциация РусКрипто

Information Technologies

China is investing in R&D at a rate that eclipses both the EU and US

R&D spending in billions of dollars (current, in purchasing power parity terms)

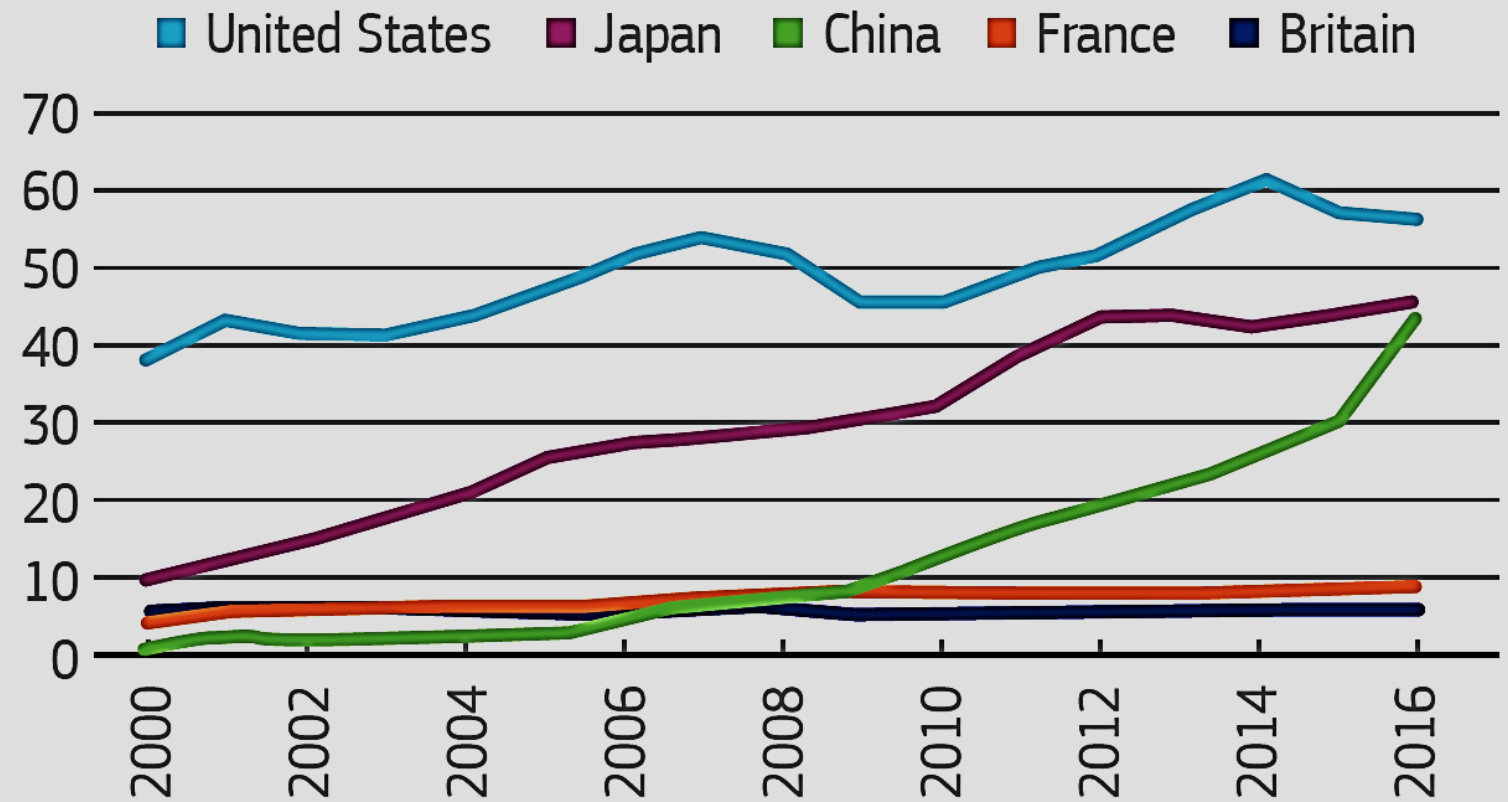


Ассоциация РусКрипто

Information Technologies

And its rate of new patent applications is surging accordingly

International patent applications (in thousands)

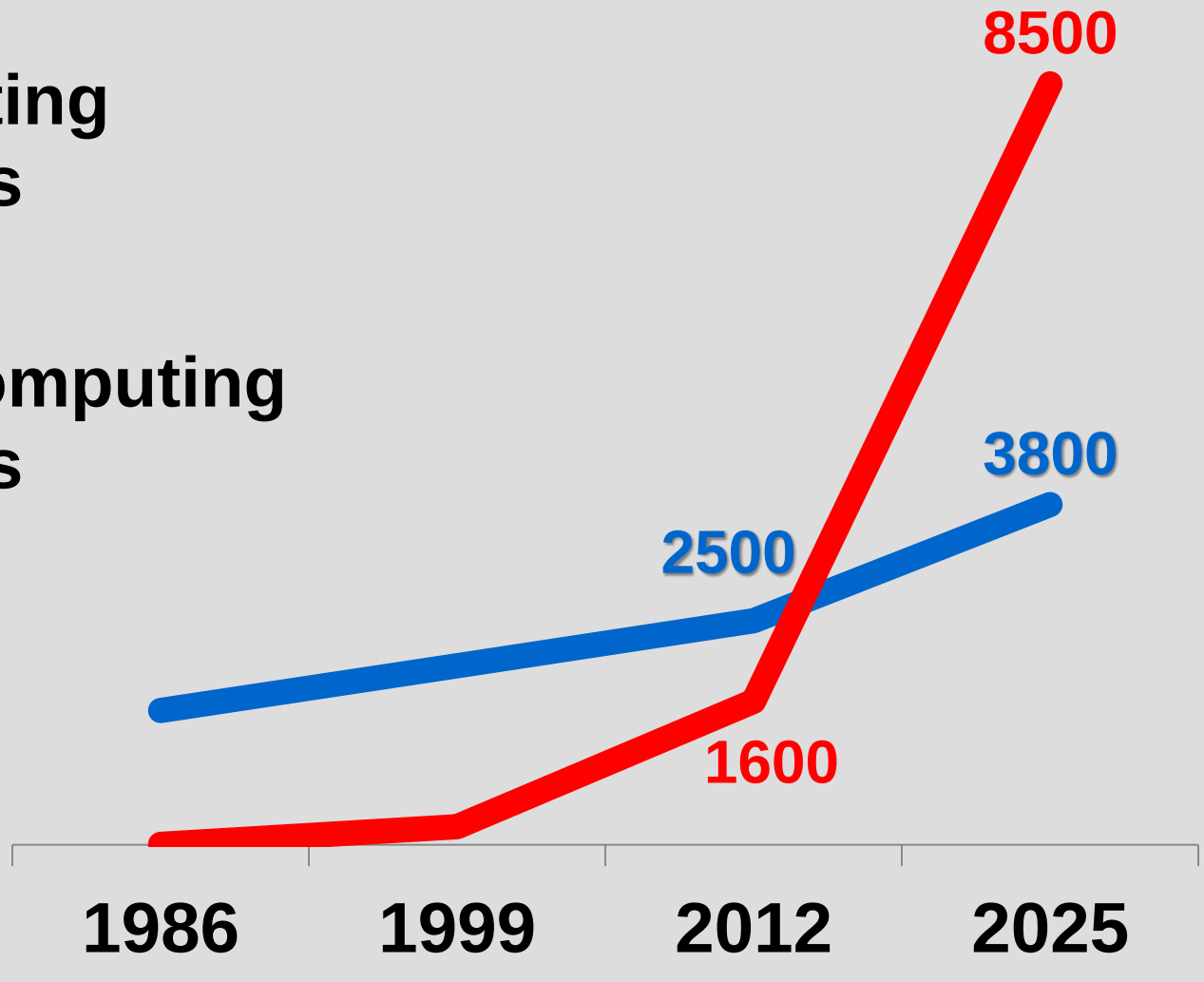


Ассоциация РусКрипто

Information Technologies

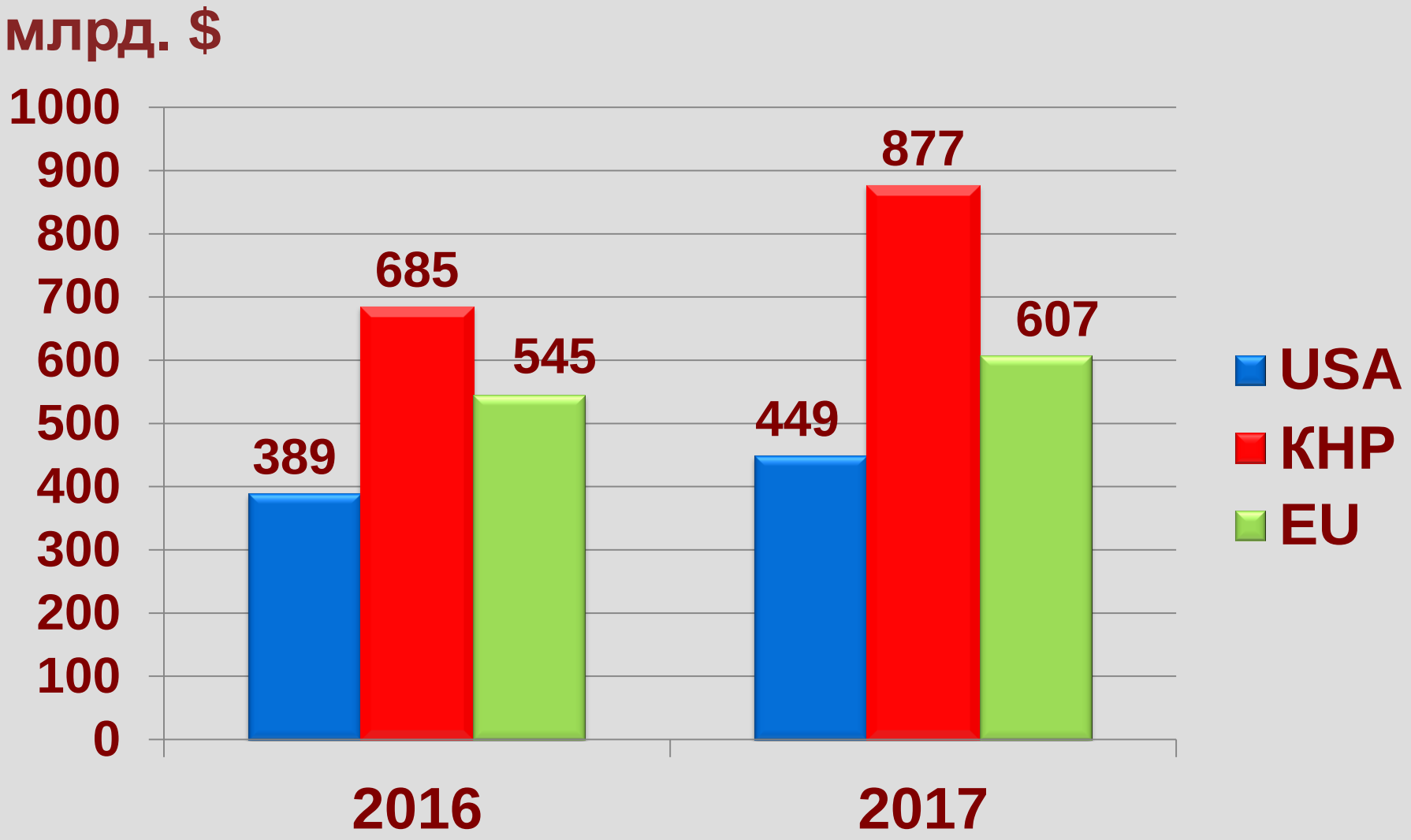
US computing PhD degrees

Chinese computing PhD degrees



Ассоциация РусКрипто

eCommerce



Ассоциация РусКрипто

Quantum Cryptography

- В 2017 г. в Китае создана самая большая в мире the QKD-линия длиной 2,000 км., соединившая Пекин и Шанхай.
- В 2017 г. в Китае произведена квантовая передача ключа между спутником и наземной станцией, что позволило создать работающую QKD-линию, соединившую Китай и Австрию

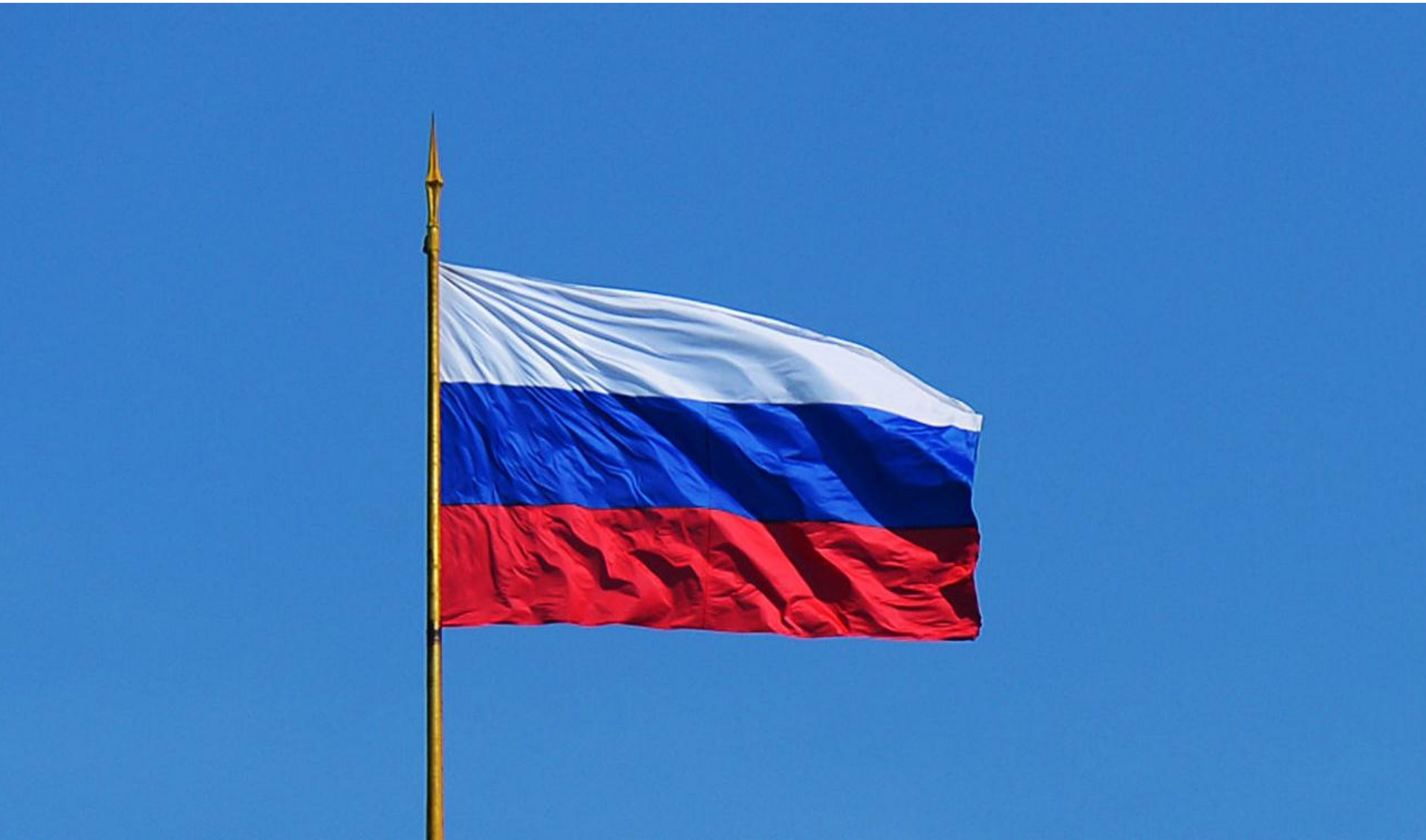
Ассоциация РусКрипто

Quantum Cryptography Standardization

- В Китае ведется интенсивная работа по выработке стандартов для квантовой криптографии.
- Работу координирует CCSA (China Communication Standardization Association).

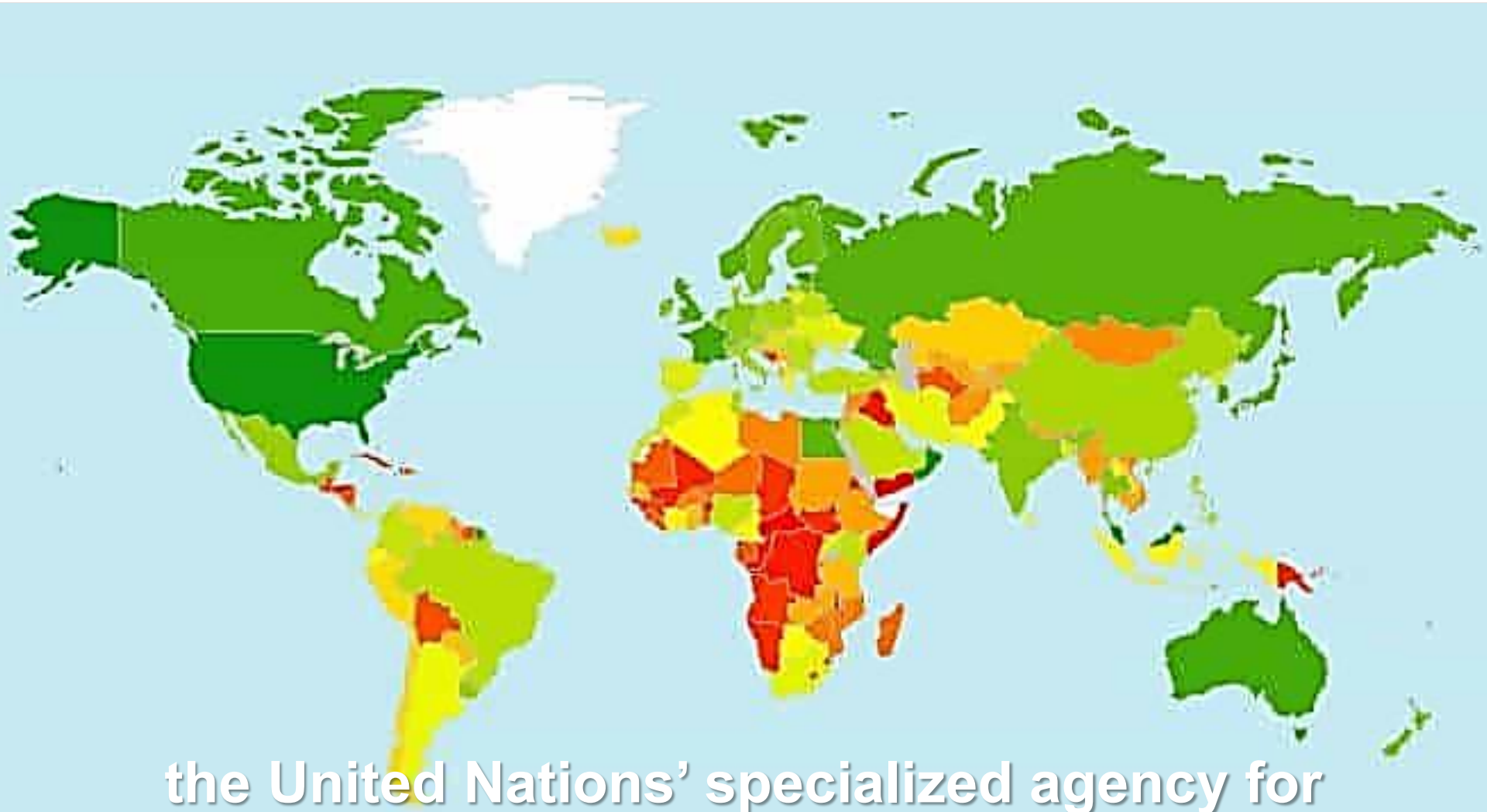
Ассоциация РусКрипто

Российская криптография



Ассоциация РусКрипто

The International Telecommunications Union (ITU)



the United Nations' specialized agency for information and communication technologies.

Ассоциация РусКрипто

Конференции РусКрипто

Актуальные направления развития криптографии

Настоящее и будущее кибербезопасности

Ассоциация РусКрипто

Стандартизация криптографических алгоритмов

Разработка стандартов для квантовой и постквантовой криптографии

Ассоциация РусКрипто

Актуальные направления развития криптографии

Разработка теории обратимых вычислений

Ассоциация РусКрипто

Разработка теории обратимых вычислений

Для создания парадигмы обратимых вычислений потребуется разработать (практически «с нуля») новые направления:

- **теорию (алгебру и логику) обратимых вычислений;**
- **языки и парадигмы обратимого программирования;**
- **методы реализации прикладных программ и алгоритмы обратимого программирования;**
- **обратимую схемотехнику;**
- **физическую реализацию обратимых элементов.**

Ассоциация РусКрипто

Разработка теории обратимых вычислений

Как следствие, переход всей IT технологии на концепцию реализации обратимых вычислений заставит пересмотреть как существующие криптографические примитивы, так и многие фундаментальные принципы их построения.

АИС

Ассоциация РусКрипто

РусКрипто'2019

XXI Международная научно-практическая конференция