

*Весело о грустном, или
обсуждение нетиповых
инцидентов в области
защиты информации в
финансовых организациях
в 2016-2017 годах*



Информационная безопасность в финансовом секторе,
Москва, 07.06.2017

Плешков Алексей Константинович

Образование

окончил МИФИ в 2006 году, факультет «Информационная безопасность», специалист по безопасности банковских систем.

Опыт работы

более 12 лет в Банке ТОП-3 РФ

более 17 лет в сфере ИБ

*9 лет – выявление внутренних и внешних нарушителей,
активное противодействие мошенничеству.*

Крутые отчеты и статистика





Случаи из жизни

Политические войны в кибер-пространстве



| | |
|-----|---------------|
| 907 | United States |
| 574 | China |
| 77 | Netherlands |
| 70 | Russia |
| 67 | Austria |
| 51 | Hong Kong |
| 48 | Thailand |
| 47 | Taiwan |
| 44 | France |
| 38 | Mil/Gov |

| | |
|------|---------------|
| 1871 | United States |
| 73 | Hong Kong |
| 55 | Thailand |
| 39 | Netherlands |
| 34 | Portugal |
| 32 | Turkey |
| 31 | Canada |
| 30 | Liechtenstein |
| 23 | Austria |
| 23 | Norway |

Каждому банку по DDoS

<http://map.norsecorp.com>

<http://www.digitalattackmap.com>

<https://cybermap.kaspersky.com>

| ATTACKS | | | | | | | |
|------------------------|-----------------------------|-----------------|----------------|------------------------------|---------|------|-------|
| Timestamp | Organization | Attacker | IP | Location | Service | Type | Port |
| 2014-06-29 10:57:53.73 | Shanghai RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |
| 2014-06-29 10:57:54.85 | Allycan Computing Co., LTD | Hangzhou, China | 192.92.75.26 | San Francisco, United States | unknown | | 33435 |
| 2014-06-29 10:57:54.86 | N/A | unknown, Chile | 199.116.121.93 | San Francisco, United States | unknown | | 33435 |
| 2014-06-29 10:57:57.52 | Thelma RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |
| 2014-06-29 10:57:57.53 | Thelma RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |
| 2014-06-29 10:57:57.53 | Thelma RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |
| 2014-06-29 10:57:57.54 | Thelma RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |
| 2014-06-29 10:57:57.55 | Thelma RD clients (WeBDC) | Moscow, Russia | 188.126.225.71 | unknown, Austria | http | | 80 |

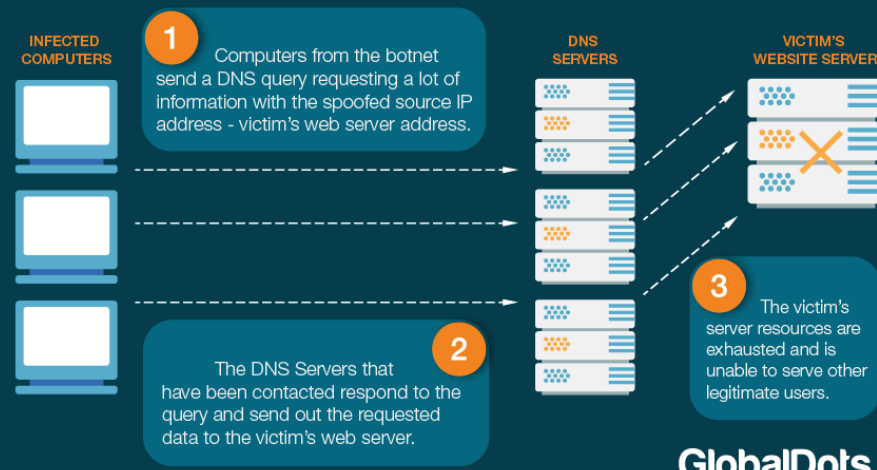
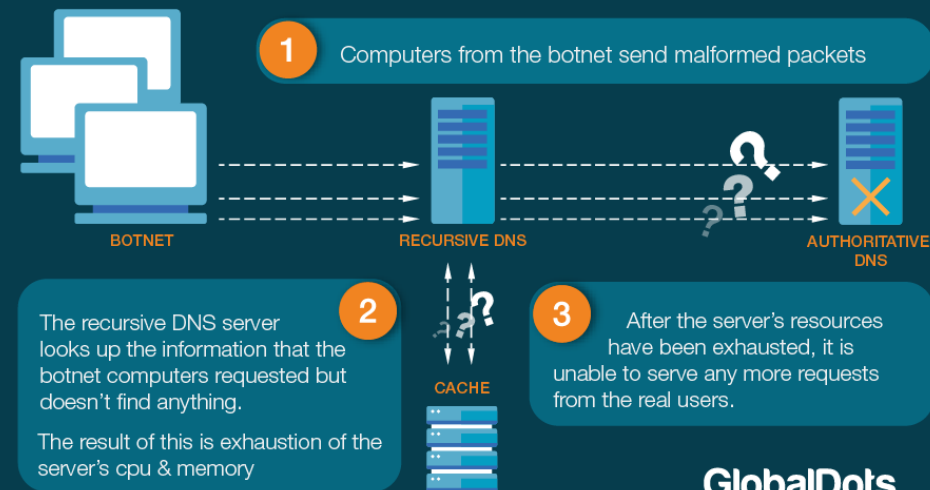
| ATTACK TYPES | | |
|--------------|--------------|-------|
| # | Service | Port |
| 524 | vnc | 5900 |
| 241 | unknown | 33435 |
| 180 | http | 80 |
| 143 | http-alt | 8080 |
| 126 | ssh | 22 |
| 94 | microsoft-ds | 445 |
| 67 | sip | 5060 |
| 64 | telnet | 23 |

© Norse

DNS FLOOD



DNS Amplification



Вредоносное программное обеспечение



SWIFT под угрозой

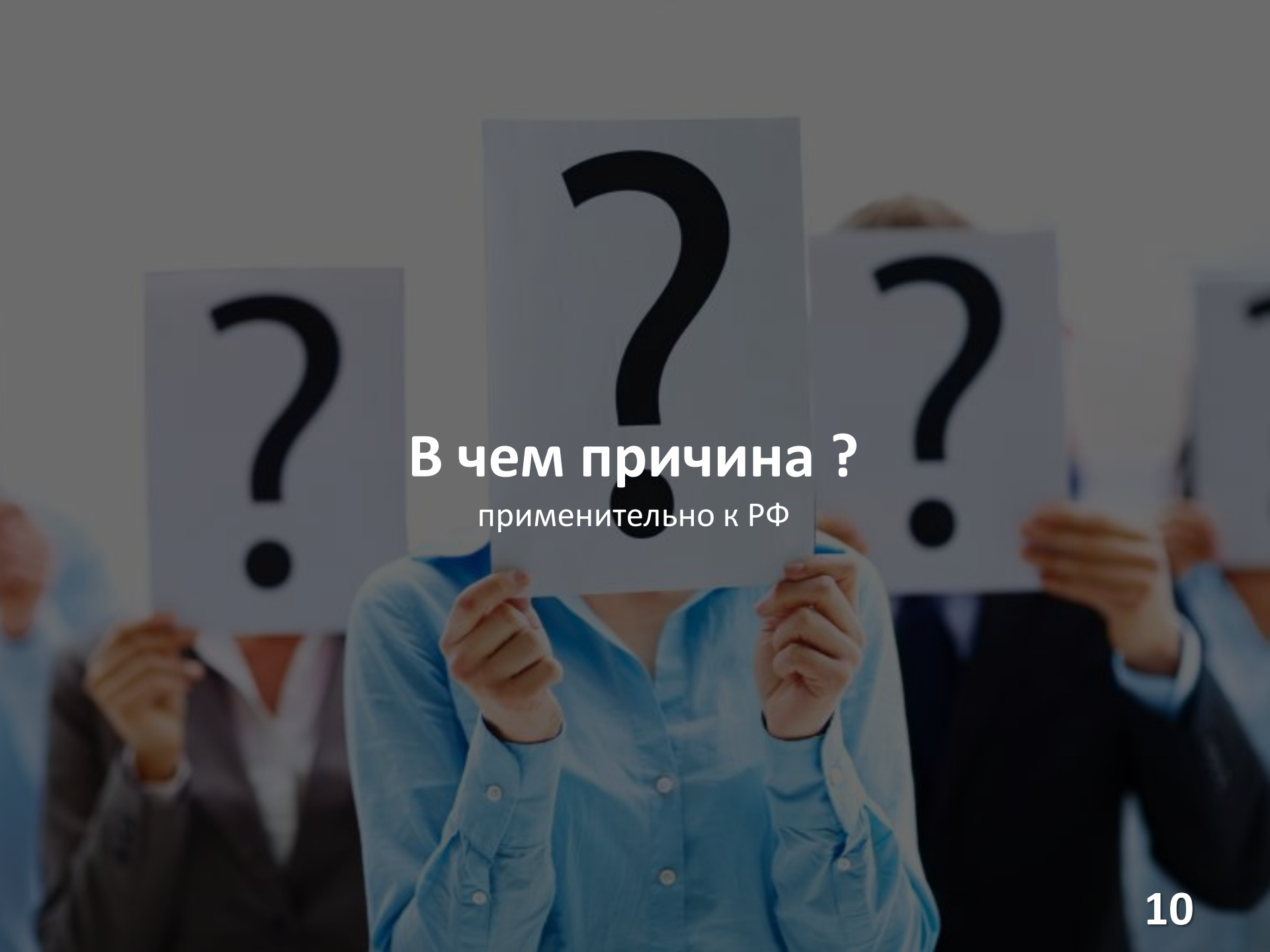


SWIFT ДАВНО под угрозой



Shadow Brokers

The NSA Hackers Are Back!



В чем причина ?
применительно к РФ

Нестабильность в отрасли



Нужда заставила



Инертность в принятии решения



Менталитет



Заплаточный подход



Деньги под ногами



Романтика и безнаказанность

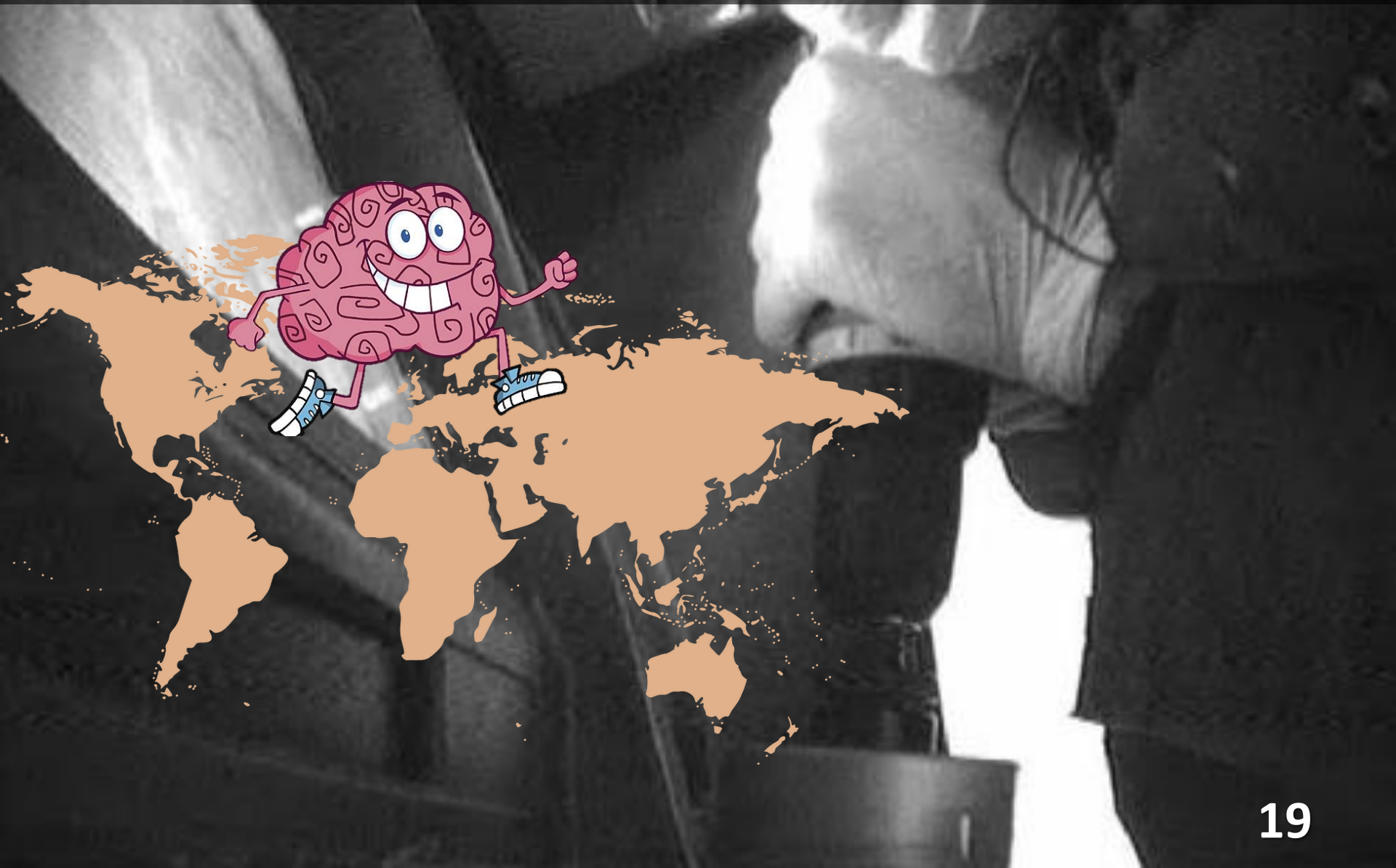


Опережающие темпы развития
преступности

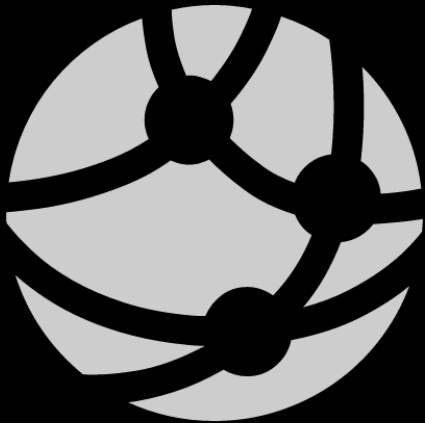


**ОСТОРОЖНО!
МОШЕННИКИ!**

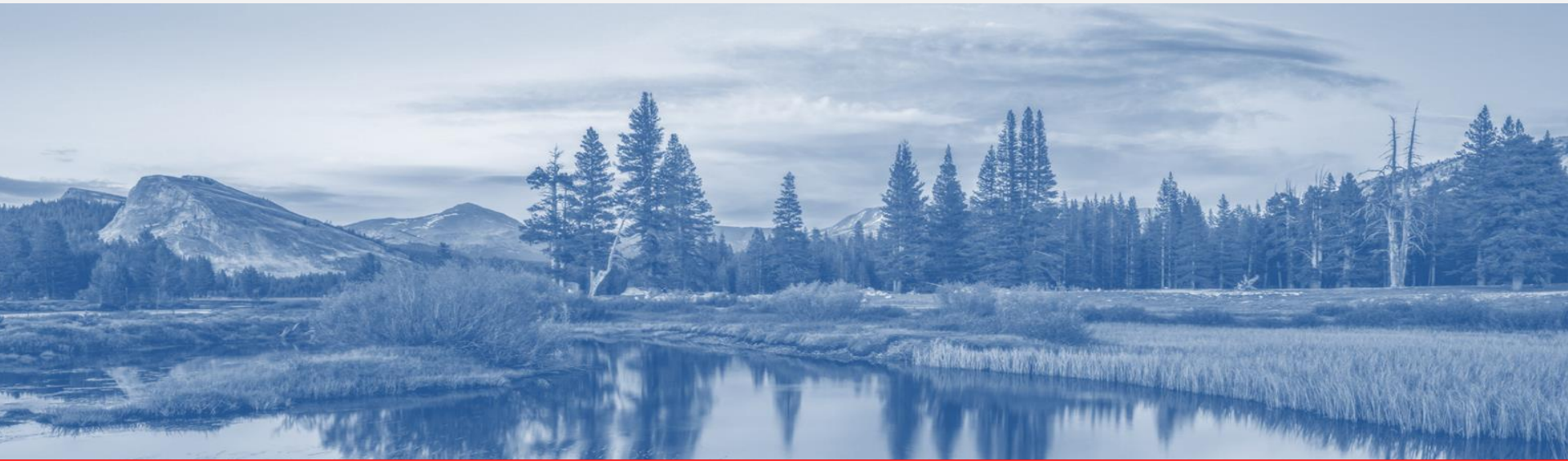
Обмен опытом с «западными коллегами»



Анонимность и скрытность от большого брата



Спасибо за внимание!



Готов ответить на Ваши вопросы