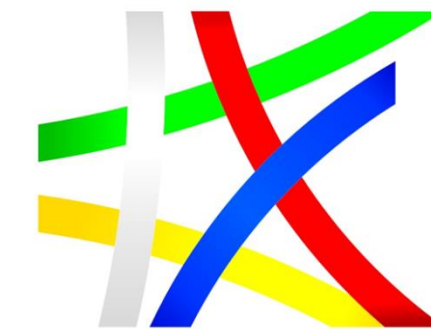




ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ



ОПЕРАТИВНА ПРОГРАМА
**ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ**

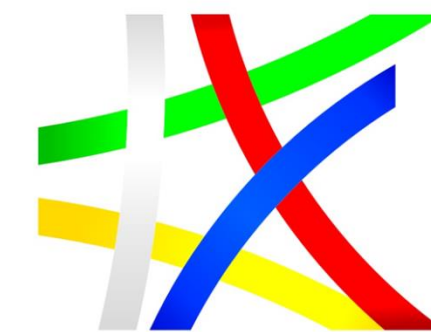
SECURITY AND COMPLIANCE OF FINANCIAL AND PERSONAL DATA

Boyan Yanchev, Chief Technology Officer

30.11.2018 г.



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ



ОПЕРАТИВНА ПРОГРАМА
**ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ**

Сдружение Клъстер Айтос (ITOS) е създадено през 2013 година.

Членове на сдружението: водещи компании в областта на информационните технологии, утвърдени строителни фирми, научни организации към БАН, НПО, читалище и общини

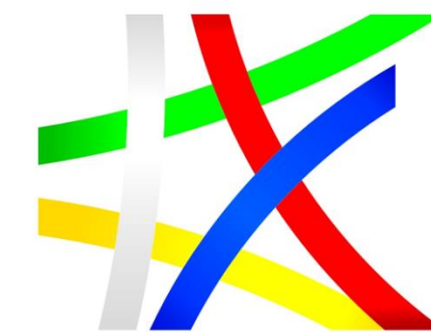
Сдружението работи за стимулиране развитието на информационните технологии , инфраструктурата за предоставянето на ИТ услуги; Аутсорсинга на ИТ услуги от България , облачни услуги, поддръжка на ИТ инфраструктурата, информационни системи.

Цели: Повишаване на квалификацията на български ИТ специалисти и подпомагане на международното сътрудничество в областта на информационните технологии.



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Сдружение Клъстер АЙТОС изпълнява проект № BG16RFOP002-2.009-0043 „Развитие на капацитета и интернационализацията на продуктите на Клъстер Айтос /ITOS/“ с финансовата подкрепа на ЕС чрез Европейския фонд за регионално развитие.



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- **Общата цел на проекта е да насърчи устойчивото развитие на "Клъстер АЙТОС" чрез осигуряване на подкрепа за интернационализация на новите и съществуващите продукти на клъстера, както и изграждане на споделена инфраструктура за общите клъстерни дейности.**
- Специфичните цели на проекта са:
 1. Повишаване степента на интеграция и сътрудничество на компаниите, работещи в сектора на информационните технологии в посока максимално използване на техния капацитет за разработка на конкуренти бизнес продукти и услуги и насърчаване активното присъствие на регионалния, националния и външните пазари. В рамките на проекта се извършва диверсификация на продуктите на Клъстер Айтос като с общи усилия на членовете на организацията се създава нов, конкурентен и търсен на регионалния пазар продукт – Платформа за облачно автоматизирано тестване на уеб и мобилни приложения.
 2. Осигуряване на подкрепа за развитието на споделена клъстерна инфраструктура чрез създаване и оборудване на Симулационен център и развойна лаборатория към него за разработване и тестване на нови услуги и продукти на Клъстер Айтос, които да допринесат за интернационализацията на организацията. Новосъздадения център се разполага в град Габрово.
 3. Насърчаване на клъстерния маркетинг чрез осигуряване на необходимия експертен персонал за създаване на сътрудничества и интернационализация на клъстерните продукти: наемане на експерт по интернационализация, ангажиране на консултантска компания, която да подпомогне навлизането на продуктите на пазара във Великобритания, както и разработване на Стратегия за интернационализация на Клъстера.
 4. Подпомагане развитието на "Клъстер АЙТОС" и привличането на нови членове чрез организиране и участие в събития за представяне на клъстера и неговите продукти в страната и чужбина: пазари за ново-разработената услуга са Сърбия, Босна, Франция, Белгия, Германия, Великобритания и Македония.
 5. Повишаване капацитета на Клъстера за създаване на сътрудничества и интернационализация чрез специализирани обучения, в които да вземат участие служители на членовете на Клъстера.

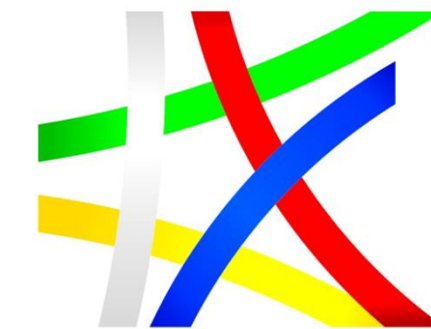


Сдружение Клъстер Айтос



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Съвременни технологии & предизвикателства



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Облачни технологии (Cloud computing)
- Big Data
- Internet of Things (IoT)
- Artificial Intelligence (AI)
- Blockchain, криптовалута
- Електронно правителство
- Software Defined Networks / Storage / DataCenter
- Bring Your Own Device (BYOD)
- Mobile First

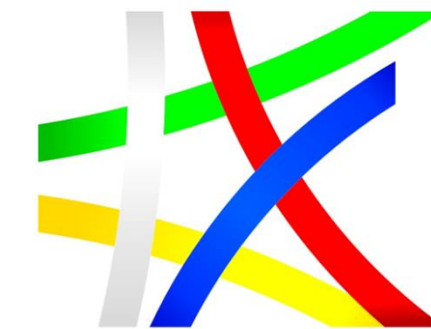


Сдружение Клъстер Айтос



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Съвременни регулации & предизвикателства



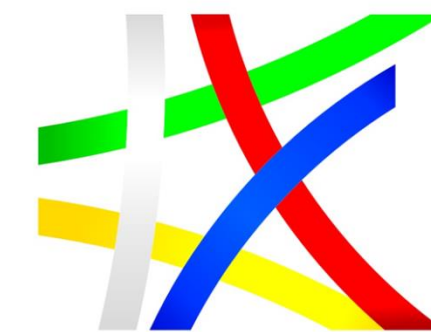
ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- PSD 2
- MiFID II
- GDPR
- PCI-DSS
- ISO27001
- ISO31000
- ePrivacy
- Cyber Security
- NIS Directive



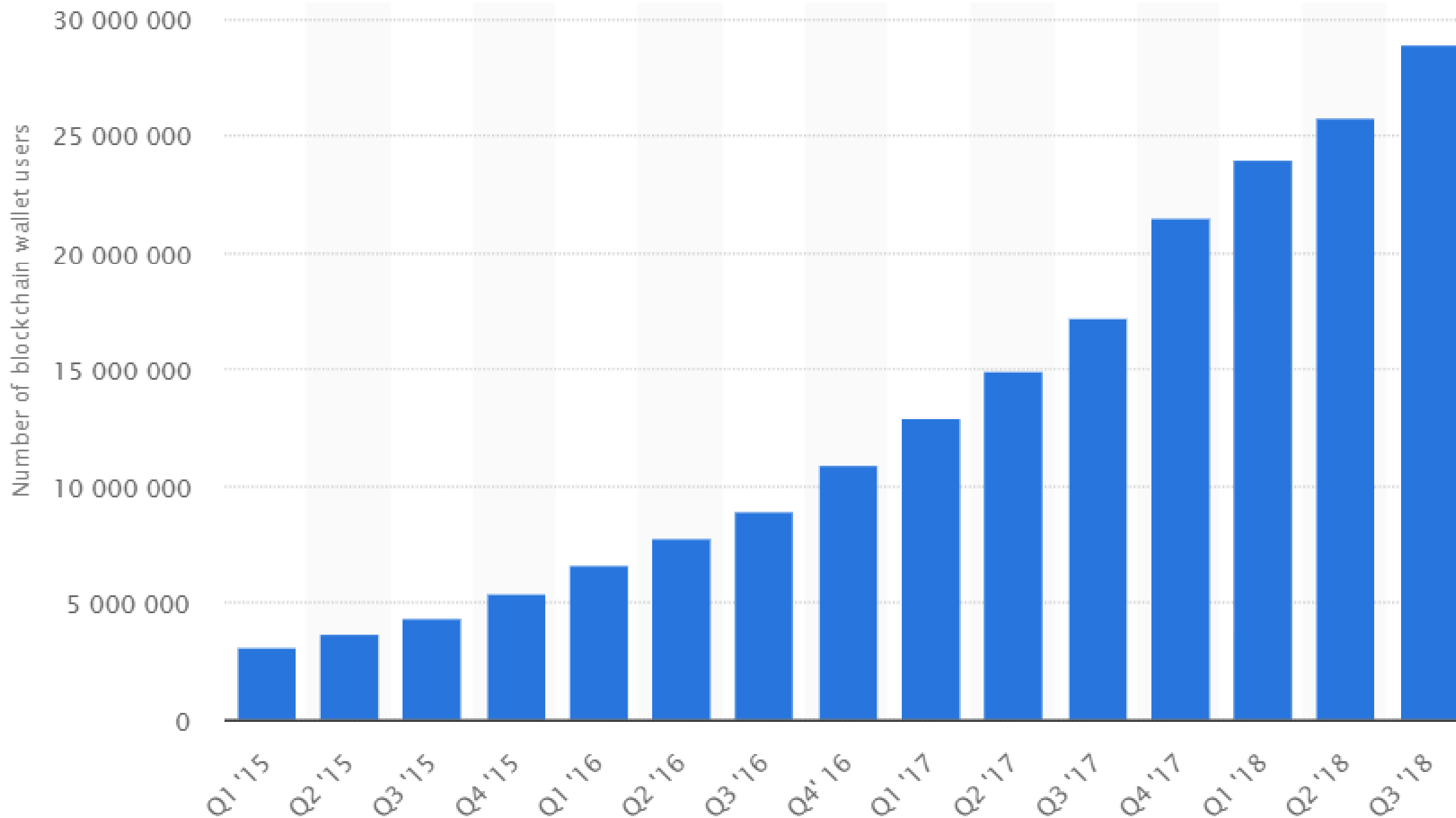
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Тенденции в информационния свят



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

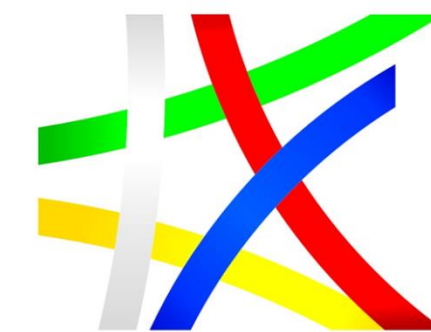
Number of Blockchain wallet users worldwide





ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

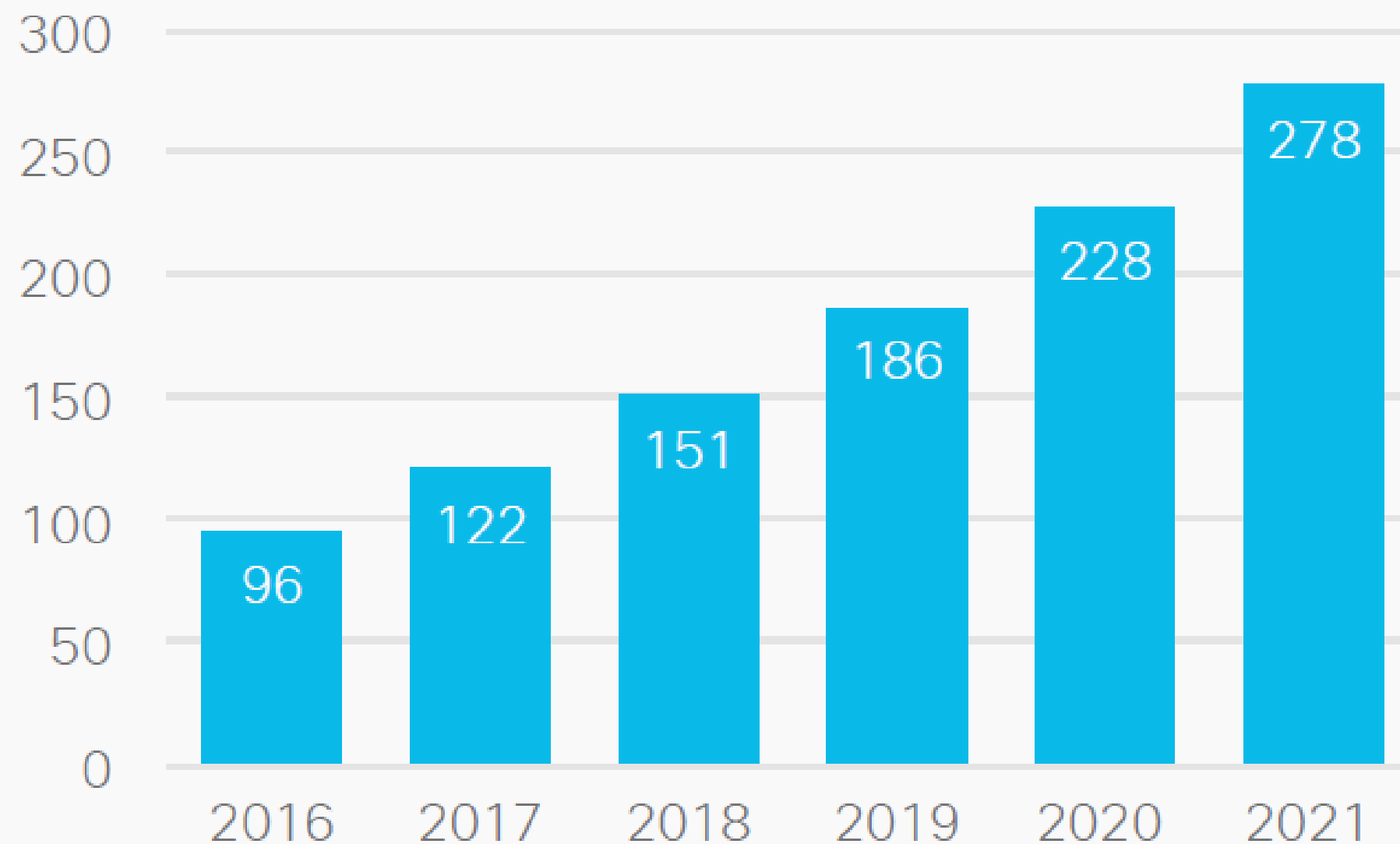
Годишно нарастване трафик



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

24% CAGR
2016–2021

Exabytes
per month

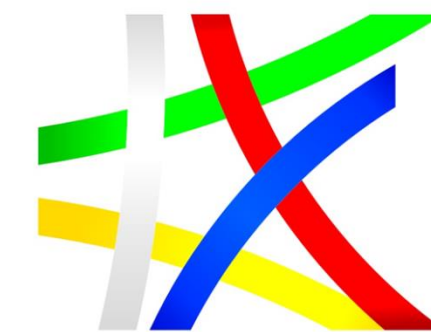


Cisco VNI Global IP Traffic Forecast, 2016–2021.



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

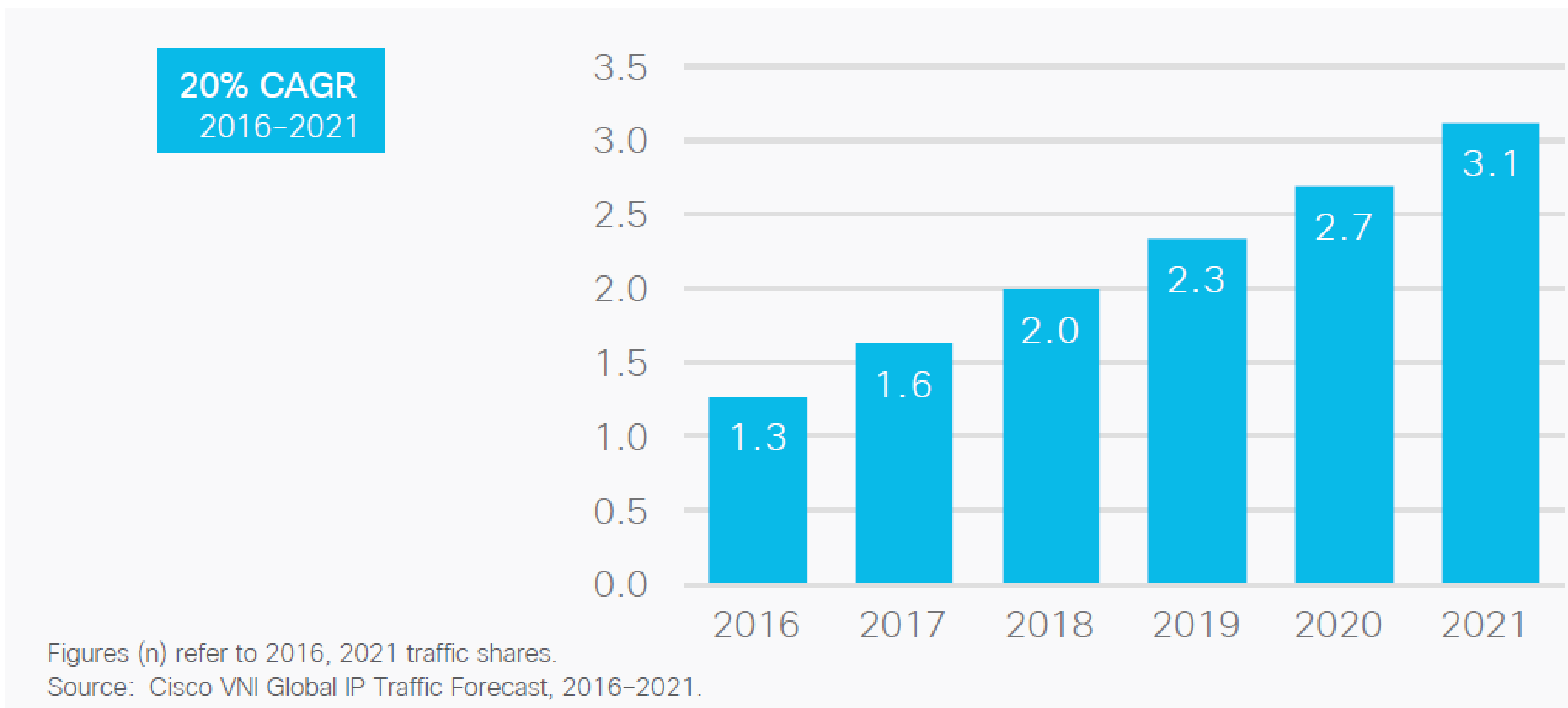
Distributed Denial-Of-Services



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

DDoS атаки с трафик над 1 Gbit/s, в милиони

Global DDoS attacks forecast, 2016-2021

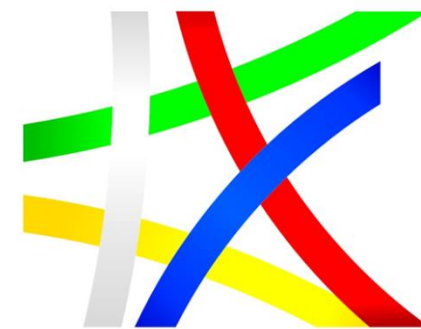




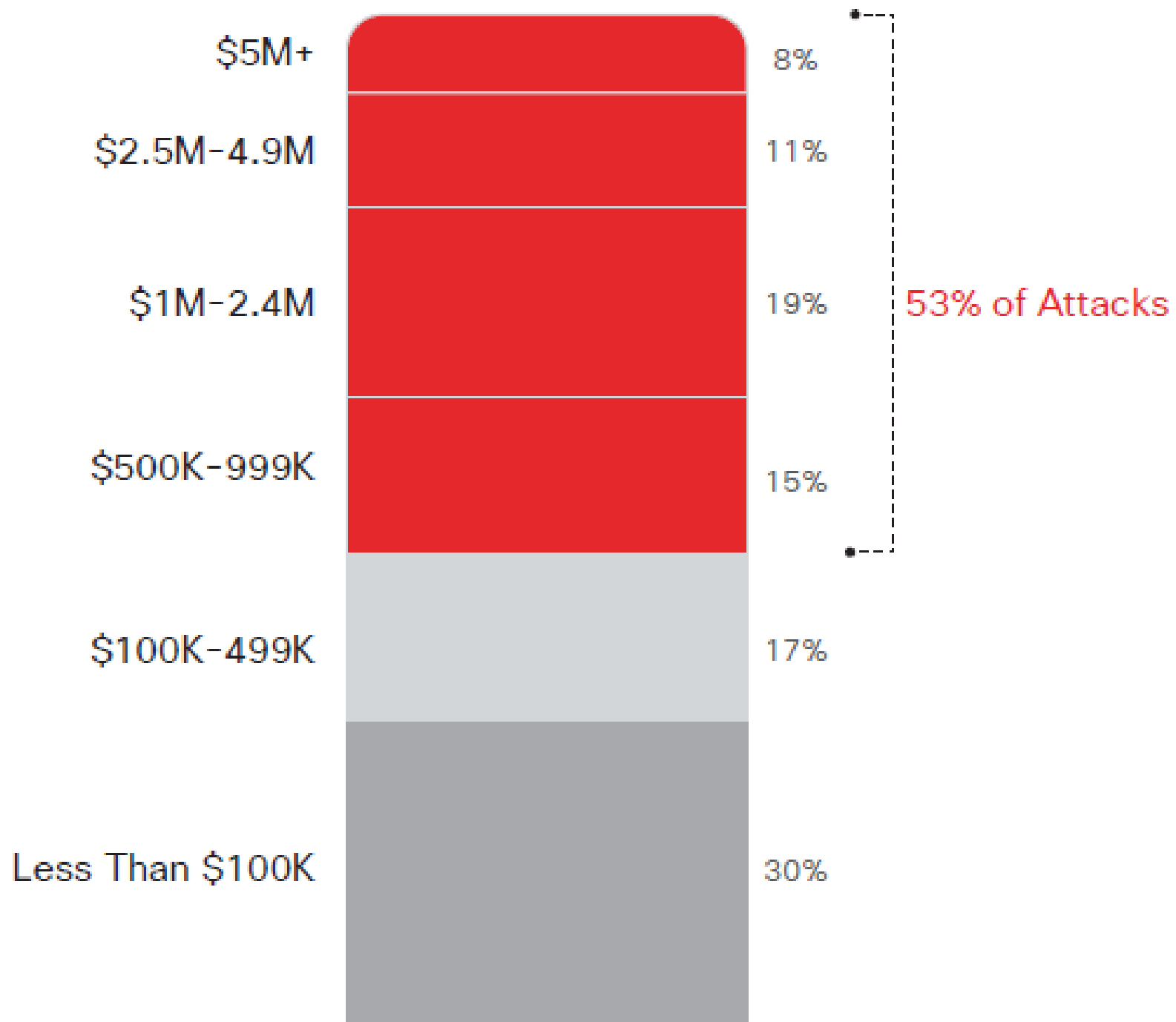
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Кражба на данни

Колко струва кражбата на данни и информация?



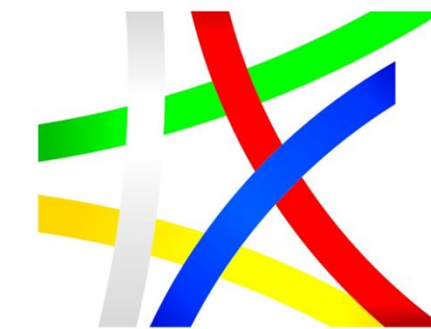
ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ





ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Съвременни заплахи



ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

\$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do

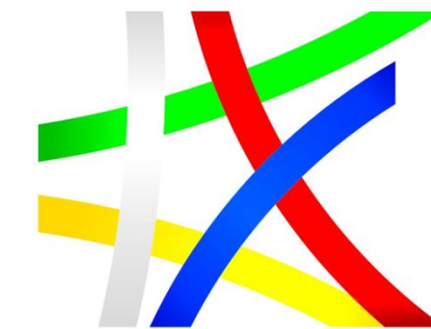
- \$1.1 billion worth of cryptocurrency was stolen in the first half of 2018, and it's relatively easy to do, according to cybersecurity company Carbon Black.
- "It's surprising just how easy it is without any tech skill to commit cybercrimes like ransomware," Carbon Black Security strategist Rick McElroy says
- The necessary malware, which even occasionally comes with customer service, costs an average of \$224 and can be as cheap as \$1.04 on the "dark web."

Source: CNBC



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Penetration тестове




ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Оценка на способността да защитим мрежи, приложения, данни, системи и потребители/клиенти от недоброжелателни хакери;
- Проверка на защитата на активите и репутацията на компанията за избягване на финансови загуби и негативна публичност, които могат да бъдат причинени от компрометиране на системите и данните на организацията;
- Предоставяне на подробна информация за действителни заплахи, които могат да бъдат експлоатирани;
- Идентифициране и оценка за това кои уязвимости са критични за организацията, кои са по-незначителни;
- Ефективни методи за повишаване сигурността на системите в организацията;
- Набелязване на зони за подобрения и аргументиране на бюджети;
- Оценка на риска

OWASP - Open Web Application Security Project


OWASP Top 10 - 2013	➔	OWASP Top 10 - 2017
A1 – Injection	➔	A1:2017-Injection
A2 – Broken Authentication and Session Management	➔	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	➡	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	➡	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	➔	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Decentralized Application Security Project (or DASP) Top 10 of 2018

 1. Reentrancy

 2. Access Control

 3. Arithmetic Issues

 4. Unchecked Return Values For Low Level Calls

 5. Denial of Service

 6. Bad Randomness

 7. Front-Running

 8. Time manipulation

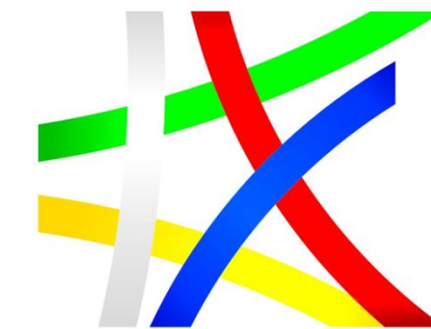
 9 Short Address Attack

- race to empty, recursive call vulnerability, call to the unknown
- Integer overflow and integer underflow
- Silent failing sends, unchecked-send
- gas limit reached, unexpected throw, unexpected kill, access control breached
- nothing is secret
- time-of-check vs time-of-use (TOCTOU), race condition, transaction ordering dependence (TOD)
- timestamp dependence
- off-chain issues, client vulnerabilities



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Други услуги за сигурност



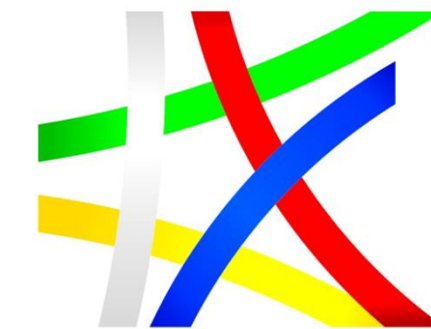
ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Одит на информационната сигурност
- Анализ на трафика
- Анализ на безжичната мрежа
- Внедряване на стандарти, политики и процедури за сигурност
- Анализ и оценка на риска
- Изработване на стратегия
- Изграждане, внедряване и изпълнение на процеси по управление на инциденти
- SOC – проактивен мониторинг и контрол
- Security Awareness обучения и учения



ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Благодаря за вниманието



ОПЕРАТИВНА ПРОГРАМА
**ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ**

Въпроси?

- <http://www.clusteritos.org/>
- office@clusteritos.org