НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

О кибербразведке и кибербезопасности КВО

Георгий Георгиевич Петросюк,
директор департамента информационных технологий

Иван Сергеевич Калачев,
начальник отдела департамента информационных технологий

ФГБУ «Национальный исследовательский центр «Институт им. Н. Е. Жуковского»

г. Москва, 2020

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

ОСНОВНОЙ ЭТАП КОМПЬЮТЕРНОЙ АТАКИ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

КИБЕРРАЗВЕДКА

Основные «разведовательные» силы:

- Производители оборудования, транспорта и бытовой техники
- Производители системного и прикладного программного обеспечения
- Производители аппаратного обеспечения, сетевого и периферийного оборудования, средств информатизации и автоматизации, мобильных устройств
- Производители систем и средств информационной безопасности
- Владельцы WEB ресурсов, облачных сервисов и WEB приложений
- Деструктивные силы

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

КИБЕРРАЗВЕДКА

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Производители программного обеспечения
(примеры)

Windows 10 собирает следующие типы данных (перечень не полный):

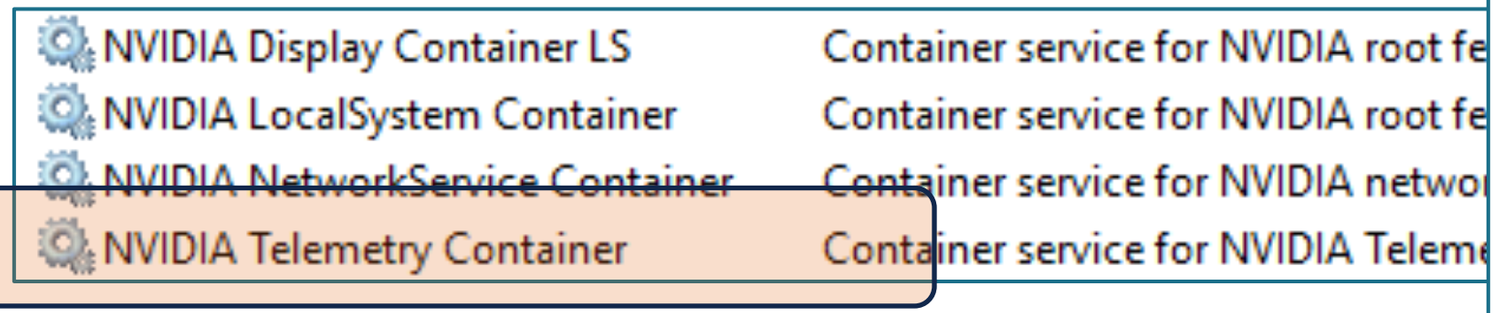
- имя ОС, информация о версии, сборке и языке;
- **Organization ID, user ID, Device ID, Device class (Desktop, Server, Mobile);**
- **параметры устройства (параметры панели управления, параметры реестра);**
- **характеристики устройства (данные CPU, OEM, BIOS, HDD, RAM, является ли виртуальной машиной, камера устройства);**
- предпочтения и настройки для устройства (BitLocker, SecureBoot);
- **данные о подключенной к устройству периферии (HWID);**
- **информация о сети устройства (IP address, Hostname, Domain, Proxy, GW, DHCP, DNS, AP MAC addr, IMEI, MCCO, SSIDs, BSSIDs);**
- **данные об использовании приложений (SMS, MMS, Vcard, входящие и исходящие звонки);**
- данные о состоянии приложения или продукта;
- **настройки пользователя (панель управления, параметры);**
- health and crash информация об устройстве (лог-файлы, файлы .doc, .ppt, .csv);
- данные о производительности устройства и его надежности;
- **данные об обновлениях, установленных приложениях и истории установок;**
- **данные о потребляемом контенте (фильмы, ТВ, книги, музыка, фото);**
- **данные браузеров Microsoft и данные Cortana**;
- **данные о поисковой активности (данные рукописного ввода, ввода с клавиатуры и устной речи, данные журнала браузера, текст, набранный в поисковые строки, текст автозаполнения, URLs);**
- **информация о лицензии и дате покупки.**
- и др. информация

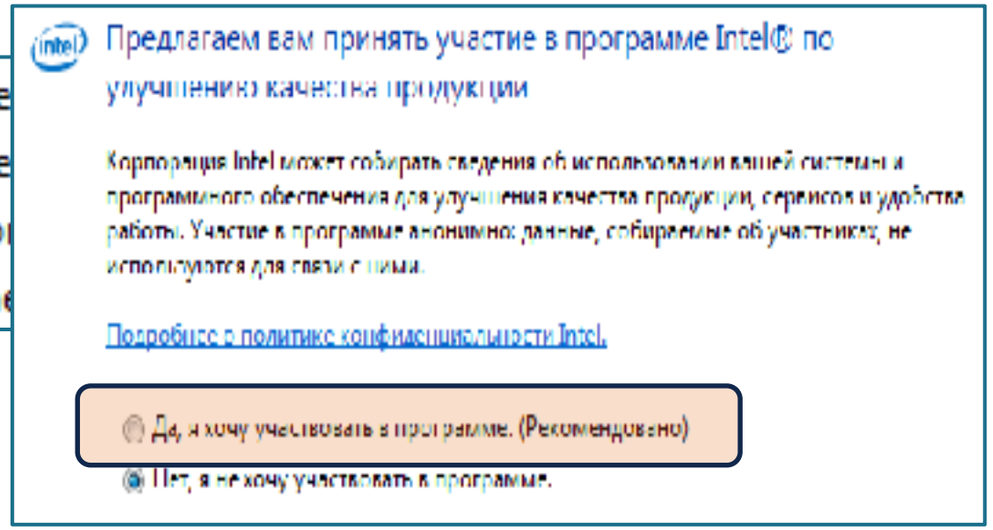
https://docs.microsoft.com/en-us/windows/configuration/windows-diagnostic-data
https://privacy.microsoft.com/ru-RU/

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Производители оборудования, систем и средств информационной безопасности
(примеры)

Практически в каждом современном программном или аппаратном продукте **имеется функция слежения и отправки статистики**, как правило, включенная по умолчанию. Об этом может не говориться в пользовательском соглашении.





4. КОНФИДЕНЦИАЛЬНОСТЬ И СБОР ЛИЧНОЙ ИНФОРМАЦИИ

В кратком изложении **мы собираем, храним и используем определенную информацию о вас, вашем устройстве** (как определено ниже) **и его взаимодействии с другими устройствами.** Некоторая часть этой информации может использоваться для вашей идентификации, включая, помимо прочего, **имя, адрес, номер телефона, адрес электронной почты, информацию о кредитной карте, изображение лица, образец голоса или другие биометрические данные** (в совокупности «Личные данные»), и может содержать **данные личного характера, хранящиеся в файлах вашего устройства**.

По этим причинам **вы не сможете отказаться от сбора подобной информации**, кроме как путем удаления соответствующего Продукта.

https://www.avira.com/ru/end-user-license-agreement-terms-of-use

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Сбор данных и телеметрия в браузерах

Данные о взаимодействии: Firefox отправляет нам данные о вашем взаимодействии с этим браузером (количество открытых вкладок и окон, количество посещенных страниц, число и тип установленных дополнений, продолжительность сеансов и т. д.) и об использовании функций Firefox, предлагаемых компанией Mozilla или нашими партнерами (таких, как поиск Firefox и поиск по партнерским ссылкам).

Технические данные: Firefox отправляет нам данные о версии и языке браузера, операционной системе устройства и конфигурации оборудования, объеме памяти, сбоях и ошибках, результатах автоматизированных процессов, таких как обновление, безопасный браузинг или активация. Когда Firefox отправляет нам данные, временно передается и ваш IP-адрес (как элемент журналов нашего сервера).

Поисковые запросы: Поисковые запросы в диспетчере дополнений отправляются в компанию Mozilla, чтобы предоставить вам с рекомендуемые дополнительные компоненты.

Данные о взаимодействии: Мы получаем сводные данные о посещениях сайта AMO и доступе к диспетчеру дополнений в Firefox, а также об использовании контента на этих страницах. Вы можете получить дополнительную информацию о методах обработки данных на веб-сайтах Mozilla.

Технические данные для занесения нежелательных дополнений в черный список: Браузеры Firefox для ПК и Android периодически подключаются к службам Mozilla для защиты пользователей от вредоносных дополнений. Для обновления черного списка ваших дополнений требуются сведения о версии Firefox, языке, операционной системе устройства и установленных дополнениях. Подробнее.

Получение сведений о веб-странице и технических данных для службы SafeBrowsing Google: Чтобы защитить вас от вредоносного контента, браузер Firefox отправляет основную информацию о загрузках нераспознанных файлов (включая имя файла и URL-адрес, с которого он был загружен) в службу SafeBrowsing Google.

17.02.2020

Более 500 вредоносных расширений для Chrome собирали данные пользователей. Вредоносный код внедрял рекламу в браузеры и перенаправлял пользователйей на фишинговые сайты.

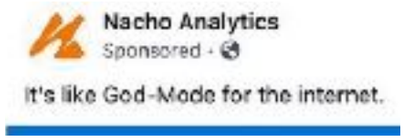
https://www.securitylab.ru/news/505103.php

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Сбор данных расширениями браузеров.

Примеры.

«Режим бога для Интернета»:



Отслеживались действия миллионов пользователей через расширения Chrome и Firefox почти в реальном режиме времени (с часовой задержкой).

Microsoft OneDrive	Файлы с хостинга OneDrive, включая налоговые декларации
Nest	Видеозаписи с камер безопасности Nest
NetApp	URL конференций Zoom с netapp.zoom.us
Palo Alto Networks	**Данные из корпоративной сети**
Pfizer	**Данные из корпоративной сети**
Roche	**Данные из корпоративной сети**
Skype	URL из чатов Skype
SpaceX	**Данные из корпоративной сети**
Symantec	**Данные из корпоративной сети**
Tesla	**Данные из корпоративной сети**

- GPS-координаты пользователей;
- налоговые декларации, деловые документы, слайды корпоративных презентаций на OneDrive и других хостингах;
- видео с камер безопасности Nest;
- номера VIN недавно купленных автомобилей, имена и адреса их владельцев;
- Вложения к сообщениям Facebook Messenger и фотографии Facebook, даже отправленные приватно;
- данные банковских карточек;
- маршруты путешествий;
- и многое другое.

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Сбор данных пользователей WEB-сайтами

(примеры)

xakep.ru

- xakep.ru
- chimpstatic.com
- doubleclick.net
- fonts.googleapis.com
- google-analytics.com
- googleadservices.com
- googletagservices.com
- rambler.ru
- yandex.ru
- yastatic.net

Крупные Банки

- google-analytics.com
- ssl.google-analytics.com
- googletagmanager.com
- www.googletagmanager.com
- yandex.ru
- mc.yandex.ru

- fonts.googleapis.com
- google-analytics.com
- www.google-analytics.com
- googletagmanager.com
- www.googletagmanager.com
- gstatic.com

Российская газета

- static.1dmp.io
- adfox.ru
- ads.adfox.ru
- ajax.googleapis.com
- chartbeat.com
- static.chartbeat.com
- cloudflare.com
- cdnjs.cloudflare.com
- fonts.googleapis.com
- google-analytics.com
- www.google-analytics.com
- gstatic.com
- fonts.gstatic.com

Скрипты Google Analytics установлены на 55,3% сайтов в интернете.

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Сбор данных пользователей WEB-сайтами

(примеры)

Historical trends in the usage statistics of traffic analysis tools for websites

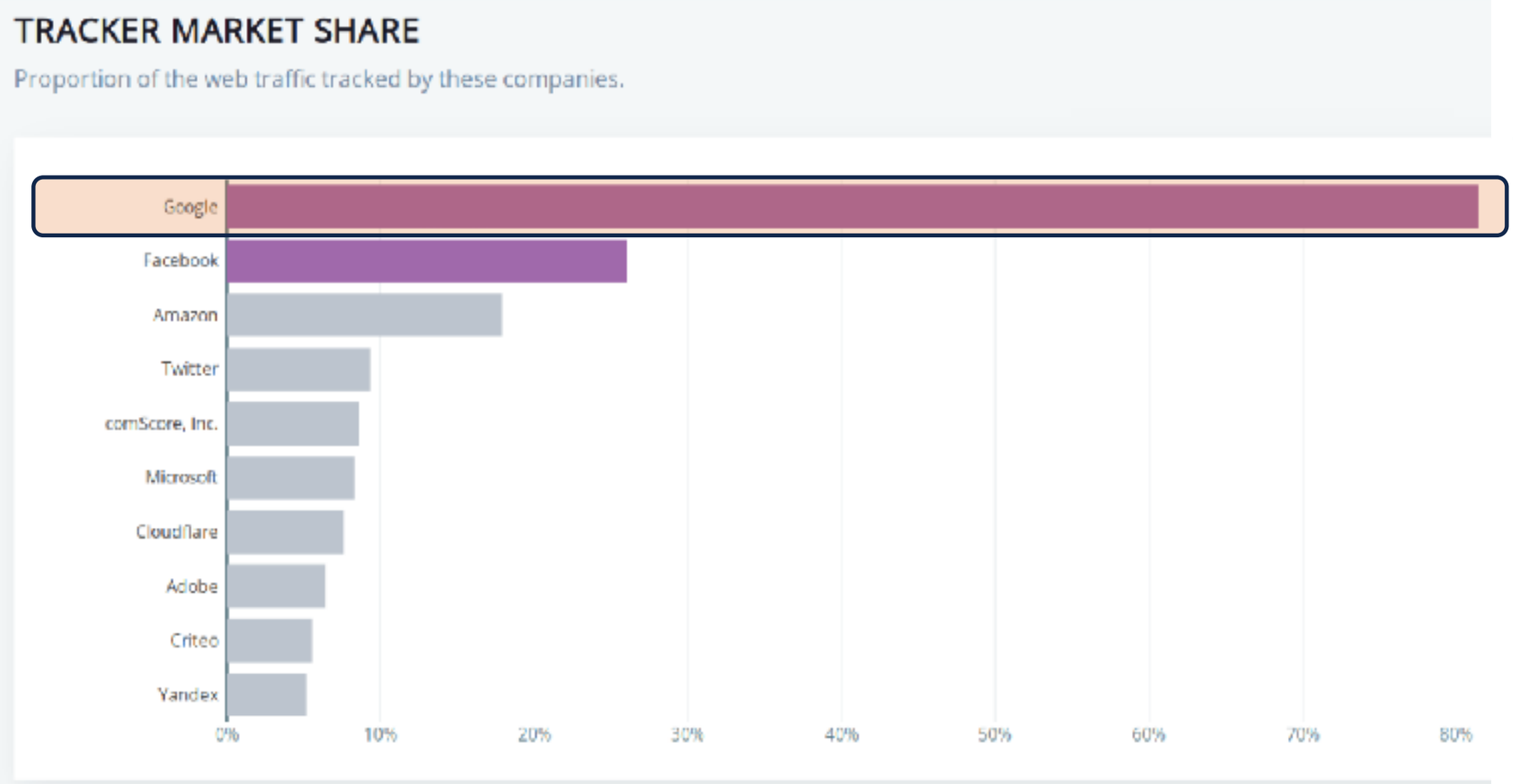
This report shows the historical trends in the usage of traffic analysis tools since September 2019.

	2019 1 Sep	2019 1 Oct	2019 1 Nov	2019 1 Dec	2020 1 Jan	2020 1 Feb	2020 1 Mar	2020 1 Apr	2020 1 May	2020 1 Jun	2020 1 Jul	2020 1 Aug	2020 1 Sep	2020 16 Sep
None	34.1%	34.5%	34.9%	34.9%	34.9%	35.1%	35.2%	36.1%	36.2%	35.1%	34.7%	34.7%	34.3%	34.4%
Google Analytics	56.0%	55.9%	55.5%	55.5%	55.4%	55.1%	55.0%	53.8%	53.6%	54.6%	55.0%	55.0%	55.0%	55.2%
Facebook Pixel	8.5%	8.5%	8.5%	8.7%	8.0%	8.0%	9.1%	9.0%	9.0%	9.3%	9.4%	9.5%	9.7%	9.7%
Yandex.Metrica	5.8%	5.8%	5.9%	6.1%	6.5%	6.7%	6.9%	7.0%	7.2%	7.3%	7.4%	7.4%	7.4%	7.4%
WordPress Jetpack	4.8%	4.7%	4.7%	4.7%	4.6%	4.6%	4.6%	4.6%	4.6%	4.7%	4.8%	4.8%	4.8%	4.8%
Hotjar	2.7%	2.7%	2.7%	2.7%	2.8%	2.8%	2.8%	2.8%	2.8%	2.9%	2.9%	2.9%	2.9%	3.0%
LiveInternet	2.3%	2.2%	2.2%	2.3%	2.4%	2.5%	2.5%	2.5%	2.5%	2.6%	2.6%	2.5%	2.5%	2.5%
New Relic	1.5%	1.4%	1.4%	1.4%	1.4%	1.4%	1.5%	1.5%	1.4%	1.4%	1.3%	1.3%	1.3%	1.3%
Matomo	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.0%	1.0%	0.9%	1.0%	1.0%	1.0%	1.0%	1.0%
Top.Mail.Ru	0.8%	0.8%	0.8%	0.9%	0.9%	0.9%	0.9%	0.9%	1.0%	1.0%	1.0%	1.0%	1.0%	0.9%
StatCounter	0.9%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%
Baidu Analytics	0.8%	0.8%	0.8%	0.7%	0.7%	0.6%	0.6%	0.6%	0.7%	0.7%	0.7%	0.7%	0.7%	0.7%

https://w3techs.com/technologies/history_overview/traffic_analysis/all

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

ЛИДЕРЫ СЛЕЖКИ



Топ трекеров в Интернете, ранжированных по доле веб-трафика, из которого они собирают данные.

Google собирает данные более чем с 80% измеренного веб-трафика.

Источник: WhoTracks.me, компания Cliqz GMBH.

29.01.2020

Трекеры Facebook установлены на 30% из 10 000 самых популярных сайтов. Аудитория достигает **1 миллиарда человек в месяц.**

https://habr.com/ru/news/t/486012/

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Сбор данных пользователей веб-сервисов
(примеры технологий сбора)

Отслеживание IP адреса, с которого пришел запрос (как правило, это «белый IP-адрес» интернет шлюза компании/организации)

Отслеживание внутреннего IP адреса компьютера в корпоративной сети, с которого пришел запрос. Совместно с IP-адресом шлюза можно уникально идентифицировать компьютер в локальной сети организации.

Использование особенности протокола HTTP, а именно – referer, который является одним из заголовков запроса клиента. Содержит URL источника запроса. Если перейти с одной страницы на другую, referer будет содержать адрес первой страницы.

Использование файлов cookie

Использование «неубиваемых cookie» или Evercookie. Технология использования cookie, сохраняющая их в 13 местах на компьютере пользователя. Объединяет в себя HTTP-cookie, Flash cookies или Local Shared Objects и контейнеры HTML5.

CAPTCHA

«**Веб-маяки**» - элементы программного кода, включенные в веб-страницы, электронные сообщения и рекламу, которые уведомляют владельца о просмотре этих страниц, электронных сообщений и рекламы или о переходе по соответствующим ссылкам, в том числе на нескольких устройствах и доменах

Использование отпечатка браузера или Browser Fingerprinting - уникальный идентификатор конфигураций веб-браузера и операционной системы, который формируется на основе собранных данных различными технологиями отслеживания. Позволяет создавать «цифровой отпечаток» компьютера и дает возможность идентифицировать уникальный компьютер (и в корпоративной сети тоже) с точностью до 100%.

Использование истории посещенных пользователем вебресурсов.

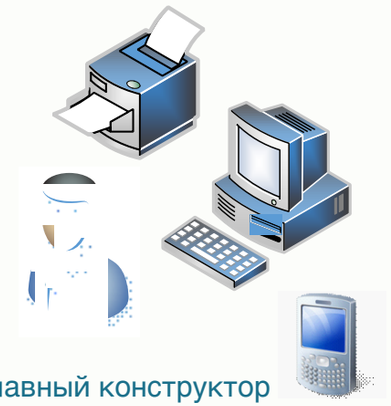
Публичные сервисы службы доменных имён (Google DNS, Яндекс DNS). Многие организации используют в качестве серверов для преобразования IP адресов в доменные имена глобальные публичные, где данные журналируются и анализируются, дополняя общую картину собранной информации.

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

«ПРИНУДИТЕЛЬНАЯ» КИБЕРРАЗВЕДКА

intel ... Microsoft ... facebook ... SIEMENS Ingenuity for life ... GE ... amazon.com Google

СБОР ДАННЫХ НА ЗАКОННОМ ОСНОВАНИИ



Главный конструктор
Иванов М.И.,
ivanovmi@corp.ru

Корпоративная сеть

ОС Windows 7/8/10/, прикладное и системное ПО:
IP адрес, конфигурация оборудования и подключенные устройства, **домен, учетная запись, почтовый адрес**, версия ОС, **установленные приложения**, их версии и конфигурации, **средства и системы информационной безопасности**, какие WEB ресурсы посещает, какие документы скачивает из Интернет, какие документы обрабатывает и с кем взаимодействует и т.д.

Главный бухгалтер
Иванова Н.И.,
ivanovni@corp.ru

Администратор АСУ,
Иванов А.М.
ivanovni@corp.ru

объект КИИ

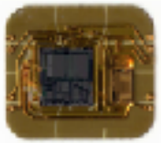
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

СБОР ДАННЫХ О ПРОМЫШЛЕННЫХ СИСТЕМАХ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

МОБИЛЬНАЯ КИБЕРРАЗВЕДКА

SIM карта



Процессор, память, I/O, операционная система, файловая система, приложения

Baseband-процессор

Процессор, память, I/O, операционная система, файловая система

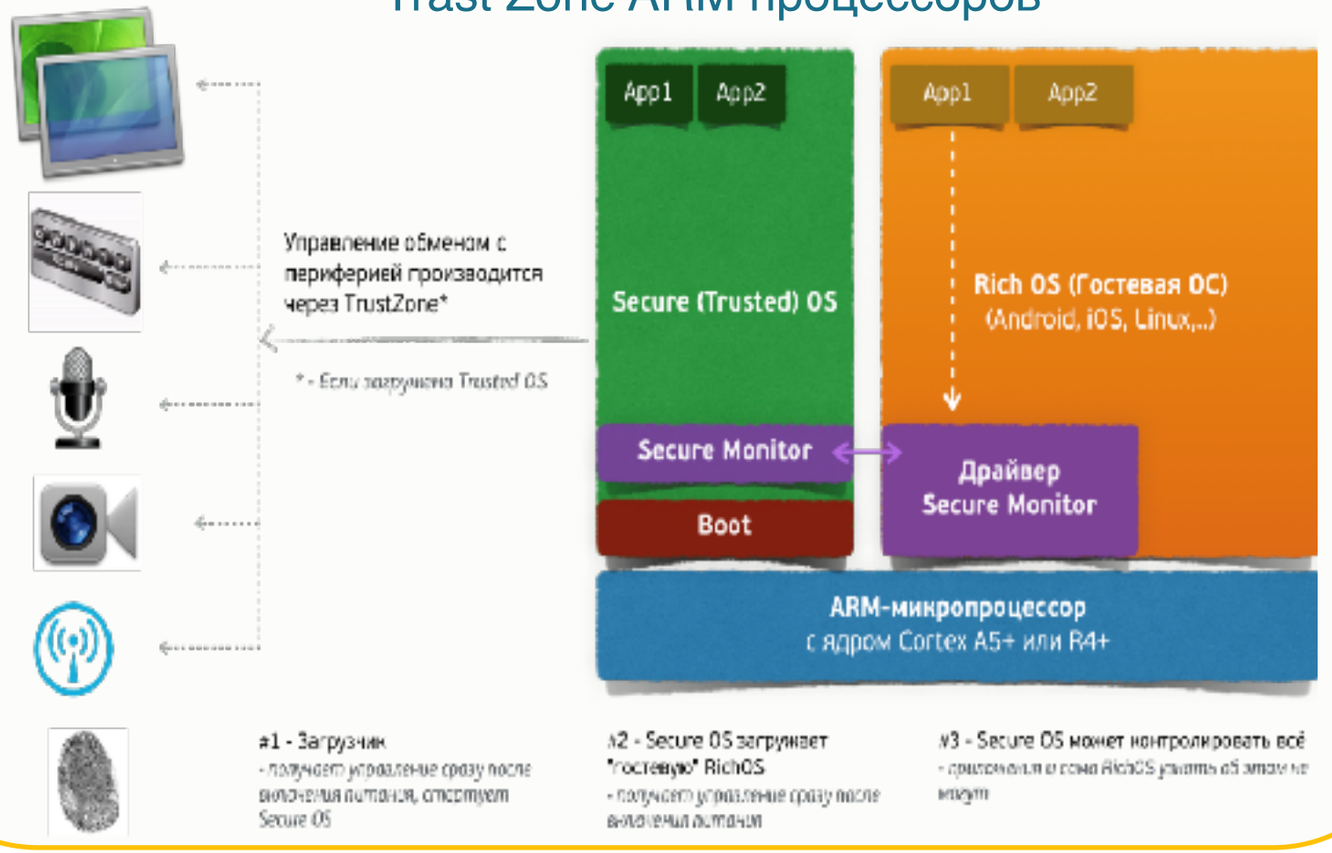
Радиомодуль

2G, 3G, 4G, 5G, CDMA, Wi-Fi, Bluetooth, NFC TCP/IP

Видео/фото камеры и микрофоны

Сканер отпечатков пальцев

Trast Zone ARM процессоров



Датчики

- GPS/ ГЛОНАСС
- акселерометр
- гироскоп
- магнетометр
- Холла
- гравитации
- вращения
- барометр
- гигрометр
- педометр
- температурный
- приближения
- света
- пульсометр

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

«Следящие» лидеры – США и не только.

25.10.2018

После анализа более **959 тыс.** приложений из американских и британских магазинов установлено: **88,4%** — могут обмениваться данными со структурами, принадлежащими **Google, Facebook** (**42,5%**), **Twitter** (**33,8%**), **Verizon** (**26.27%**), **Microsoft** (**22.75%**), **Amazon** (**17,91%**) и многие другие.
90% приложений на Android делятся информацией о пользователях с минимум пятью компаниями.

https://hightech.fm/2018/10/25/android-shares

08.02.2020

Министерство внутренней безопасности США подтвердило, что отслеживало перемещение миллионов людей через их смартфоны. Данные о местоположении берутся из обычных приложений и игр, которые просят разрешение на использование геопозиции.

https://www.iphones.ru/iNotes/ssha-priznalis-v-slezhke-za-millionami-smartfonov-v-realnom-vremeni-02-08-2020

15.08.2020

В сотни мобильных приложений (около 500) внедрено шпионское ПО, разработанное военными США.

https://safe.cnews.ru/news/top/2020-08-12_v_sotni_mobilnyh_prilozhenij

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

«Следящие» лидеры – США и не только.

15.09.2020

Китайская компания собирала персональные данные влиятельных людей по всему миру.

В утёкшей базе данных обнаружились досье на 24 миллиона человек.

Данные включали:

дата рождения, адреса, семейное положение, фотографии, список родственников, аккаунты в соцсетях, образование, профессиональные достижения и список преступлений. СМИ отмечают, что большинство информации собрано из открытых источников, но есть и конфиденциальные данные, например банковские записи и заявления о приёме на работу.

https://www.securitylab.ru/news/512101.php

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

ПРИНУДИТЕЛЬНАЯ «ЦИФРОВАЯ ПРОЗРАЧНОСТЬ»

США

СБОР ДАННЫХ НЕ ОГРАНИЧЕН

Предположение!

Электронное досье

(формируется в США)

Иванов М.И., рост, вес, заболевания, увлечения, …..
Семейное положение …..
Проживает …..,
Дружит с Ивановым А.М. и
Квартиру убирает пылесос Robot, схема и изображения прилагаются. личная почта: Ivanov@google.com, **работает главным конструктором ПАО «Corp»,** на работу ездит по маршруту №21 трамвая с Ивановой Н.И. служебная почта: ivanovmi@corp.ru

….

И еще как минимум, сотни (или тысячи) других типов собираемых в реальном времени данных!

Изменения в реальном времени!

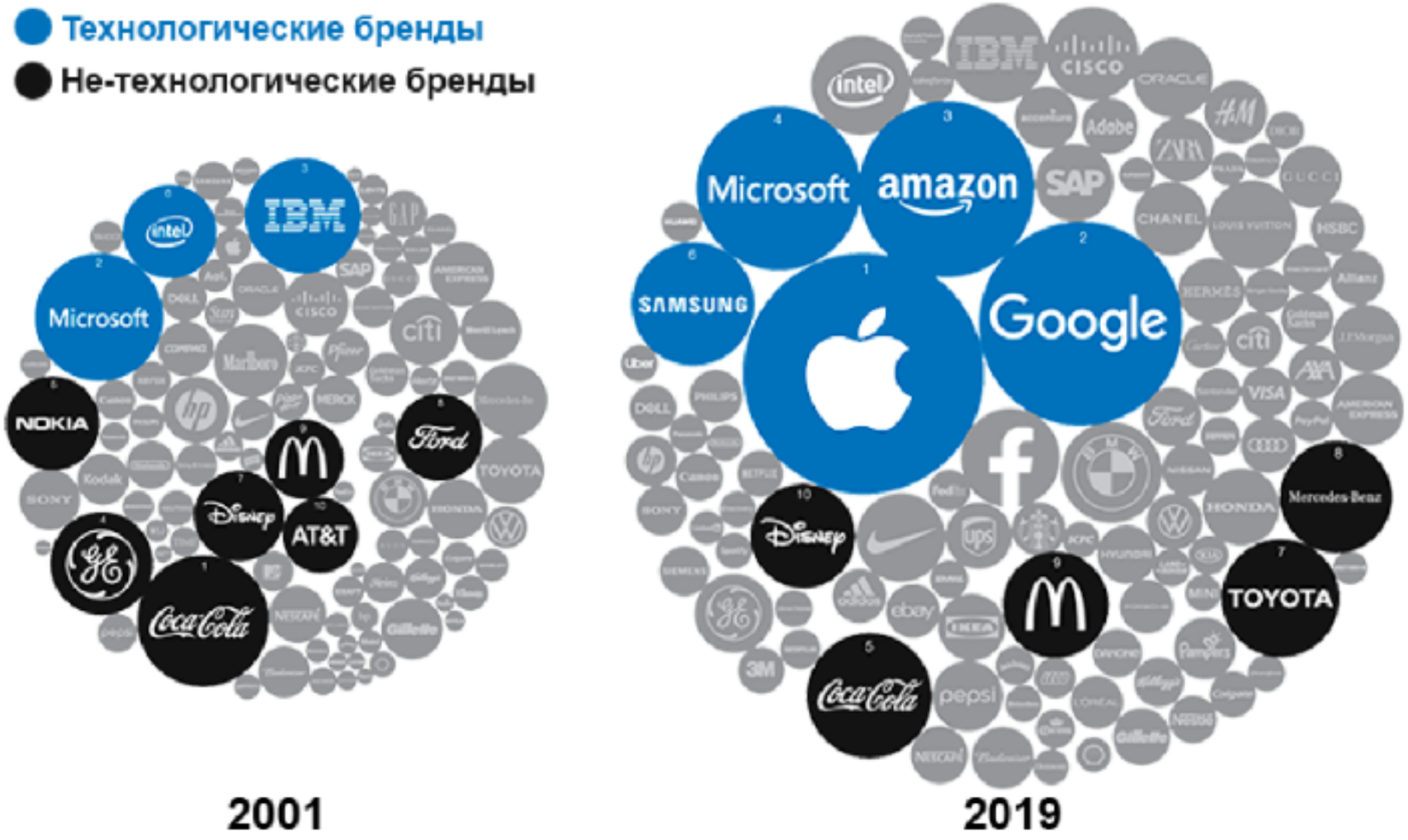
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

НАДЗОР - КАПИТАЛИЗМ

21.01.2019

Профессор Ш.Зубофф из Гарварда считает, что: **«Facebook, Google и Amazon не просто собирают наши данные — они строят новую версию капитализма, основанную на слежке – «надзор-капитализм» («шпионящий капитализм»).**

https://hightech.plus/2019/01/21/sistema-manipulyacii-google-i-facebook-vihodit-iz-pod-kontrolya



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Крупнейшие мировые поставщики облачных услуг

Облака.
Примеры.

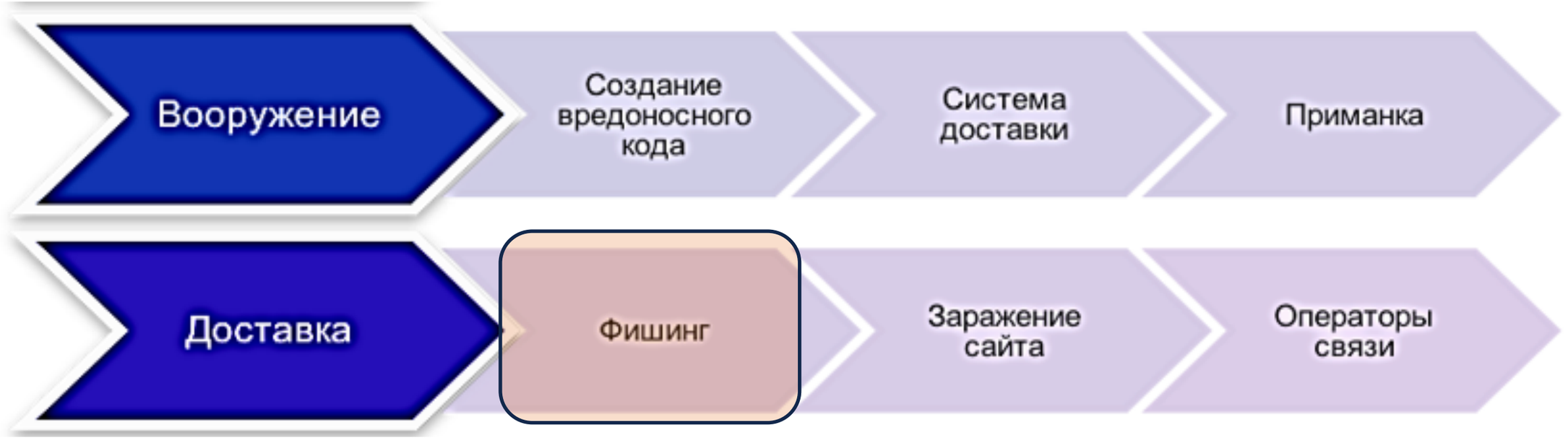
Размещение ЦОД крупнейших мировых поставщиков облачных услуг

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Информация
о корпоративных сетях наших учреждений, предприятий и организаций и персональная информация о наших сотрудниках в реальном времени, на законном основании или скрытно собирается и обрабатывается в основном за пределами РФ в компаниях, находящихся в большинстве своем под юрисдикцией одной страны – США

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

КИБЕРБЕЗОПАСНОСТЬ КВО



28.02.2019

Исследование Microsoft: за 2018 год число фишинговых атак выросло на 350%

https://news.microsoft.com/ru-ru/security-intelligence-report/

04.12.2019

Фишинг является основным вектором проникновения в организации госсектора. По данным компании Positive Technologies, с него начинают атаку **87%** APT-группировок.

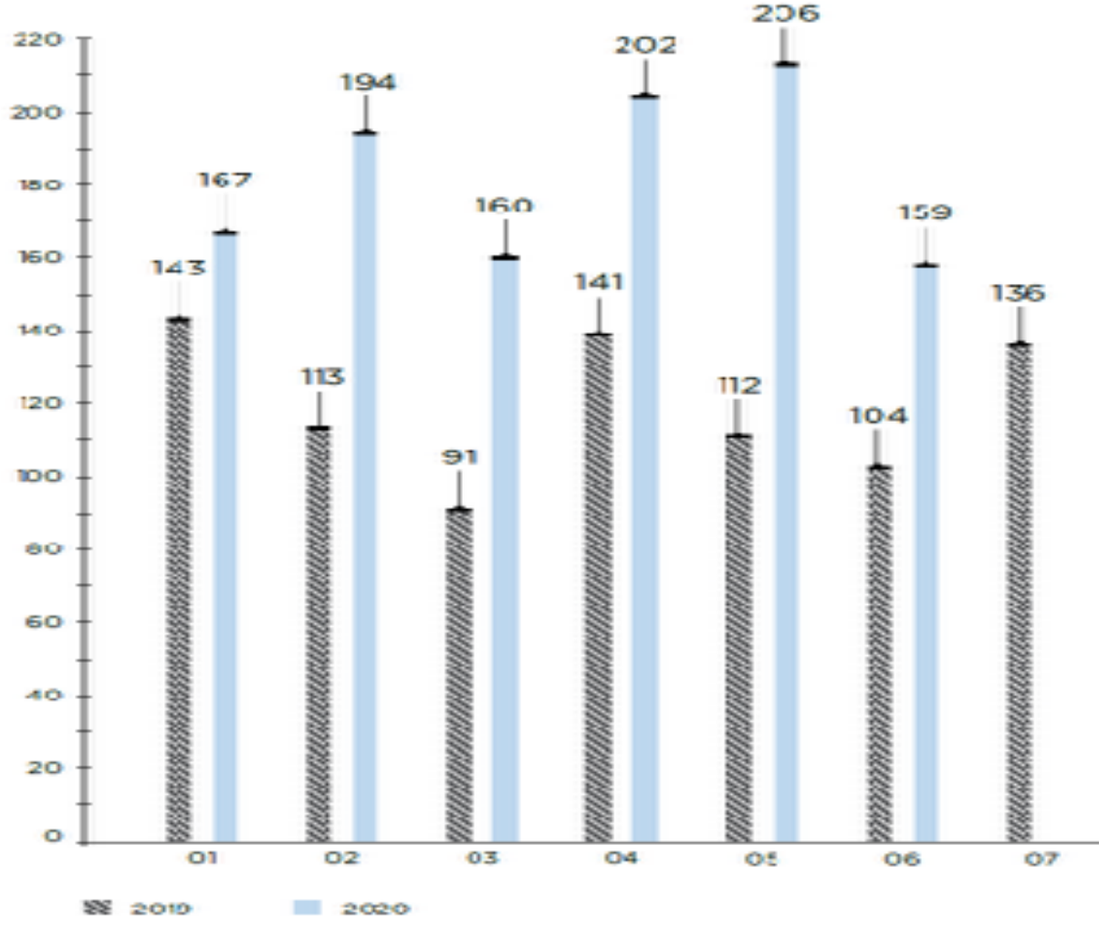
https://www.securitylab.ru/analytics/503090.php

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

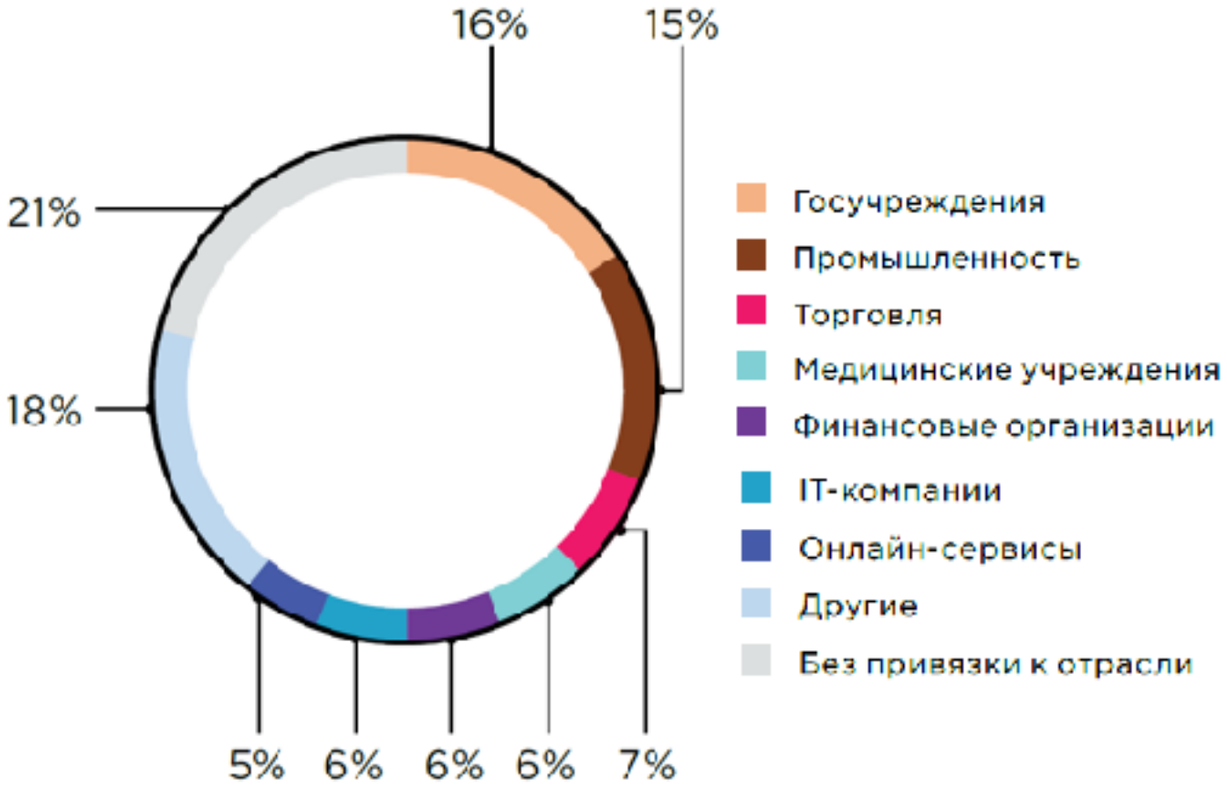
КИБЕРБЕЗОПАСНОСТЬ КВО

16.06.2020.

Positive Technologies - итоги второго квартала 2020 года. Продолжается фиксироваться преобладание **целенаправленных атак** над массовыми - **63%**. Наибольший интерес представляют **государственные учреждения, промышленные компании, финансовый сектор и сфера науки и образования.**



https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

КИБЕРБЕЗОПАСНОСТЬ КВО

29.11.2019.

Специалисты компании Group-IB в 2019 году выявили **38 атакующих хакерских группировок, за которыми стояли государства**, а 2019 год стал годом открытых военных кибероперaций.

Объекты критической инфраструктуры многих стран на сегодняшний день уже скомпрометированы.

https://www.anti-malware.ru/news/2019-11-29-1447/31430

14.08.2020

Хакерская группировка атакует банки и **энергетические компании.**

https://www.securitylab.ru/news/511161.php

09.09.2020.

Вымогатель Netwalker атаковал крупнейшего **энергопоставщика** Пакистана – компании K-Electric, что привело к сбою в работе её биллинговых и online-сервисов

https://www.securitylab.ru/news/511884.php

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Специальные службы

Внутренняя организационная структура Центра по кибербразведке ЦРУ, включает, как минимум, пять подразделений:

- **группа инженерных разработок** (Engineering Development Group, EDG) создает и тестирует бэкдоры, эксплоиты, трояны и вирусы;
- **отдел мобильных устройств** (Mobile Devices Branch, MDB) занимается поиском уязвимостей в операционных системах Android, iOS и Windows;
- **отдел интегрированных устройств** (Embedded Devices Branch, EDB) разрабатывает механизмы взлома интернета вещей;
- **отдел автоматизированных имплантатов** (Automated Implant Branch, AIB) разрабатывает атакующие системы для автоматического заражения вредоносными программами и контроля системы пользователей Windows, Mac OS X, Solaris, Linux;
- **отдел сетевых устройств** (Network Devices Branch, NDB) занимается атаками на инфраструктуру интернета и веб-серверы.

https://www.infowatch.ru/resources/analytics/leaks-monitoring/17457

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

СПАСИБО ЗА ВНИМАНИЕ!

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ИМЕНИ Н.Е. ЖУКОВСКОГО

Дополнительная информация

1. . Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей. Часть 7 // Защита информации. Инсайд. - 2019. - №6 (90)

2. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей. Часть 6 // Защита информации. Инсайд. - 2019. - №5 (89)

3. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев., С.Л. Груздев. О конфиденциальности корпоративных сетей. Часть 5 // Защита информации. Инсайд. - 2019. - №3 (87)

4. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей. Часть 4 // Защита информации. Инсайд. - 2018. - №6 (84)

5. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей. Часть 3 // Защита информации. Инсайд. - 2018. - №5 (83)

6. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей. Часть 2 // Защита информации. Инсайд. - 2018. - №4 (82)

7. Г.Г. Петросюк, И.С. Калачев, А.Ю. Юршев. О конфиденциальности корпоративных сетей // Защита информации. Инсайд. - 2018. - №3 (81)

https://www.aladdin-rd.ru/company/pressroom/articles/o-konfidencialnosti-korporativnyh-setej