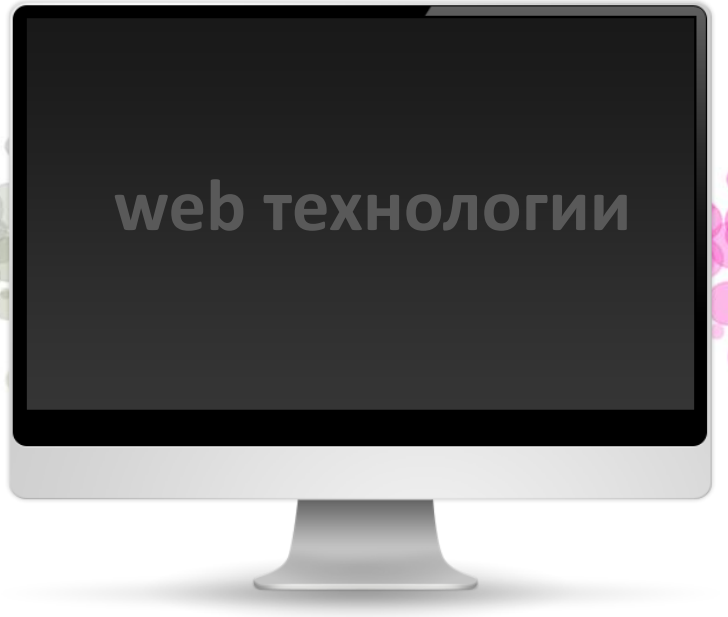
Брестский государственный
технический университет



IoT

ФАКУЛЬТЕТ
ЭЛЕКТРОННО-
ИНФОРМАЦИОННЫХ
СИСТЕМ

Весна 2022

План лекции

- IoT
- DeepNet
- DarkNet


amazon

Интернет для машин

Концепция интернета вещей базируется на принципе межмашинного общения: без вмешательства человека электронные устройства «общаются» между собой.

Интернет вещей – это автоматизация, но более высокого уровня.

Интернет для машин

Сама идея, что устройства могут обмениваться информацией друг с другом без участия человека, появилась еще в конце 70-х годов.

Однако потребовалось 20 лет, чтобы подключить первое устройство к сети и еще 9 лет, чтобы сформулировать само определение Интернета вещей.

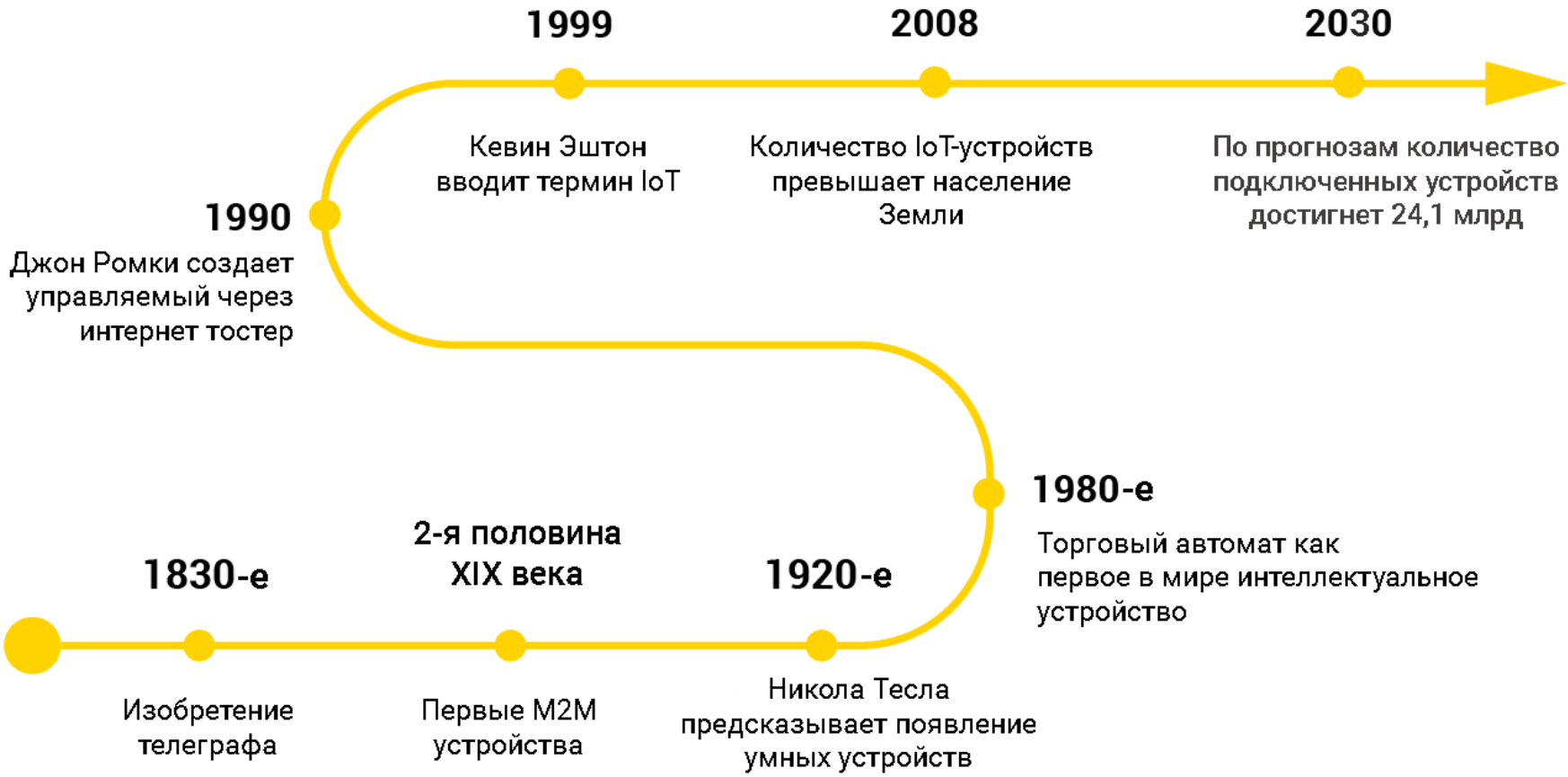
Интернет для машин

Термин «Интернет вещей» был впервые употреблен в 1999 году Кевином Эштоном, предпринимателем и соучредителем центра Auto-ID Labs (независимая сеть лабораторий и исследовательская группа в области сетевой радиочастотной идентификации и новых сенсорных технологий) при Массачусетском технологическом институте.

Интернет для машин

Эштон состоял в команде, которая сумела изобрести способ подключения объектов к интернету с при помощи технологии RFID.

RFID-метка — это метка идентификации, позволяющая идентифицировать объекты посредством радиосигналов; на нее можно нанести определенную информацию, а позднее считать устройством.


1830-е
Изобретение телеграфа
2-я половина XIX века
Первые M2M устройства
1920-е
Никола Тесла предсказывает появление умных устройств
1980-е
Торговый автомат как первое в мире интеллектуальное устройство
1990
Джон Ромки создает управляемый через интернет тостер
1999
Кевин Эштон вводит термин IoT
2008
Количество IoT-устройств превышает население Земли
2030
По прогнозам количество подключенных устройств достигнет 24,1 млрд

1990

На выставке Interop представлен тостер Sunbeam Deluxe, который можно было включить через интернет.

1993

Правительство США дает разрешение гражданам пользоваться GPS.

1996

G.M. запускает сервис OnStar.

1998

Учёный в области информатики Марк Вейзер создает фонтан, который работает, синхронизируясь с переменами на фондовом рынке.

1999

Кевин Эштон придумывает термин "Интернет вещей".

2000

LG создает первый холодильник, который можно подключить к интернету.

2007

Джеймс Парк и Эрик Фридман запускают FitBit.

2008

Количество подключенных устройств стало большем, чем людей.

2009

Google тестирует беспилотные технологии Toyota Prius; St. Jude Medical создает беспроводной кардиостимулятор, с помощью которого можно удаленно следить за пациентом.

2010

Тони Фаделл и Мэтт Роджерс становятся основателями Nest.

2014

Cisco, GE, AT&T, Intel и IBM формируют международный консорциум промышленного Интернета вещей и создают стандарты IoT.

2016

Alphabet выпускает Google Home; Apple выпускает HomeKit; G.M. инвестирует $500 миллионов в Lyft.

2013

Выход Google Glass; Intel формирует свое отделение IoT; Amazon анонсирует сервис доставки дронами.

2015

Mattel анонсирует Барби с подключением к интернету; Федеральное агенство воздушного транспорта одобряет производство опыляющих дронов; Moocall начинает продавать сенсоры, котрые сообщают фермерам о том, что их корова родила.

2017

Lyft и G.M. планирует провести испытания беспилотного такси.

2018

По оценке Cisco, к 2018 году количество подключенных мобильных устройств составляет 10 миллиардов, а к 2020 году это количество превысит 50 миллиардов.

2021

BMW, Ford и Volvo выпустят полноценные беспилотные авто.

Из чего состоит IoT? Архитектура

Для простоты попробуем разбить стек технологий IoT на четыре технологических уровня и рассмотреть их раздельно.

Конечные устройства

Устройства — это объекты, которые фактически образуют «вещи» (Things) в Интернете вещей. Они играют роль интерфейса между реальным и цифровым мирами и принимают разные размеры, формы и уровни технологической сложности в зависимости от задачи, которую они выполняют в рамках конкретного развертывания IoT.

Конечные устройства

Практически любой материальный объект можно превратить в подключенное устройство путем добавления необходимых элементов (датчиков или приводов вместе с соответствующим программным обеспечением).

Программное обеспечение

Это то, благодаря чему подключенные устройства можно назвать «умными». Программное обеспечение отвечает за связь с облаком, сбор данных, интеграцию устройств и за анализ данных в реальном времени.

Также оно предоставляет возможности для визуализации данных и взаимодействия с системой IoT.

Коммуникации

Уровень коммуникации включает в себя как решения для физического подключения (сотовая и спутниковая связь, LAN), так и специальные протоколы, используемые в различных средах IoT (ZigBee, Thread, Z-Wave, MQTT, LwM2M).

Платформа

Устройства способны «ощущать», что происходит вокруг и сообщать об этом пользователю через определенный канал связи.

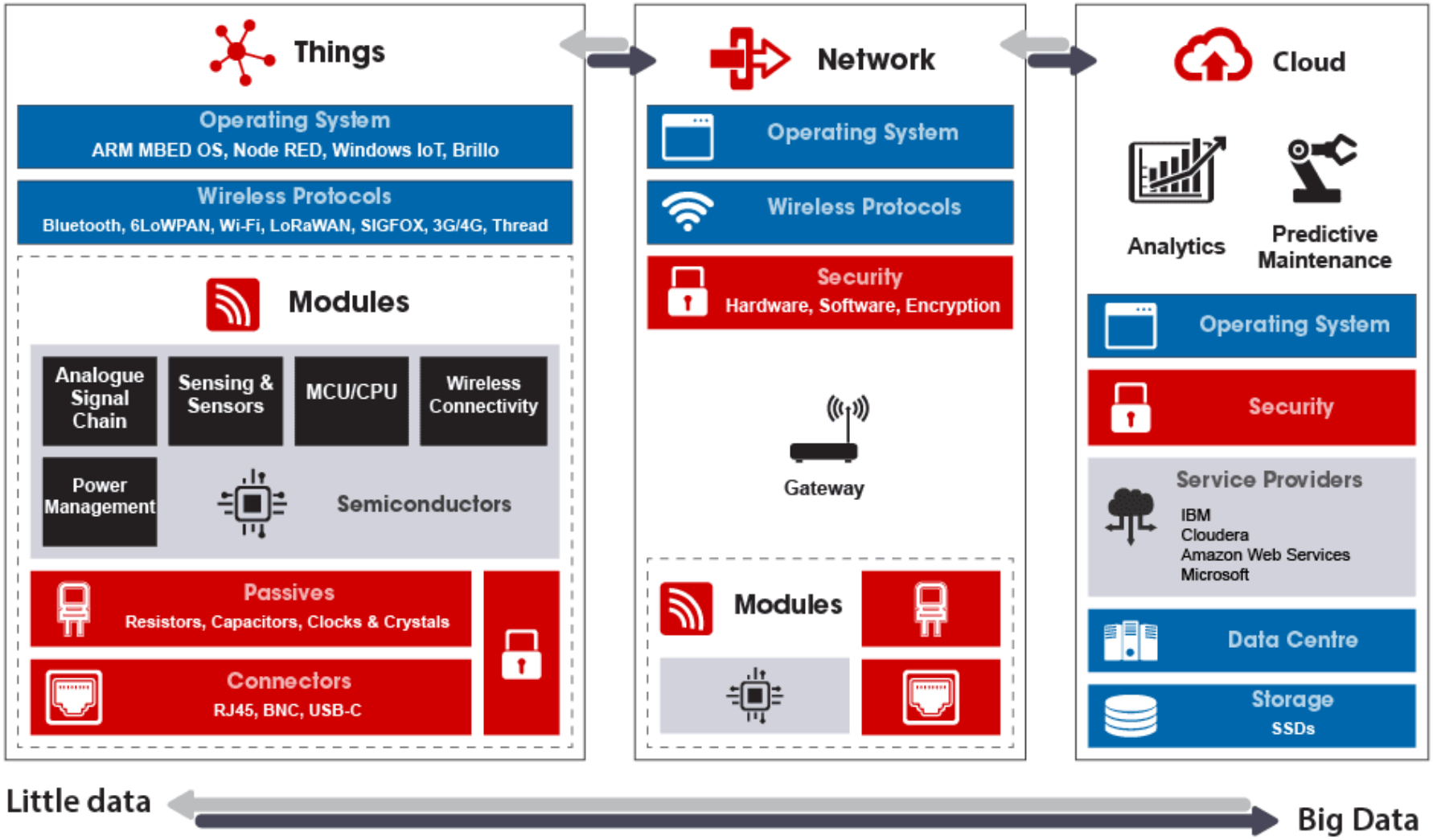
IoT-платформа — это место, где все эти данные собираются, анализируются и передаются пользователю в удобной форме.

Платформы могут быть установлены локально или в облаке.

Интернет для машин

В отличие от «умных» домов, узлы системы используют TCP/IP-протоколы для обмена данными через каналы глобальной сети интернет.

Рассматриваемый метод коммуникации дает преимущество – возможность объединять системы между собой, строить «сеть сетей», что позволяет изменить бизнес-модели отраслей и даже экономики целых стран.


Things
Operating System
ARM MBED OS, Node RED, Windows IoT, Brillo
Wireless Protocols
Bluetooth, 6LoWPAN, Wi-Fi, LoRaWAN, SIGFOX, 3G/4G, Thread
Modules
Analogue Signal Chain
Sensing & Sensors
MCU/CPU
Wireless Connectivity
Power Management
Semiconductors
Passives
Resistors, Capacitors, Clocks & Crystals
Connectors
RJ45, BNC, USB-C
Network
Operating System
Wireless Protocols
Security
Hardware, Software, Encryption
Gateway
Modules
Cloud
Analytics
Predictive Maintenance
Operating System
Security
Service Providers
IBM
Cloudera
Amazon Web Services
Microsoft
Data Centre
Storage
SSDs
Little data
Big Data

Интернет для машин

- устройства, которые вошли в сеть и взаимодействуют друг с другом;
- способ подключения – M2M – то есть машины – для – машин, без участия человека;
- работа с большим объемом данных. Применение технологий Big Data.

Технологии IoT

IoT (Industrial IoT, IIoT) объединяет концепцию межмашинного общения, использование BigData и проверенные технологии автоматизации производства.

Ключевая идея IIoT – в превосходстве «умной» машины над человеком, в точном, постоянном и безошибочном сбор информации.

Технологии IoT

Главное отличие Интернета вещей от обычных автоматизированных систем управления (АСУ ТП) в **количестве** обрабатываемых данных.

Сотни тысяч сигналов каждую секунду поступают на сервер и сразу же обрабатываются.

Благодаря этому пользователь в режиме **реального времени** видит работу оборудования.

Технологии IoT

Технологии, которые присутствуют в IoT, можно рассматривать в нескольких значимых аспектах:

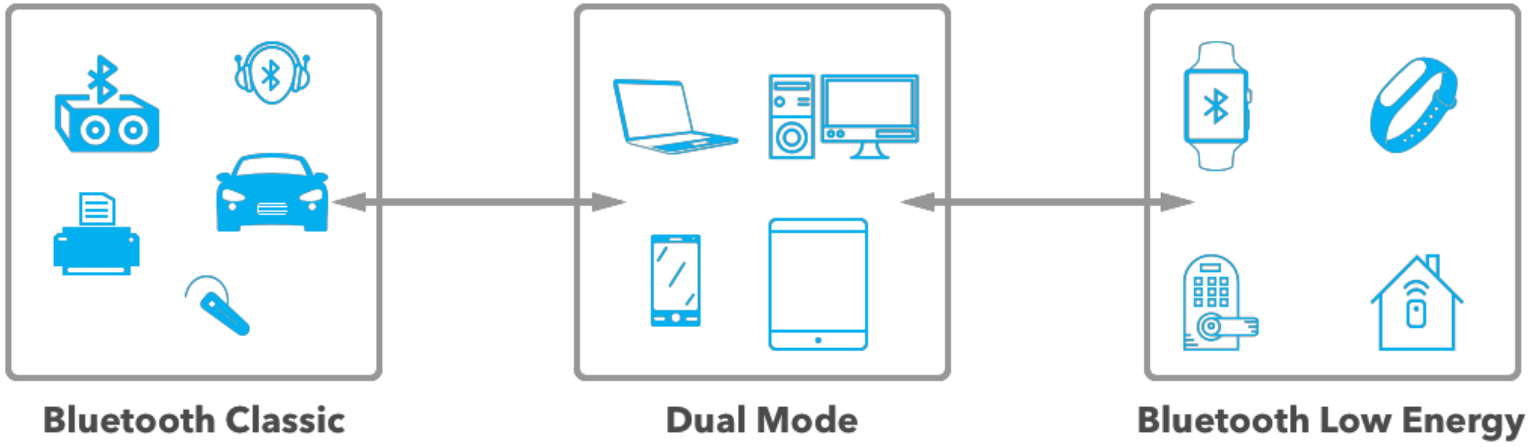
- RFID (радиочастотная идентификация), EPC (электронный код продукта);

Технологии IoT

- NFC («коммуникация ближнего поля»). Обеспечивает двусторонние взаимодействия между устройствами. Эта технология присутствует в смартфонах и служит для бесконтактных транзакций;

Технологии IoT

- Bluetooth. Широко применяется в ситуациях, когда достаточно связи ближнего радиуса действия. Чаще всего присутствует в носимых устройствах;



Технологии IoT

- Z-Wave. Низкочастотные RF-технологии. Чаще применяются для домашней автоматики, управления освещением и пр.;

Технологии IoT

- Wi-Fi. Самая популярная сеть для IoT (передача файлов, данных и сообщений).

Примеры IoT

«Яндекс-навигатор». Водители нередко пользуются этим сервисом. Смартфоны и планшеты передают координаты, направление движения и скорость в службу Яндекс, а принятая от пользователей информация анализируется на сервере компании. Получив сведения о заторе, приложение автоматически предлагает водителю варианты объезда и отображает маршрут на экране телефона или планшета.

Примеры IoT

Дистанционное снятие показаний со счетчиков водо- и энергоресурсов в домах возможно благодаря IoT-решениям – беспроводной автоматизированной диспетчеризации.

В ЖКХ нашли применение в системах интеллектуальной диспетчеризации – «умных» приборов учета ресурсов. Подключенные к интернету счетчики передают показания в «облако», а диспетчер видит расход в отдельном доме, квартале или городе.

Примеры IoT

Система для мониторинга влажности, температуры грунта и других характеристик почвы. Она работает как в частных, так и в государственных хозяйствах, где выращивают овощи и фрукты.

Датчик, «закрепленный» за отдельным растением или участком да данные поступают оператору, выводя на экран контрольного дисплея состояние саженца (группы растений) и рекомендации по улучшению их плодоносных свойств

Примеры IoT

Примеры IoT-устройств можно рассматривать в нескольких отдельных и связанных единой концепцией группах, таких как:

1) **носимые технологии.**

(фитнес-браслеты Fitbit и умные часы Apple Watch легко синхронизируются с другими мобильными устройствами).

Примеры IoT

2) **инфраструктура и разработка.**

(приложение CitySense в онлайн-режиме анализирует данные об освещении и автоматически включает или выключает фонари).

3) **здоровье.**

Некоторые системы, которые отслеживают состояние здоровья. Приложение UroSense отслеживает уровень жидкости в организме и, если нужно, повысит этот уровень.

Особенности LPWAN

С учетом перечисленных требований и ограничений решением проблемы видится использование технологии на стыке высокой дальности и низкого энергопотребления.

Она называется Low-Power Wide-Area Network (сокращенно – LPWAN), или энергоэффективная сеть дальнего радиуса действия.

Применение LPWAN

Уровень энерго-потребления

Высокое

Среднее

Низкое

Wi Fi

5G

2G/3G/4G

Bluetooth

zigbee

VSAT

RFID

WPAN

LoRa

GoodWAN

sigfox

«Низкая»
до 20 метров

«Средняя»
до 500 метров

«Высокая»
> 10 км

Дальность передачи

IOT ANALYTICS

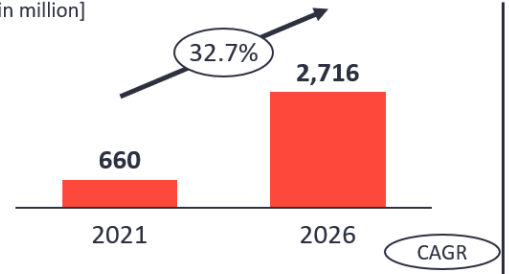
October 2021

Your Global IoT Market Research Partner

Market Snapshot: LPWAN Market 2021

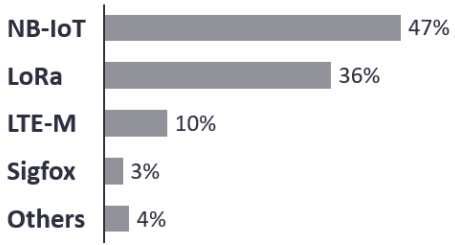
Market Size

Global installed base of LPWAN-enabled active devices [in million]



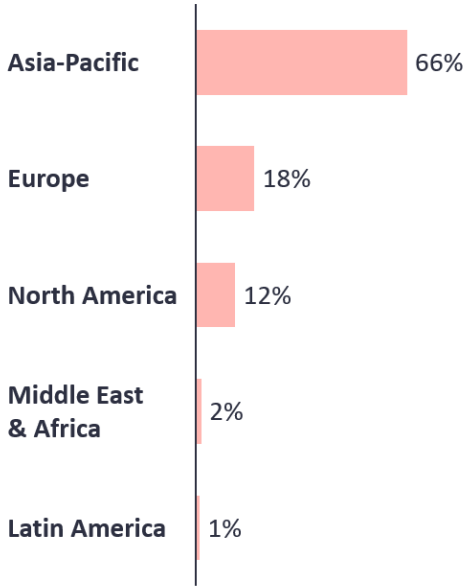
Technology Share

Technological distribution of the installed base in 2021



Regional Focus

Regional distribution of the installed base in 2021



Selection of Leading Firms in the Ecosystem

A selection of relevant LPWAN companies

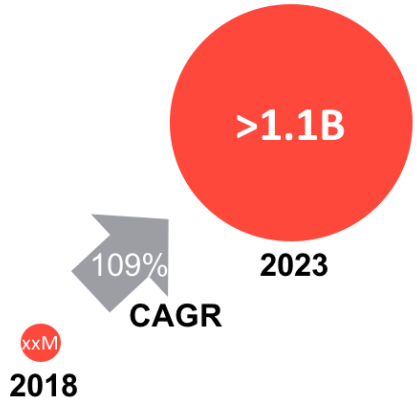
Source: IoT Analytics Research 2021; Conditions for republishing: Source citation with link to original post and company website; Non-commercial purposes only

LPWAN Market 2018 – 2023: New Report Out Now

LPWAN

LPWAN Market Development

Global LPWAN connections



Fastest growing IoT connectivity technology (2017-2023)

- Utilities the biggest segment
- Asia Pacific to become the leading adopter

7 Leading technologies

sigfox, LoRa, RPMA, WEIGHTLESS, NB-IoT, LTE-M, EC-GSM-IoT

Comparison criteria:

- Technical features
- Ecosystem
- Use case suitability
- SWOT Analysis

16 other relevant technologies

CYANCONNODE, DASH7, helium, hiber, JupiterMesh, MIOTY, NB-Fi, nwave, SAT4M2M, SilverSpring NETWORKS, СТРИЖ, Telensa, THINGSTREAM, Wi-Fi HaLow, WIREPAS, wi-SUN

Solutions in 9 market segments

- Agriculture & Forestry
- Building & Infrastructure
- Healthcare
- Home & Consumer
- Industrial
- Retail
- Smart Cities
- Transportation, Supply Chain & Logistics
- Utilities

37 LPWAN use cases analyzed in detail

Особенности LPWAN

Отсутствие относительно высоких требований к объему передаваемой информации позволило сконцентрироваться на важных параметрах технологии и обеспечить 50-километровую дистанцию взаимодействия между разнесенными устройствами, высокую энерго-эффективность, проникающую способность и масштабируемость.

Особенности LPWAN

«Дальнобойная» и энергоэффективная LPWAN отлично подходит для IoT как в бытовом, так и в промышленном секторе, где имеется потребность в автономной передаче телеметрии на дальние расстояния, потому что LPWAN гораздо лучше соответствует запросам M2M-сетей, чем ее слабый аналог (в теме передачи данных) сотовая связь – тысячи квадратных километров будут покрыты лишь одной базовой станцией. Построение такой сети проще, а обслуживание – дешевле.

Сравнение технологий IoT

Разработчики изначально не предполагали возможности обмена небольшими объемами данных между разнесенными «умными» сенсорами.

Датчику с Wi-Fi необходимо постоянное питание, а элемент умного GSM-устройства продержится 2–3 недели. Не многие пока готовы ежемесячно менять элементы питания в десятках устройств или монтировать к ним проводную систему питания.

Безопасность IoT

Данные лежат в основе работы всех подключенных устройств.

Потому не исключен несанкционированный доступ во время передачи данных.

Из за этого необходимо проверять, насколько защищены/зашифрованы данные.

Если у устройства есть UI, нужно проверить, защищен ли он паролем.

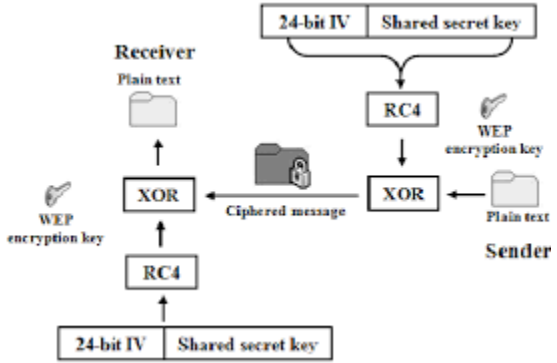
Безопасность IoT

WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное WEP-шифрование.

Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, более высокая стойкость сети к взлому.

Безопасность IoT

Часть WEP-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации), то есть меняющаяся в процессе работы сети.



Безопасность IoT WEP

Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа.

Для повышения уровня безопасности можно дополнительно к wep-шифрованию использовать стандарт 802.1x или VPN.

Безопасность IoT WPA

WPA – более стойкий протокол шифрования, чем WEP, хотя используется тот же алгоритм RC4.

Более высокий уровень безопасности достигается за счет использования протоколов TKIP и MIC.

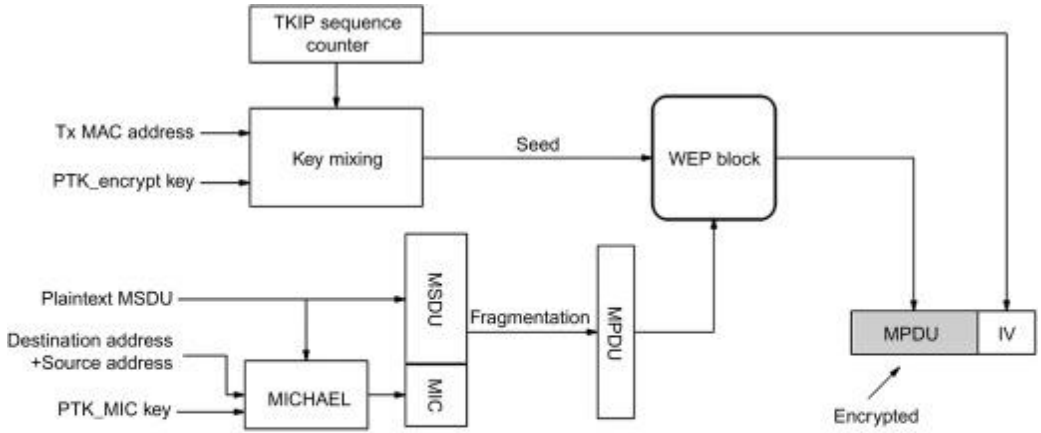
Безопасность IoT WPA

Существует два вида WPA:

- WPA-PSK (Pre-shared key). Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети.
- WPA-802.1x. Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

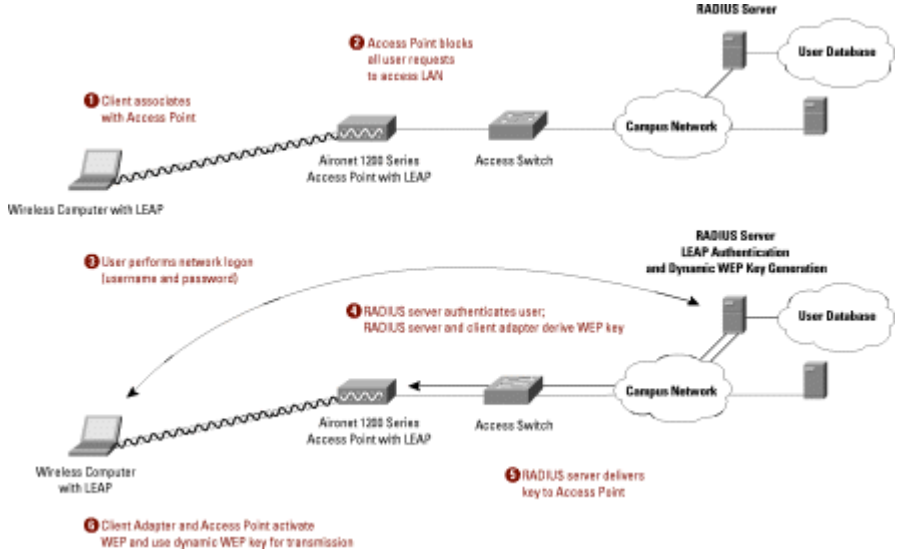
Безопасность IoT TKIP

TKIP (Temporal Key Integrity Protocol). Протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.



Безопасность IoT MIC

MIC (Message Integrity Check). Протокол проверки целостности пакетов. Защищает от перехвата пакетов и из перенаправления. Также возможно и использование 802.1x и VPN, как в случае с WEP-протоколом.



Безопасность IoT MIC

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);
- бесконтроллерные, но притом неавтономные (управляемые без контроллера).

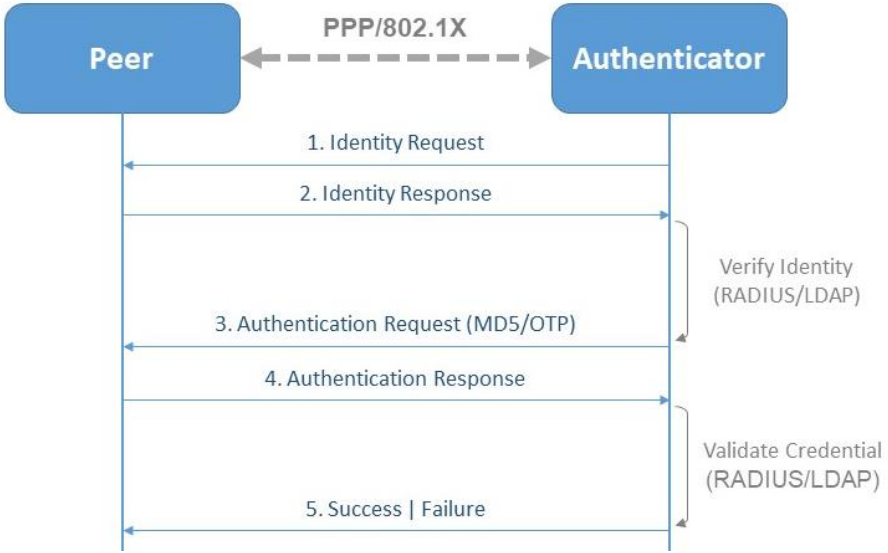
Безопасность IoT MIC

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

Протоколы разных стандартов безопасности сети

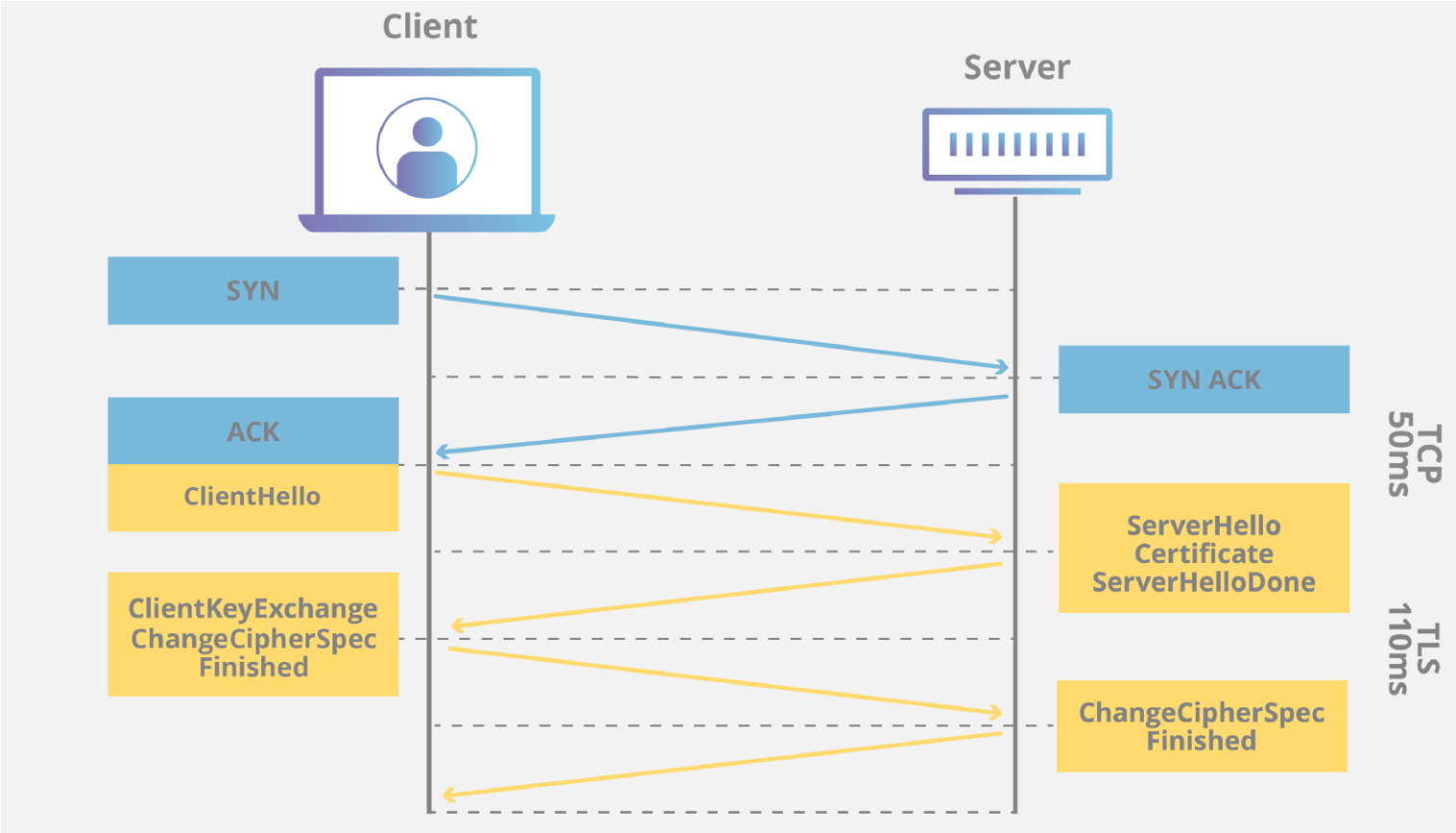
- EAP (Extensible Authentication Protocol). Протокол расширенной аутентификации. Используется совместно с RADIUS-сервером в крупных сетях.



Протоколы разных стандартов безопасности сети

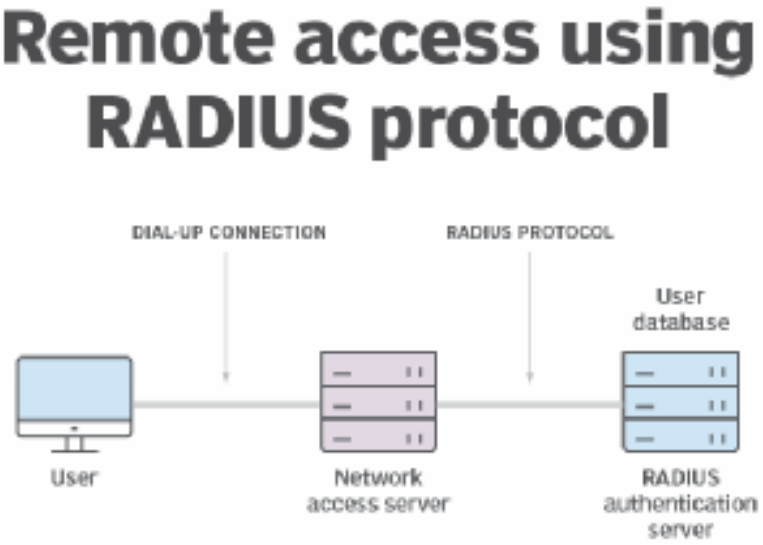
- TLS (Transport Layer Security). Протокол, который обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений.

Протокол TLS



Протоколы разных стандартов безопасности сети

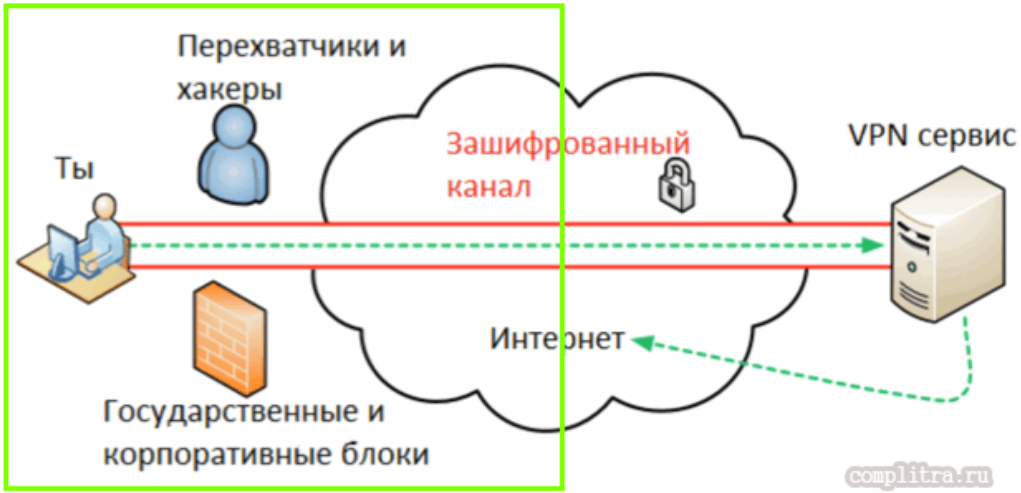
• RADIUS (Remote Authentication Dial-In User Server). Сервер аутентификации пользователей по логину и паролю.



Протоколы разных стандартов безопасности сети

• VPN (Virtual Private Network) – виртуальная частная сеть.

Протокол был создан для безопасного подключения клиентов к сети через общедоступные интернет-каналы.



Протоколы разных стандартов безопасности сети

Принцип работы VPN – создание так называемых безопасных «туннелей» от пользователя до узла доступа или сервера.

Хотя VPN изначально был создан не для Wi-Fi, его можно использовать в любом типе сетей. Для шифрования трафика в VPN чаще всего используется протокол IPSec. Он обеспечивает практически стопроцентную безопасность. Случаев взлома VPN на данный момент неизвестно.

Протоколы разных стандартов безопасности сети

Фильтрация по MAC-адресу – важное звено в обеспечении безопасности работы. MAC-адрес – уникальный идентификатор устройства (сетевого адаптера), «зашитый» в него производителем. На некотором оборудовании можно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – в принципе, MAC-адрес можно подменить.

Протоколы разных стандартов безопасности сети

Приватное скрытие SSID обеспечивает сети еще большую безопасность.

SSID – это идентификатор беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом, при сканировании всех доступных беспроводных сетей вашей сети видно не будет. Это не слишком серьезная преграда, если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в Windows.

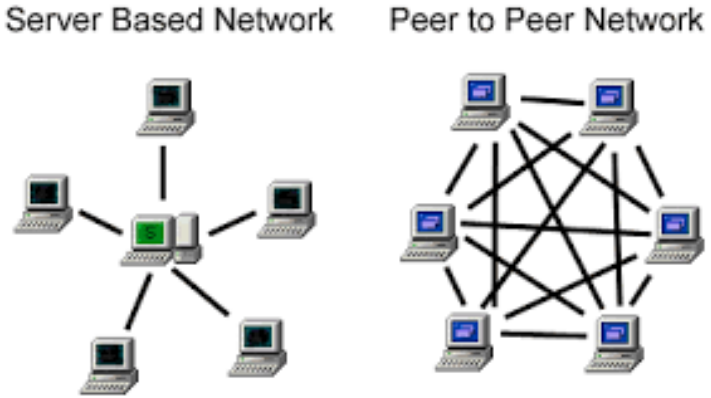
P2P

Аббревиатура P2P обозначает алгоритм «peer to peer», что в дословном переводе обозначает «равный к равному».

Пиринговый протокол отличается от привычной клиент-серверной архитектуры отсутствием выделенного сервера, так как каждый узел одновременно выполняет функции как клиента, так и сервера.

P2P

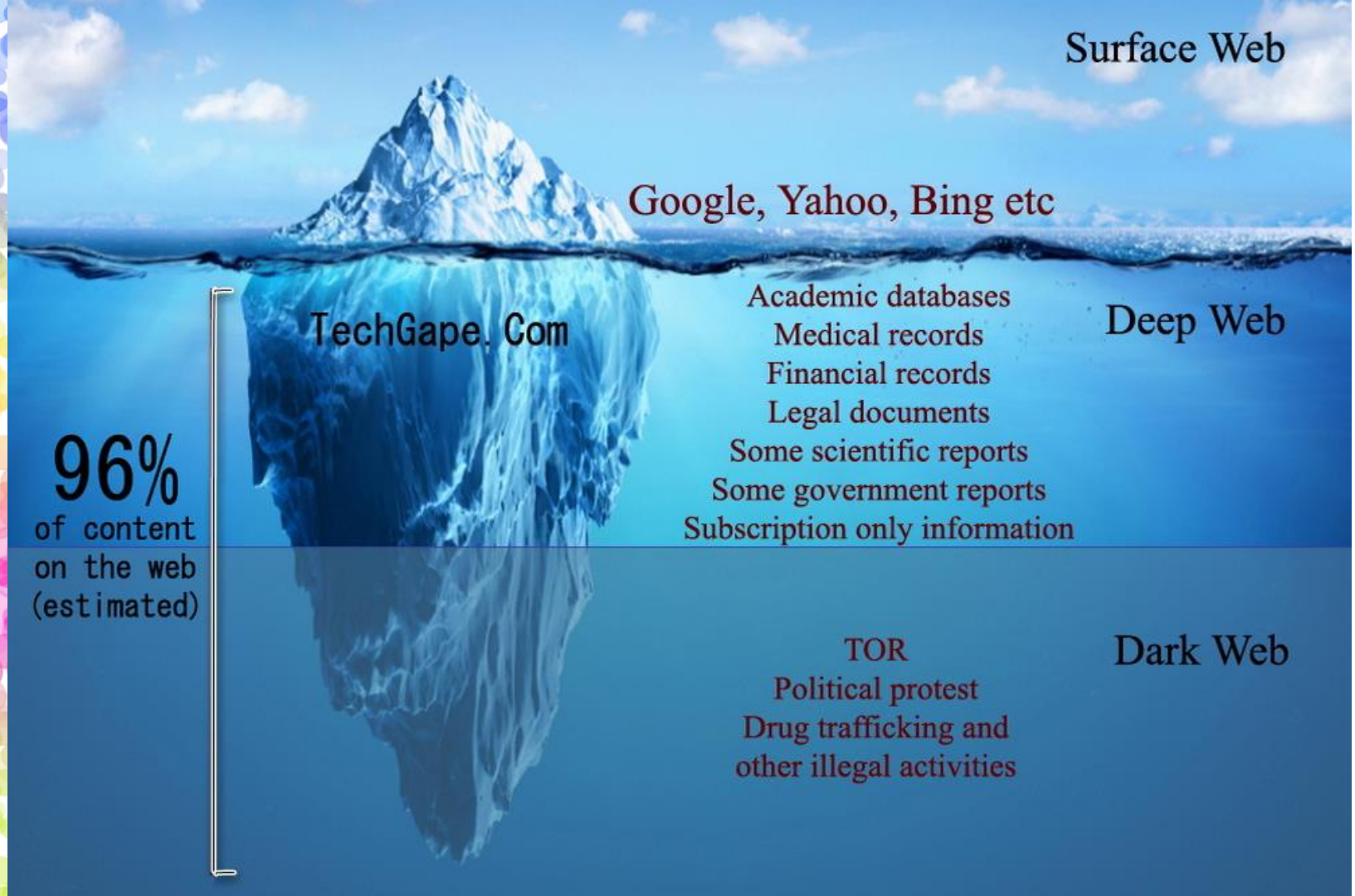
P2P-архитектура отличается повышенной отказоустойчивостью и более эффективным использованием полосы пропускания.

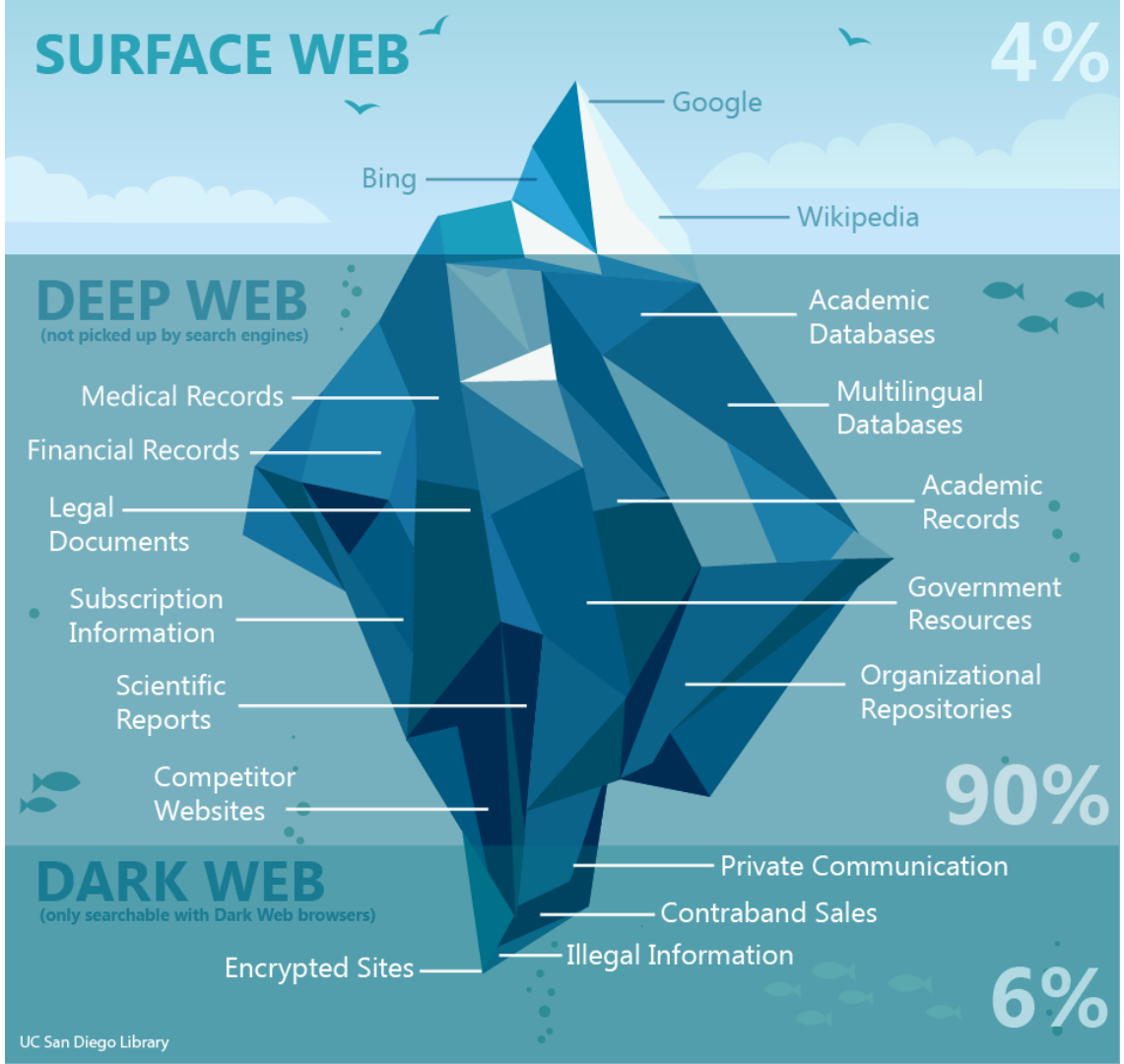


P2P

Камеры P2P начинают работать сразу после подключения к сети интернет, посредством обычного сетевого кабеля или по Wi-Fi.

Использование технологии P2P в системах видеонаблюдения позволило существенно упростить настройку оборудования и исключить применение статического IP как обязательного условия для работы всей системы.


Surface Web
Google, Yahoo, Bing etc
TechGape.Com
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Deep Web
96%
of content
on the web
(estimated)
TOR
Political protest
Drug trafficking and
other illegal activities
Dark Web


SURFACE WEB
4%
Google
Bing
Wikipedia
DEEP WEB
(not picked up by search engines)
Academic Databases
Medical Records
Multilingual Databases
Financial Records
Academic Records
Legal Documents
Government Resources
Subscription Information
Organizational Repositories
Scientific Reports
Competitor Websites
90%
DARK WEB
(only searchable with Dark Web browsers)
Private Communication
Contraband Sales
Illegal Information
Encrypted Sites
6%
UC San Diego Library

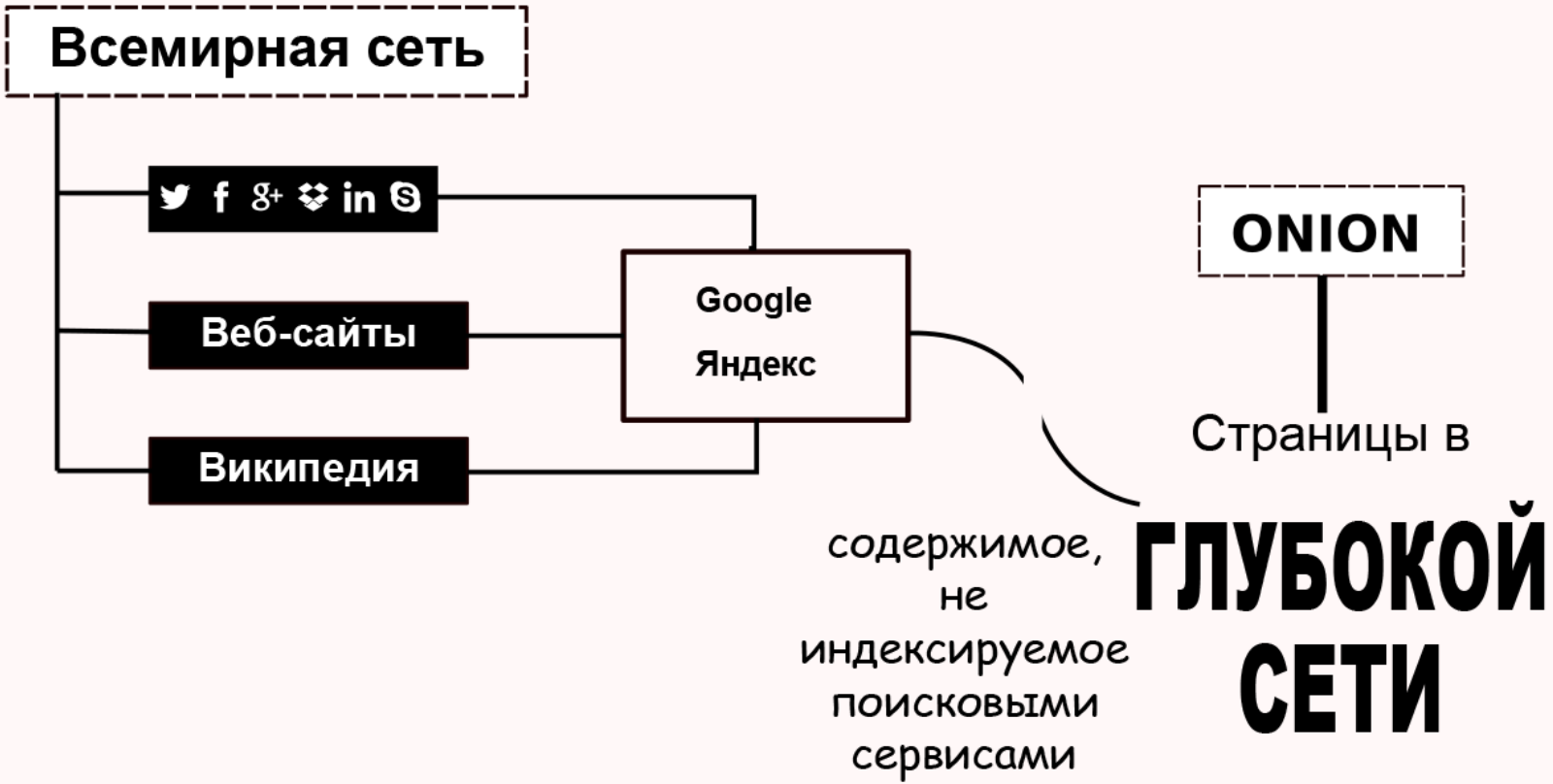
Deep Web

Хотя термины — Deep Web и Dark Web — часто заменяют друг друга, они отнюдь не равнозначны.

Наименование Deep Web относится вообще ко всем сайтам, которые не могут быть найдены посредством поисковых систем.

Deep Web

Термин произошёл от соотв. англ. invisible web. Наиболее значительной частью глубокой паутины является Глубинный веб (от англ. deep web, hidden web), состоящий из веб-страниц, динамически генерируемых по запросам к онлайн-базам данных.


Всемирная сеть
Веб-сайты
Википедия
Google
Яндекс
ONION
Страницы в
содержимое, не индексируемое поисковыми сервисами
ГЛУБОКОЙ СЕТИ

Deep Web

Таким образом, глубокая паутина включает в себя не только Dark Web, но и все пользовательские базы данных, почтовые страницы, заброшенные сайты и личные страницы, сетевые форумы с обязательной регистрацией и платный сетевой контент.

Таких страниц огромное множество.

Deep Web

Система управления контентом, тоже располагается в «глубокой паутине».

Она является скрытым дублем для каждой страницы общедоступного сайта.

Одновременно с этим, рабочие корпоративные сети также закрытые от поисковых систем и защищённые паролем, за время эксплуатации часто обрастают потайными дубликатами.

Deep Web

Если вы пользуетесь онлайн-доступом к своему банковскому счету, то ваши «защищённые паролем» данные — где-то глубоко в тенетах Deep Web.

А если прикинуть, сколько страниц генерирует одна только учетная запись на Gmail — тогда станет хотя бы приблизительно ясен истинный размер «глубокой паутины».

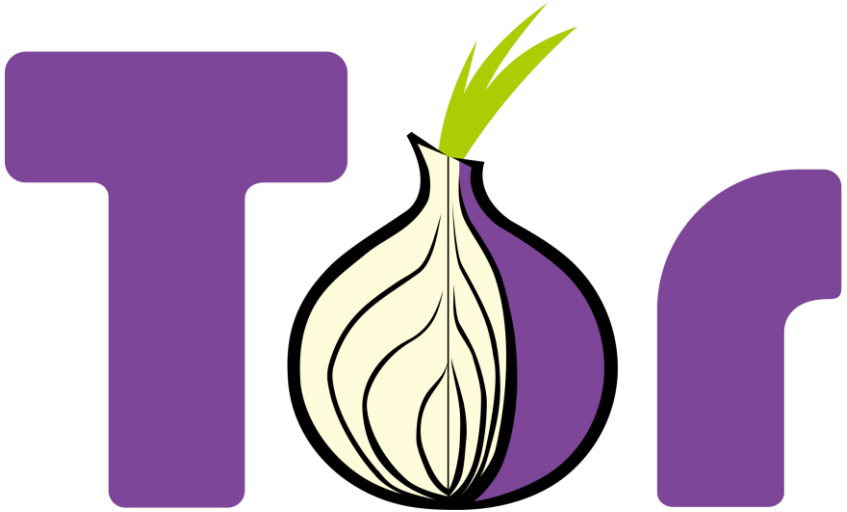
Deep Web

Вообще к DeepWeb может быть отнесён любой ресурс, доступный только по инвайтам, как, например, популярный в рунете коллективный блог Лепрозорий, или пиратский онлайн-кинотеатр Турбофильм. Таким же образом работают множество торрент-трекеров.

Изначально почта Google была доступна только по инвайтам.

Deep Web

Также это может быть ресурс, доступный только через какую-нибудь оверлейную сеть (работающую поверх Интернета), например, скрытые сервисы Tor или ипсайты I2P.



Когда иа как появился даркнет?

Изначально термином «даркнет» обозначались компьютеры в сети ARPANET, созданной в 1969 году Агентством по перспективным исследованиям (DARPA) Министерства обороны США.

Компьютерные сети – «даркнеты» – были запрограммированы получать сообщения от ARPANET, но их адреса отсутствовали в списках сетей и не отвечали на внешние запросы, оставаясь таким образом «темными» (dark).

Когда иа как появился даркнет?

Термин «даркнет» получил известность благодаря публикации в 2002 году научного доклада «Даркнет и будущее распространения информации».

Его авторами были сотрудники корпорации Microsoft Брайан Уиллман, Маркус Пейнаду, Пол Ингленд и Питер Биддл.

Когда иа как появился даркнет?

Они утверждали, что присутствие даркнета служит главным препятствием на пути развития технологий управления правами на электронные продукты (DRM) и неизбежно приведет к нарушению авторских прав.

В докладе даркнет описывался в широком смысле как любая сеть, требующая для получения доступа специфического протокола и существующая «параллельно» верхней или видимой сети.

DarkNet

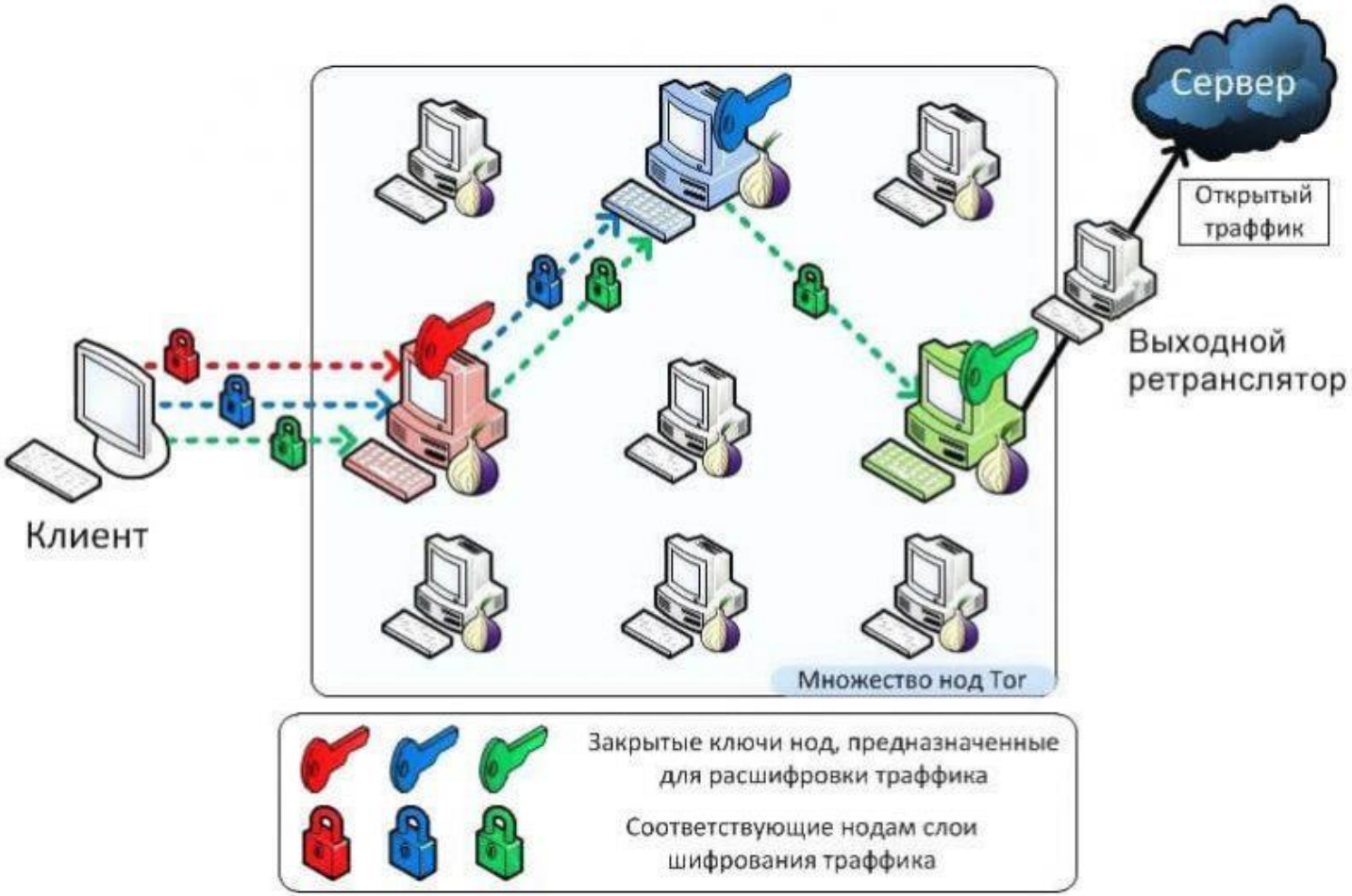
Чтобы посетить сайт из числа относящихся к Dark Web, используя Tor-шифрование, интернет-пользователю придется самому использовать Tor.

Перечень сетей причисленных к DarkNet довольно широк: The Onion Router (TOR), Invisible Internet Project (I2P), Telegram Open Network, Freenet, Zeronet, anoNet, а также mesh-сети Yggdrasill, cjDNS, Briar, Signal Offline и FireChat.

DarkNet

Под предлогом того, что в сети Tor работают многочисленные площадки торговли наркотиками, оружием, порнографией и т. п., с ней борются правоохранительные органы разных государств.

В 2014 году ФБР заплатило $1 млн исследователям из Университета Карнеги-Меллон в США за помощь в деанонимизации пользователей Tor.


Сервер
Открытый траффик
Выходной ретранслятор
Клиент
Множество нод Tor
Закрытые ключи нод, предназначенные для расшифровки траффика
Соответствующие нодам слои шифрования траффика

DarkNet

Точно как IP-адрес конечного пользователя мячиком прыгает через несколько слоев шифрования, чтобы добраться до другого IP-адреса в сети Tor, так же дело обстоит с интернет-сайтами. Каждому из узлов известны только те узлы, которые соединены с ним напрямую (о путях подключения вашего ПК к веб-серверу ему ничего не известно).

Любой переход от одного узла к другому осуществляется с использованием своего собственного набора ключей шифрования.

Как возник Tor?

Разработка Tor началась в 1995 году по заказу правительства США в «Центре высокопроизводительных вычислительных систем» Исследовательской лаборатории Военно-морских сил (NRL) в рамках проекта Free Haven совместно с Управлением перспективных научных исследований и разработок Министерства обороны США (DARPA).

Исходный код распространялся как свободное ПО.

Как возник Tor?

В начале 2000-х годов проект получил название The Onion Routing (Tor).

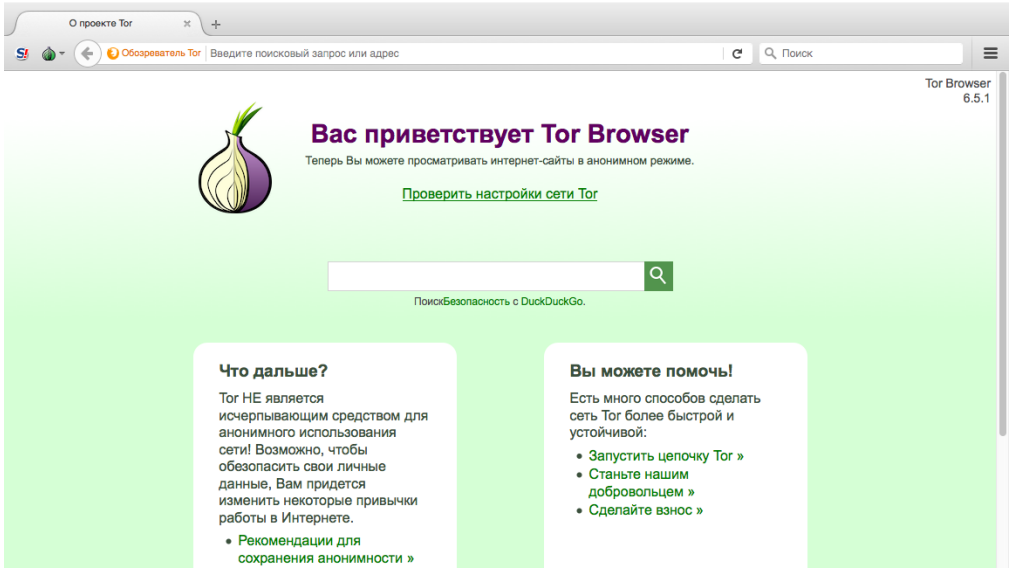
В октябре 2002 года была развернута сеть маршрутизаторов, которая к концу 2003 года включала более десяти сетевых узлов в США и один в Германии.

С 2004 года финансовую и информационную поддержку проекту оказывает правозащитная организация Electronic Frontier Foundation.

Как возник Tor?

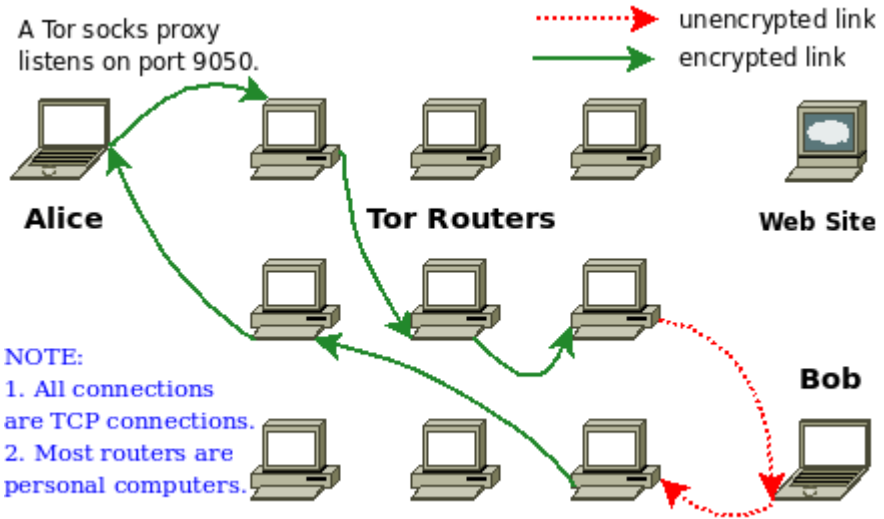
В 2006 году для развития сети Tor в США была создана некоммерческая организация Tor Project.

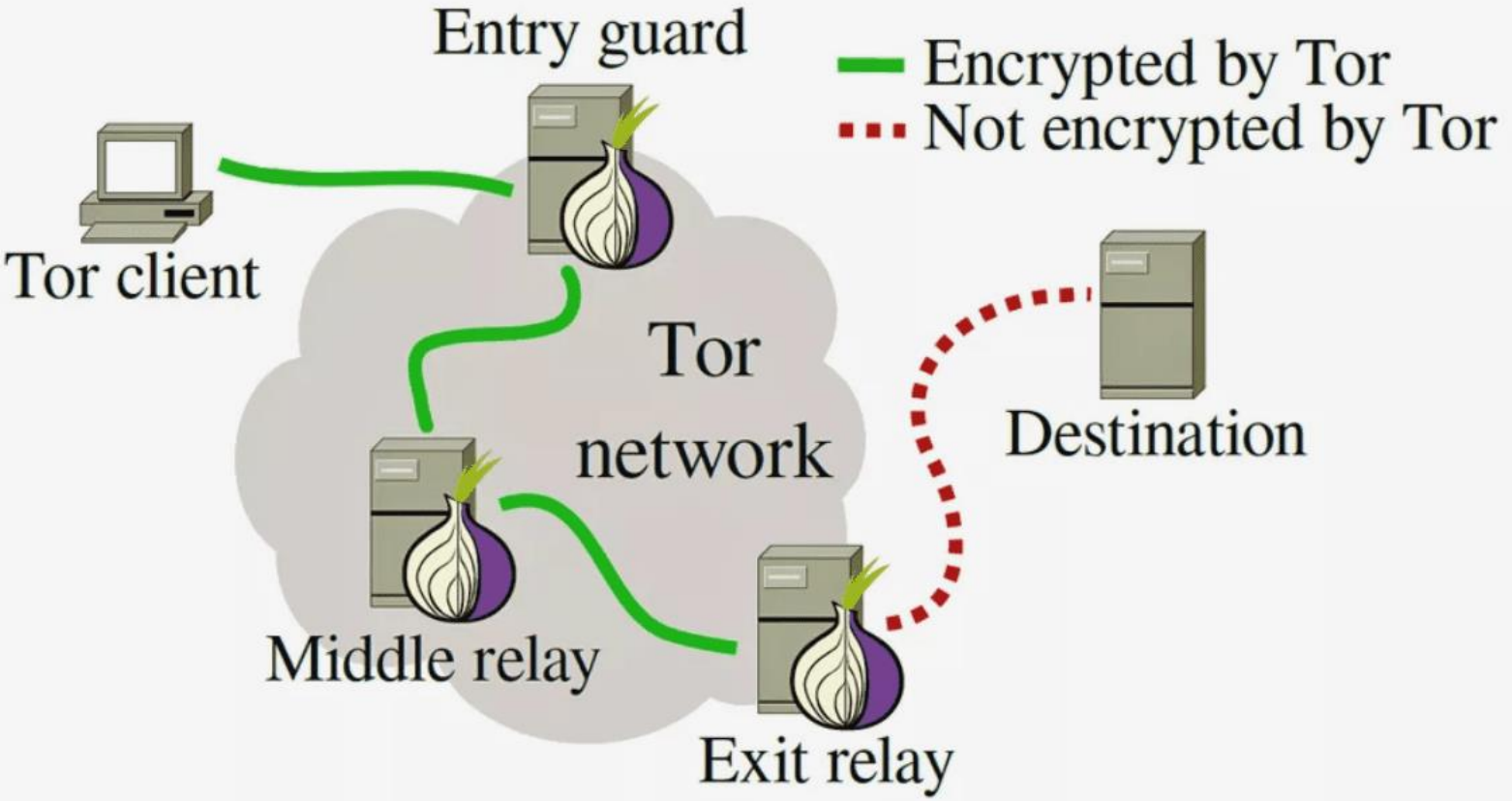
В 2008 году появился браузер Tor.



Dark Web

Такая структура снижает производительность и скорость, но существенно повышает безопасность ваших анонимных перемещений.

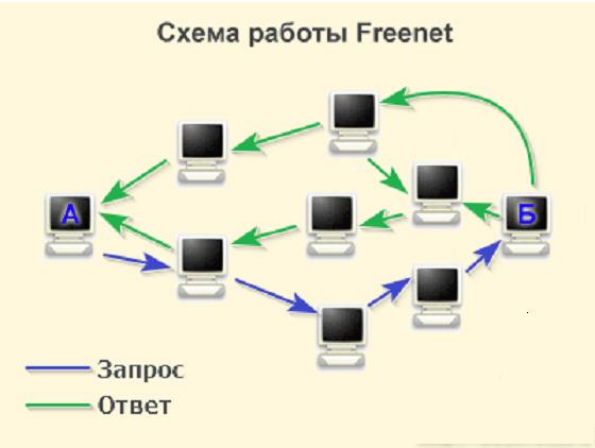



Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit relay

Freenet

Freenet – одноранговая сеть, предназначенная для децентрализованного распределенного хранения данных.

В отличие от Tor и I2P, Freenet обеспечивает анонимность только внутри собственной сети.



Freenet

В Freenet нет серверов, все данные в зашифрованном виде хранятся в компьютерах пользователей, которые объединены в общий фонд (пулинг).

Пользователи предоставляют полосу пропускания и дисковое пространство своих компьютеров для публикации или получения информации.

Freenet

Для определения местонахождения данных Freenet использует маршрутизацию по ключам, похожую на распределенную хеш-таблицу.

Пользователи могут выбирать степень защиты: чем она ниже, тем быстрее соединение, но защита данных в таком случае страдает.

Freenet

Даже при низкой степени защиты скорость соединения остается невысокой: загрузка изображения требует нескольких минут, просмотр видео невозможен, поскольку Freenet не поддерживает базы данных и скрипты, необходимые для отображения динамического контента.

Freenet делится на две части: **Opennet и Darknet**.

Opennet – общедоступный сегмент сети.

Попасть в **Darknet** можно только по приглашению другого пользователя.

I2P

I2P (Invisible Internet Project) – оверлейная анонимная сеть, состоящая из узлов двух типов:

•Маршрутизаторы. Имеют внутрисетевые и обычные IP-адреса. Доступны в обычном интернете и отвечают за работу I2P сети.

•Скрытые узлы. Не имеют IP-адресов.

I2P

I2P разграничивает маршрутизаторы и адресатов, скрывая данные о том, где находится адресат и к какому маршрутизатору подключен.

Каждый пользователь имеет несколько адресов: для соединения с сайтами, для торрентов и т. д., что усложняет отслеживание и идентификацию.

I2P

В основе I2P лежит модель туннелей – путей через несколько маршрутизаторов.

Как и в сети Tor, используется многослойное шифрование: один маршрутизатор расшифровывает один слой.

В отличие от Tor, обратный трафик передается по отдельному туннелю.

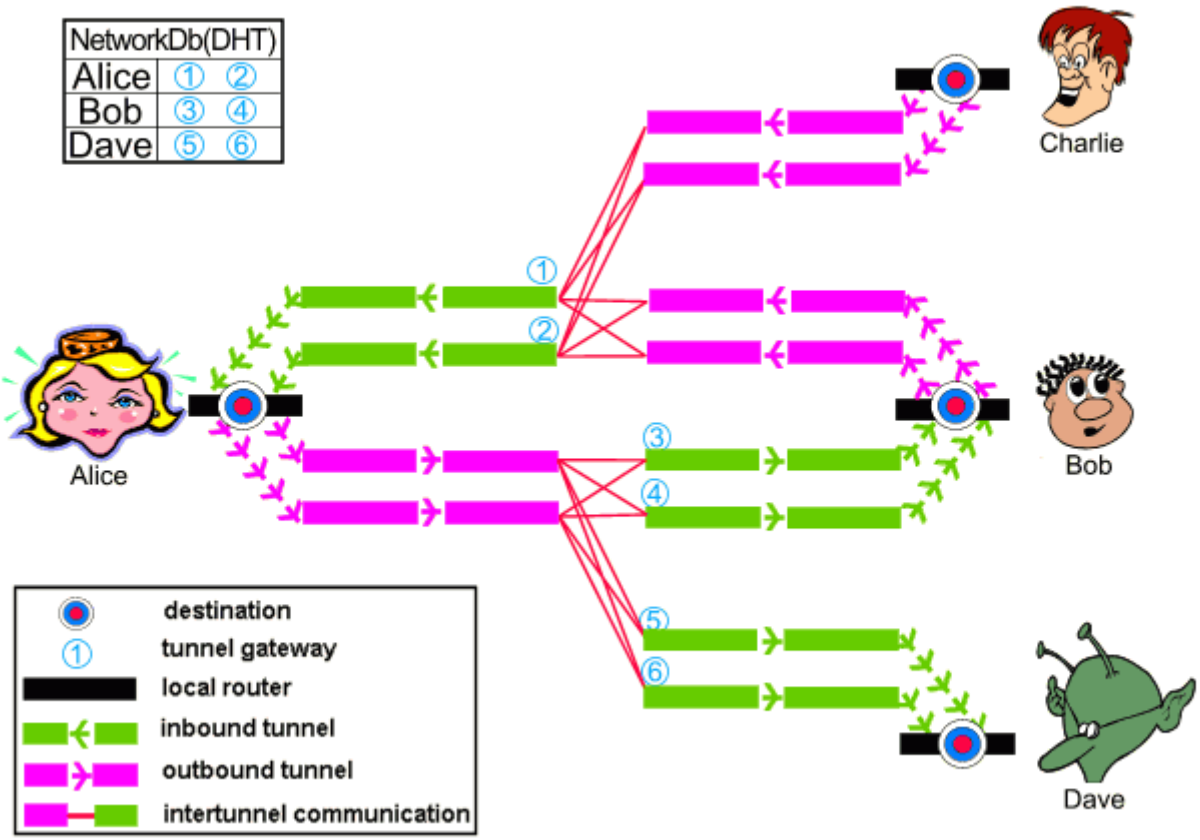
I2P

Длину туннелей пользователь может устанавливать самостоятельно.

Чем длиннее туннель, тем меньше шансы на обнаружение, но и скорость соединения соответственно ниже.

Электронные подписи и сильная криптография делают I2P самой защищенной сетью даркнета на настоящий момент.

I2P


NetworkDb(DHT)
Alice ① ②
Bob ③ ④
Dave ⑤ ⑥
Charlie
Alice
Bob
Dave
①
②
③
④
⑤
⑥
destination
tunnel gateway
local router
inbound tunnel
outbound tunnel
intertunnel communication

Dark or Deep?

Основное практическое отличие состоит в том, что словосочетания Dark Web или Deep Web обычно используются представителями массмедиа для обозначения уголков сети, полных опасностей и чьих-то потаенных замыслов, в то время как «темный интернет» — всего лишь скучные склады, где ученые хранят необработанные данные для своих дальнейших исследований.

NARUS®