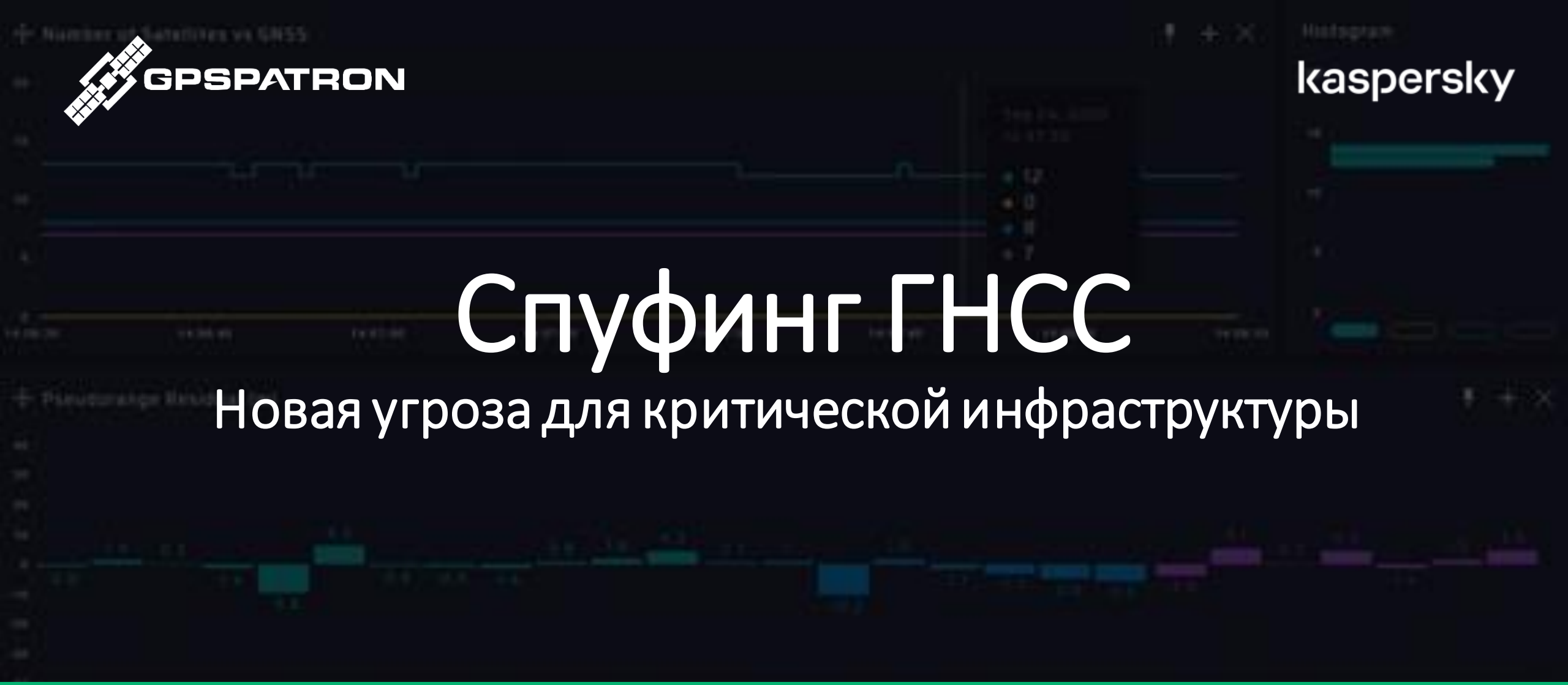


GPSPATRON

kaspersky

# Спуфинг ГНСС

## Новая угроза для критической инфраструктуры


Бородько Максим

CEO @ GPSPATRON

# Применение ГНСС в критической инфраструктуре

## Координаты

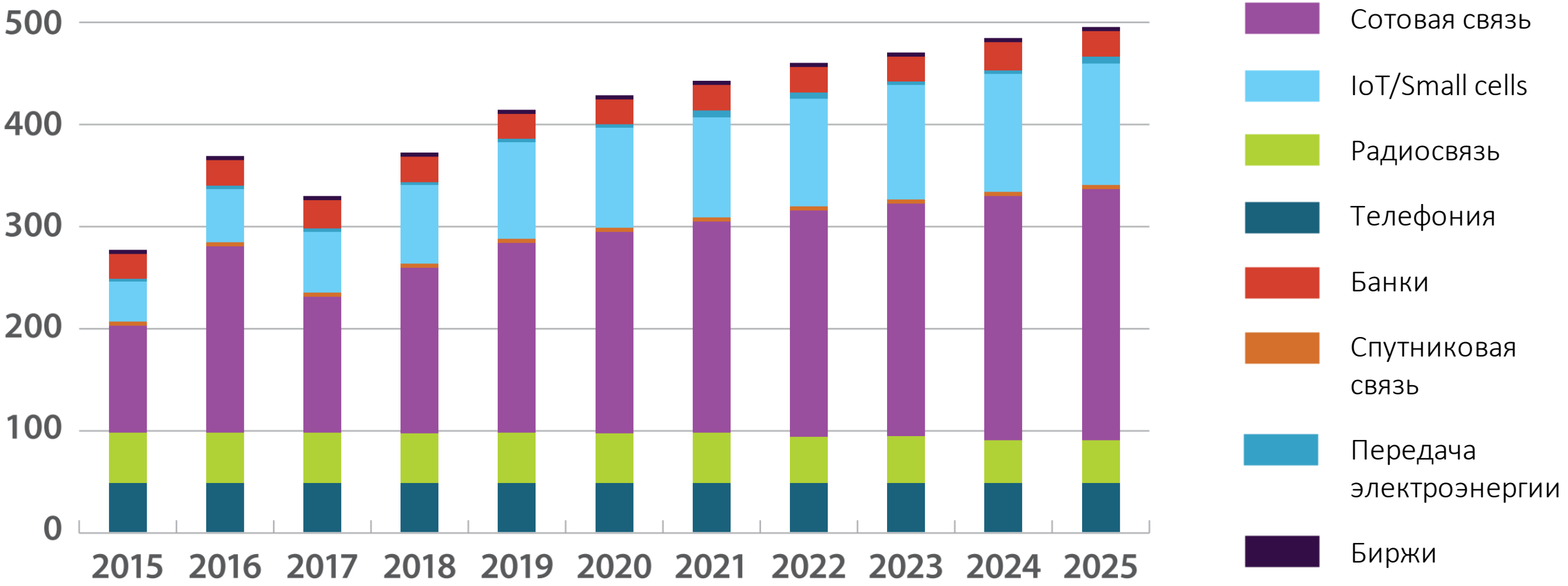
- Авиация
  - система инструментальной посадки GBAS landing system
  - управление воздушным движением ADS-B
- Морской транспорт
  - система автоматической идентификации AIS
- Железнодорожный транспорт
  - системы автоведения
- Наземный транспорт
  - Платон
  - ЭРА-ГЛОНАСС
  - Системы контроля транспортировки опасных грузов
  - Self Driving Cars

## Время

- Банки, Биржи (HFT)
  - все транзакции должны быть маркированы меткой времени в соответствии MIFID II и SEC 613
- Сотовая связь
  - 5G требует беспрецедентно высокой точности времени 60 нс.
- Цифровое телевиденье
  - передатчики DVB-T требуют высокую точность синхронизации
- Системы передачи электроэнергии
  - для балансировки системы необходимы точные измерения фазы и частоты
  - умные подстанции
- ЦОД
- Операторы газо-нефте проводов
- Автоматические системы управления

# Анализ рынка систем синхронизации времени

Количество ежегодно продаваемых серверов времени по отраслям в тысячах единиц




## 2,9M серверов времени к концу 2021

Данные из отчета Европейского Космического Агенства “Time & Synchronisation User Needs and Requirements”

# Угрозы ГНСС


## Джаминг

- генерация шума для блокирования сигналов
- относительно безопасен для серверов времени
- просто детектировать

## Спуфинг

- генерация фейковых сигналов ГНСС
- сервер времени через 15с сдвигает
- множество разных сценариев атаки

# Почему сейчас?

| $319.95 | $198.50 | $346.29 | $480 |
| --- | --- | --- | --- |
|  |  |  |  |
| HackRF One Software Defined Radio (SDR) & ANT500 Antenna Bundle<br>★★★★½ 29<br>$319.95 | ANALOG DEVICES ADALM-Pluto SDR Software Defined Radio Active Learning Module PlutoSDR<br>★★★½☆ 9<br>$198.50 | LimeSDR Flexible, Next-generation, Open Source Software Defined Radio USB 3.0 100 kHz - 3.8 GHz<br>★★★★½ 523<br>$346.29 | bladeRF 2.0 micro xA4, 47MHz to 6GHz frequency range, 61.44MHz sampling rate, 2×2 MIMO channels USB 3.0 SuperSpeed Software Defined Radio.<br>★★★★☆ 17<br>$480 |

# ГНСС спуфинг в антидрон системах

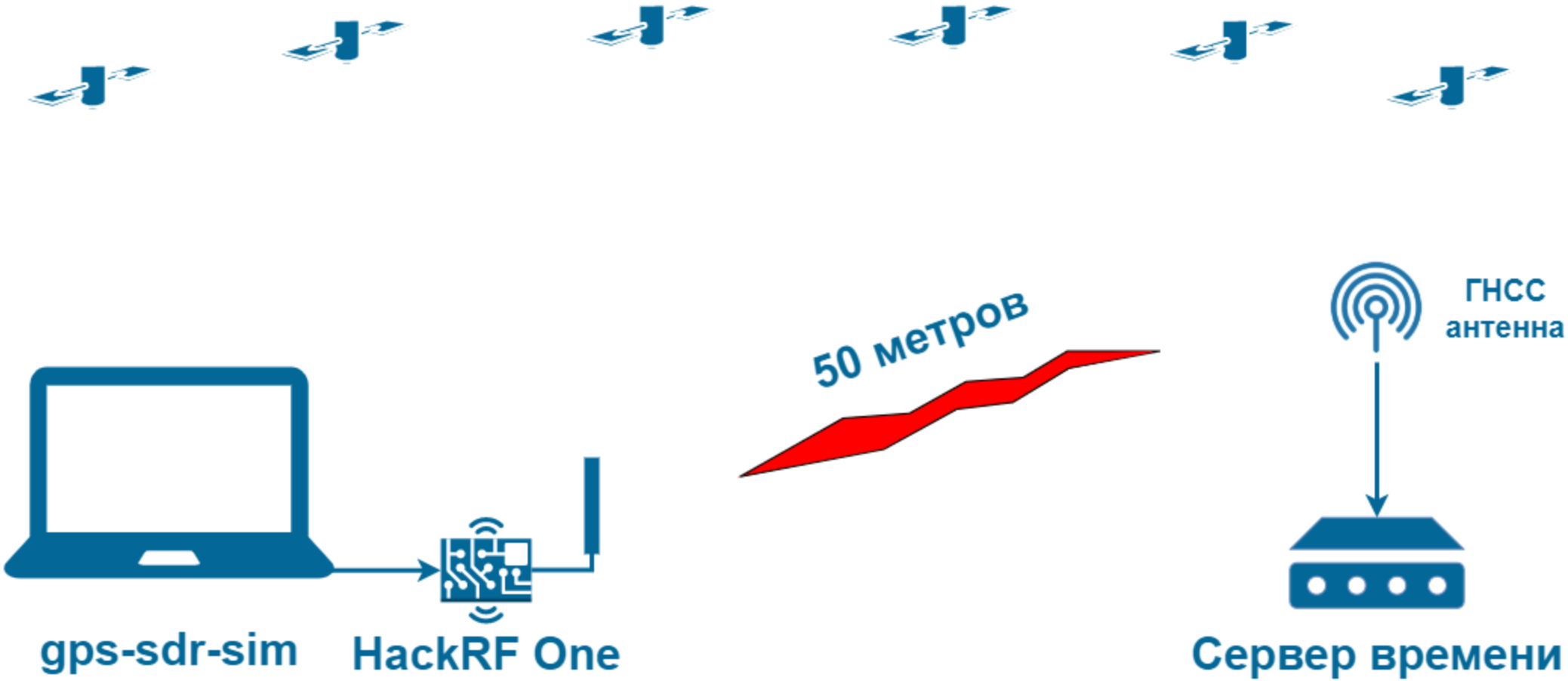
3/5 Vozdvizhenka Street

4-10 Ipatyevskiy Lane

34 Sofiyskaya Embankment

Иллюстрация из отчета C4ADS “Above us only stars. Exposing GPS spoofing in Russia and Syria”

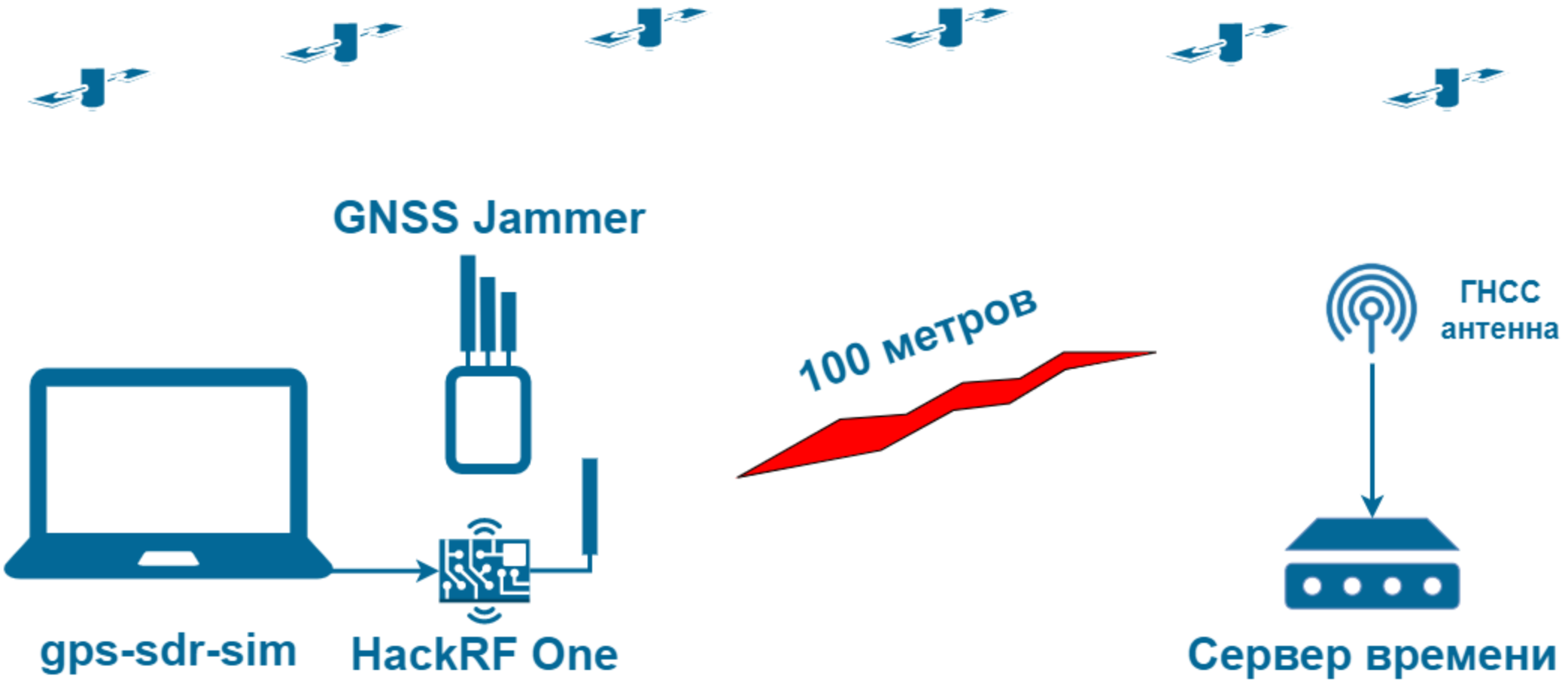
# Сценарии атак. GPS спуфинг с HackRF One




Стоимость атаки – 320 USD
Время атаки – от 15 секунд до 5 минут

Защита – использовать мульти-ГНСС приемники
Детектировать на уровне системы легко

# Сценарии атак. ГНСС спуфинг с HackRF One и джамером




Стоимость атаки – 320 + 150 USD
Время атаки – от 15 секунд до 5 минут

Защиты на уровне тайм сервера нет
Детектировать на уровне системы легко

# HackRF One + Android Phone + GNSS Jammer = Multi-GNSS Spoofer

# Усилитель + направленная антенна


RF Microwave Power
r 10W

**US $291.19**

US $3.32 Вам купон

Quantity:

1 999 piec

**Free Shipping**
to Belarus via AliExpr
Estimated Delivery o

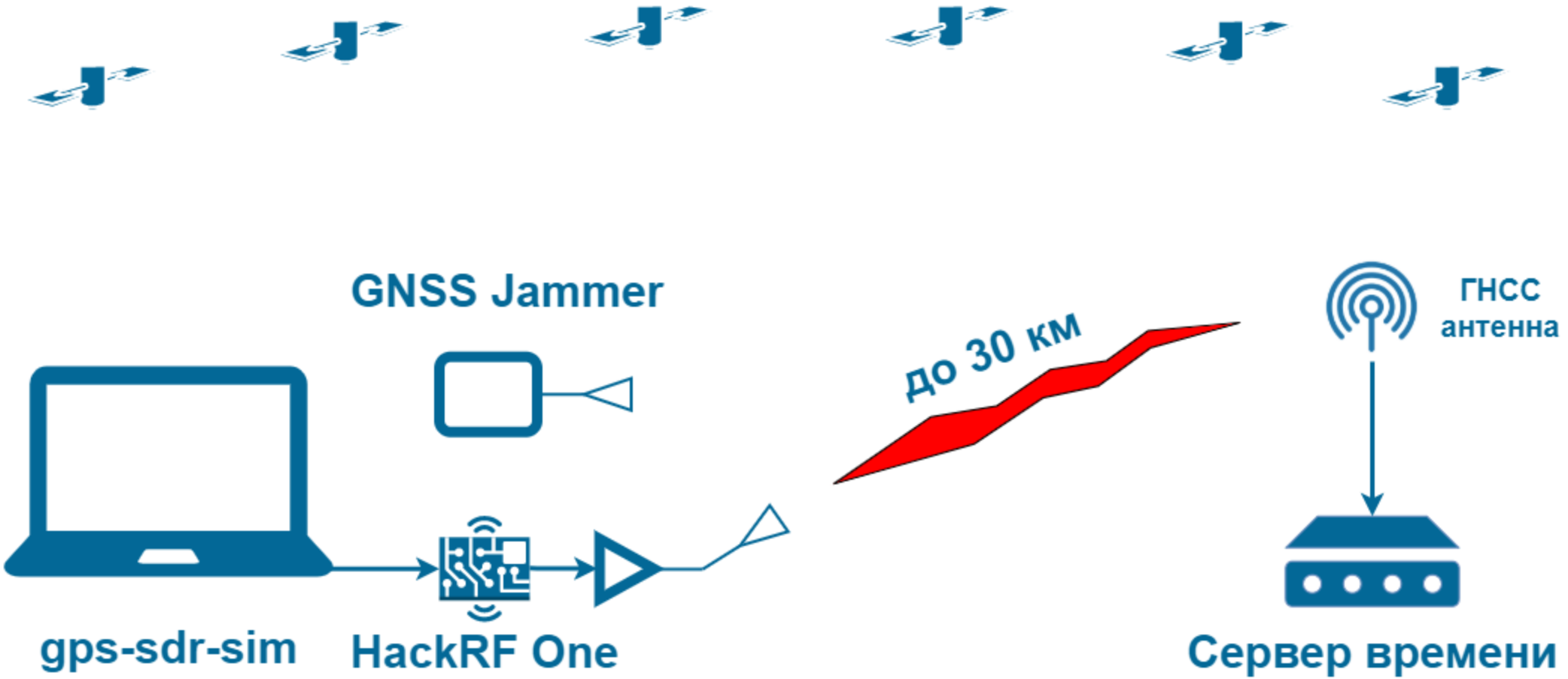
Buy Now

**75-Day Buyer Prc**
Money back guara


Выходная мощность 10 Вт

Коэффициент усиления 4 дБ

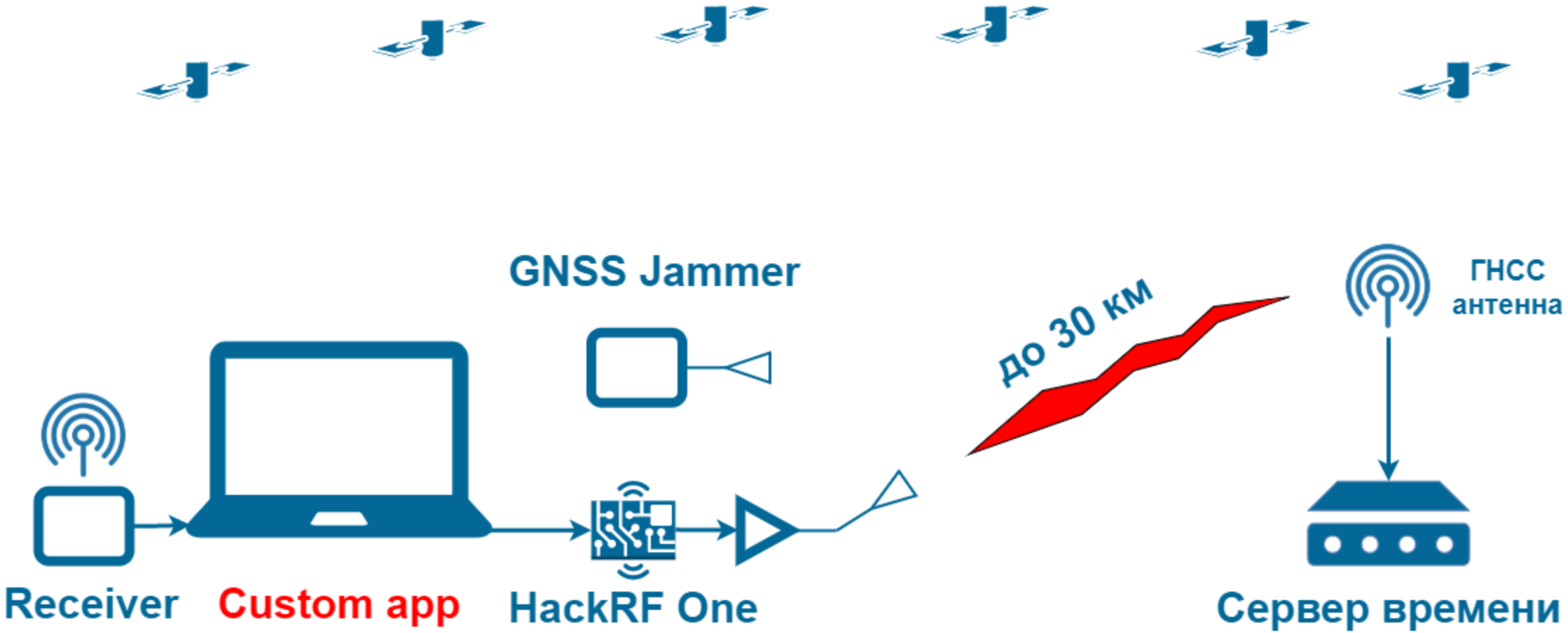
# Сценарии атак. ГНСС спуфинг с HackRF One, джамером и усилителем




Стоимость атаки – 1k USD
Время атаки – от 15 секунд до 5 минут

Детектировать на уровне системы невозможно, если будут покрыты все сервера времени

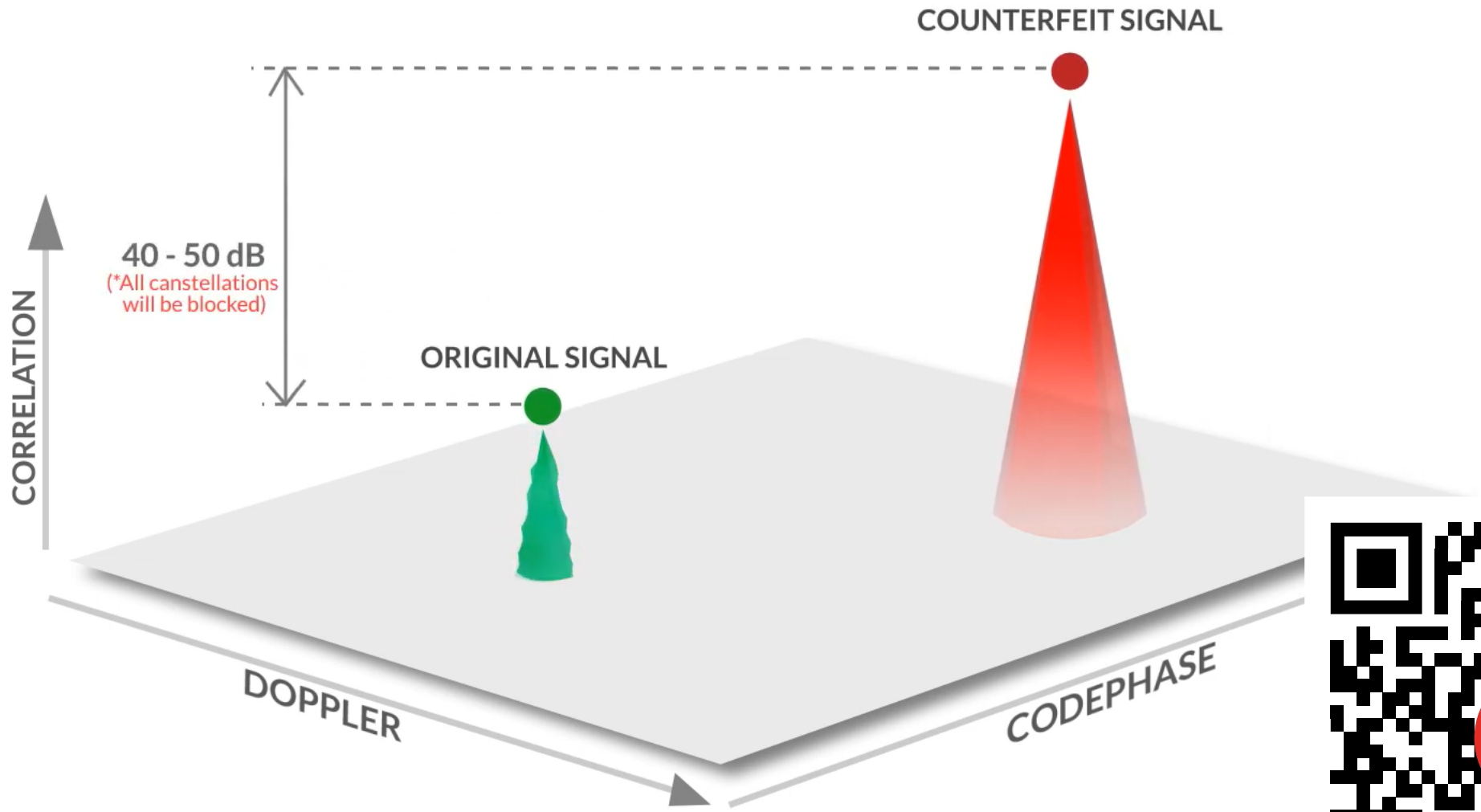
# Сценарии атак. ГНСС спуфинг с синхронизацией. Когерентная атака




Стоимость атаки – 1k\50k USD
Время атаки – мгновенно

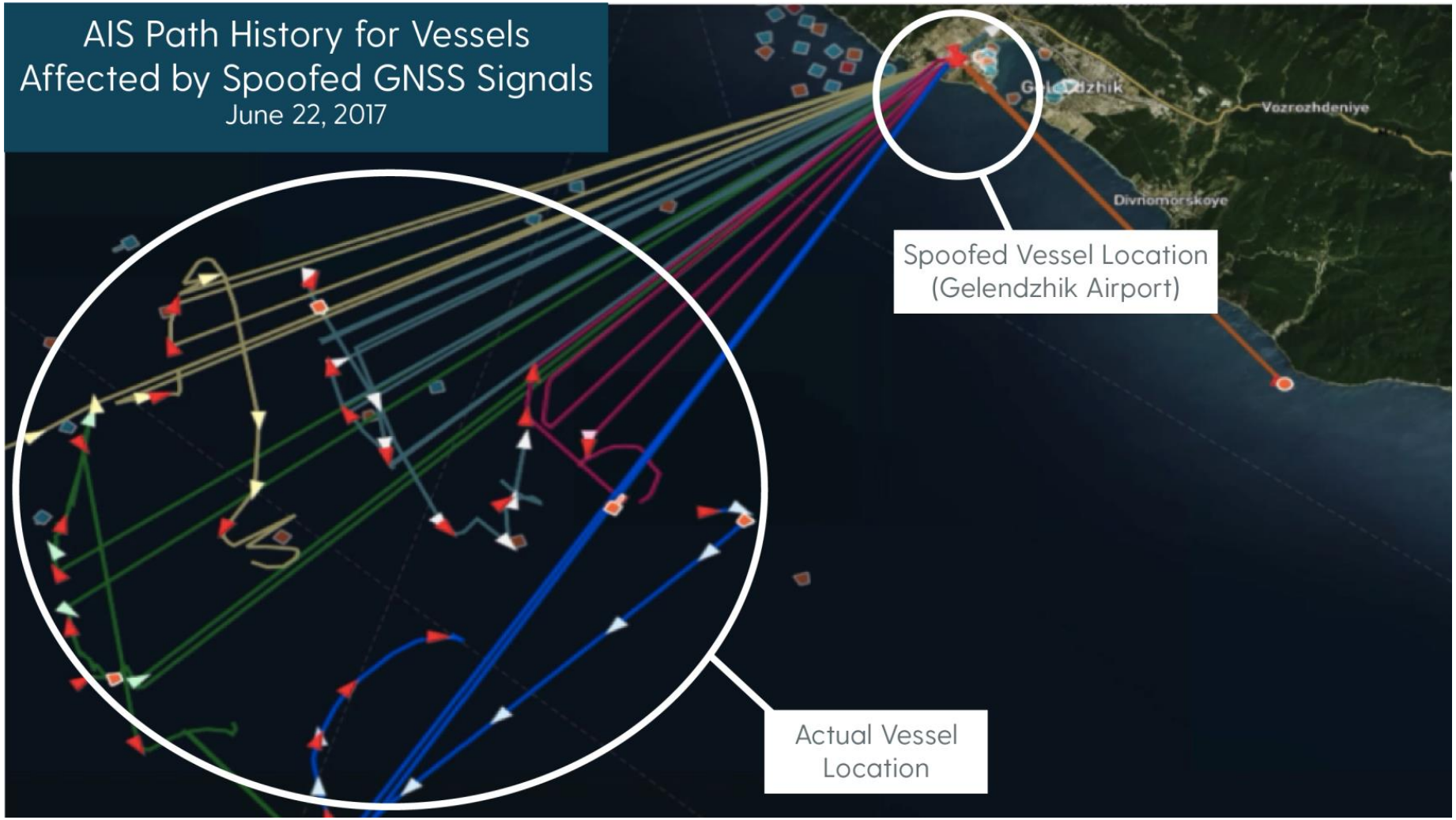
Защита – системы детектирования спуфинга с анализом пространственных характеристики + альтернативный источник PNT.

# Типы Спуфинга



# Отчет C4ADS о спуфинге в России и Сирии “ABOVE US ONLY STARS”

С февраля 2016 по ноябрь 2018 обнаружено **9883** инцидента с 1311 судами




https://www.c4reports.org/aboveusonlystars

# Декабрь 2019. Фермер с помощью ГНСС джамера защищался от дронов

South China Morning Post

SUBSCRIBE

China / People & Culture

China Society

+ FOLLOW

## China flight systems jammed by pig farm's African swine fever defences

- Reports of criminal gangs using drones to spread infection led to installation of jamming device
- Unauthorised equipment interfered with navigation systems of planes flying overhead

Mandy Zuo + FOLLOW

Published: 5:15pm, 20 Dec, 2019

Why you can trust SCMP

TOP PICKS

2.4k

*How Lever Style chairman Stanley Szeto learned from past mistakes to thrive in his industry*

In Partnership With: **Withers HK**

Post

News

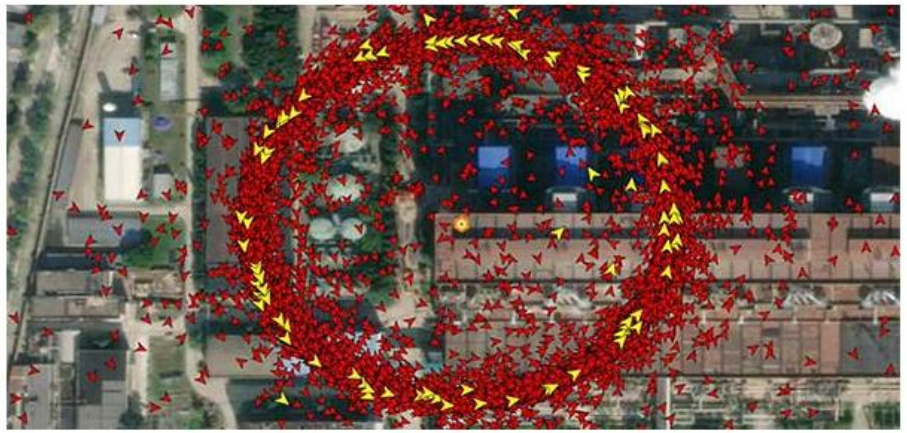
We won't join an alliance against China, Vietnam vows ahead of key US visit

25 Aug 2021

https://www.scmp.com/news/china/society/article/3042991/china-flight-systems-jammed-pig-farms-african-swine-fever

# Декабрь 2019. Спуфинг в порту Шанхая





## Chinese GPS spoofing circles could hide Iran oil shipments

December 17, 2019 - By Dana Goward

Est. reading time: 2 minutes

"GPS spoofing circles" have been discovered at 20 locations along the Chinese coast, according to the non-profit environmental group Skytruth. Of the locations observed, 16 were oil terminals; the others were corporate and government offices.

GPS spoofing in Shanghai that resulted in reported positions from ships,



https://www.gpsworld.com/chinese-gps-spoofing-circles-could-hide-iran-oil-shipments/

# Январь 2020. В 85% краж автотранспорта в Мексике используется ГНСС джаминг

EL ECONOMISTA

TOKYO 2020 ANÚNCIATE SUSCRÍBETE

El Economista > Empresas

TELECOMUNICACIONES

## Ley anti-jammer, que prohíbe los bloqueadores de video, voz y datos, entra en vigor este sábado

Este sábado 25 de enero de 2020 entrará en vigor una reforma a diversos artículos de la Ley Federal de Telecomunicaciones y del Código Penal Federal, que tiene el objetivo de reducir los delitos cometidos con el uso de aparatos que bloquean las comunicaciones inalámbricas.

*Nicolás Lucas*
24 de enero de 2020, 15:27




MÁS POPULARES


2 Los hogares ricos se beneficiaron más de los apoyos sociales; la política no es progresiva ni interseccional

*Por Ana Karen García* Hace 1 hora

La radio de religión se

https://www.eleconomista.com.mx/empresas/Ley-anti-jammer-que-prohibe-los-bloqueadores-de-video-voz-y-datos-entra-en-vigor-este-sabado-20200124-0053.html

# Август 2020. Китайские рыбаки подделывали свои координаты

stuff ☰ | environment | Log in

## Chinese vessels off Galapagos 'cloaking' in New Zealand

Andrea Vance · 10:24, Aug 06 2020


The Indonesian government is calling on Beijing to respond to accusations that Indonesian nationals were worked to death on board Chinese fishing vessels.



A fleet of Chinese "ghost ships" were falsely reporting their location within New Zealand waters while they fished off the Galapagos Islands.



most popular

1 Covid-19: Health staff able to work from home upset at being told to go to office

2 Covid-19 full coverage: Person associated with Ōtāhuhu College confirmed as Covid-19 case

https://www.stuff.co.nz/environment/122339295/chinese-vessels-off-galapagos-cloaking-in-new-zealand

**Ноябрь 2020. Морская администрация США предупреждает, что с проблемы с ГНСС, теперь стандартная ситуация на коммерческих рейсах между США, Европой и Ближним Востоком.**



Most Popular

Investors continue to buy into the tech rally, lifting global markets


As Bitcoin soars to near $50,000, Elon Musk's profit jumps by 250%


Why it's taking so long to get COVID vaccines for kids under 12

TECH • GPS

# Planes continue to fly into a GPS dark hole over the Mediterranean, puzzling experts

BY KATHERINE DUNN

November 1, 2020 4:00 PM GMT+3

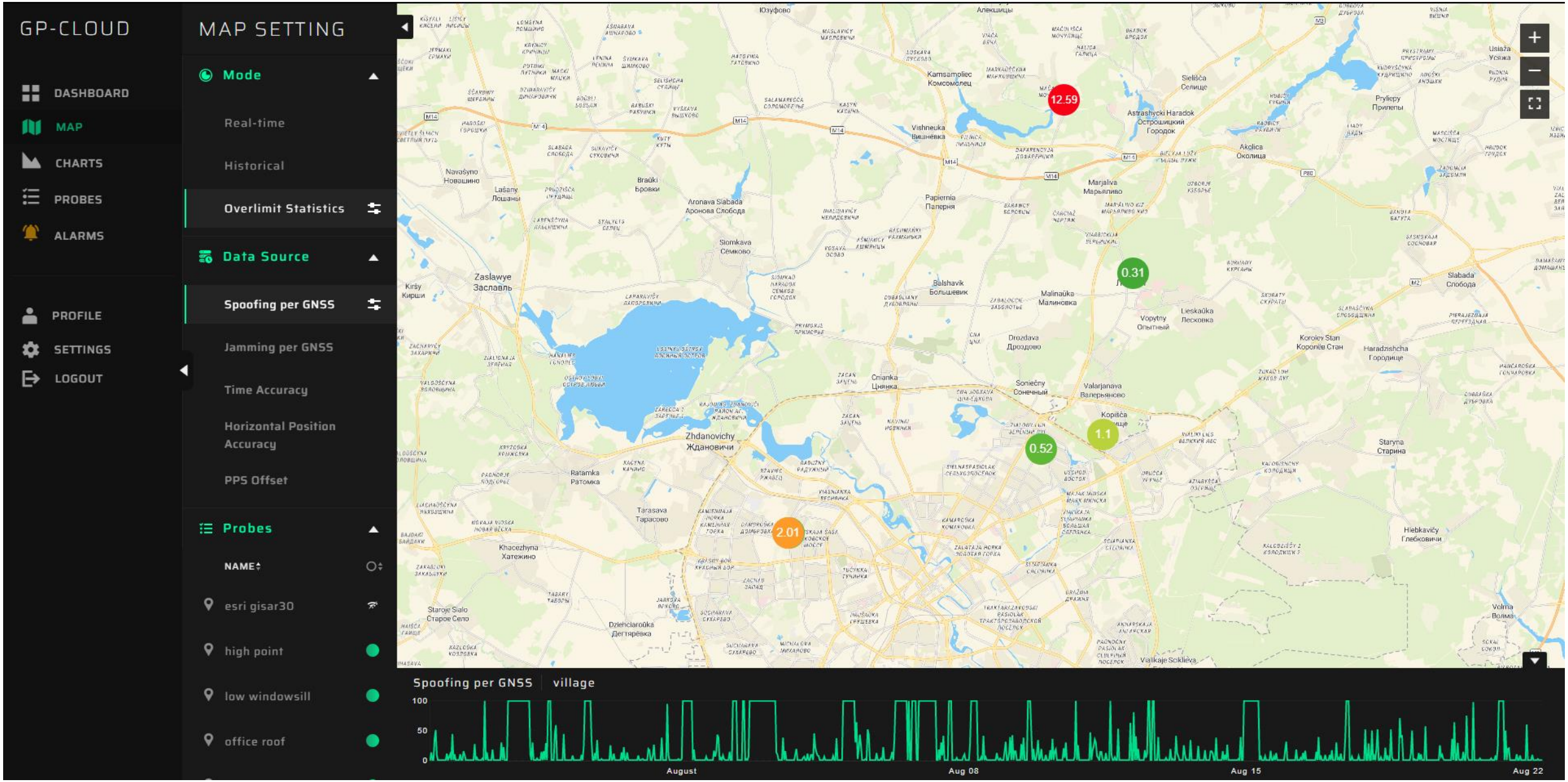

## Related Articles

INTERNATIONAL

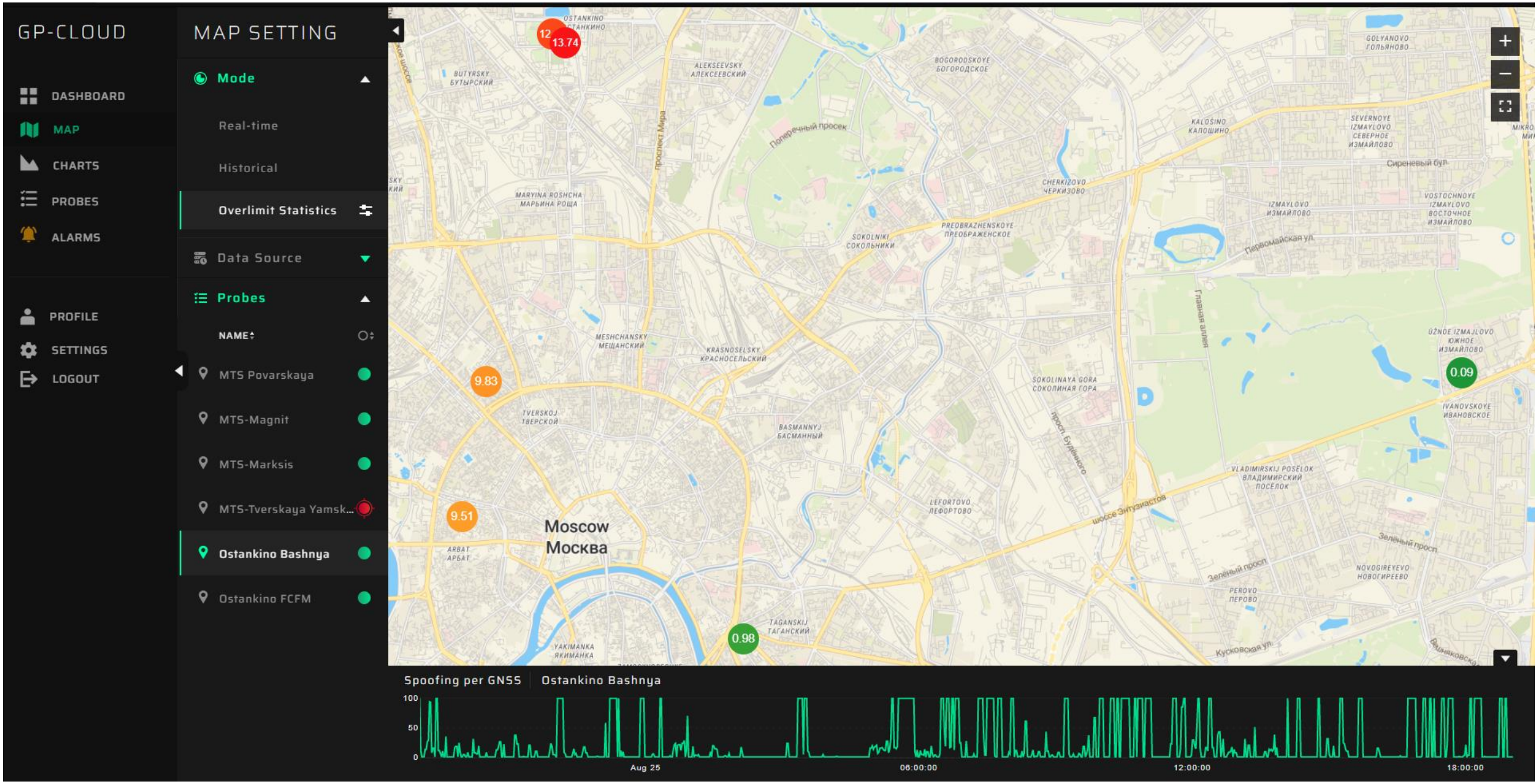
Sudoku creator and Nikoli CEO Maki Kaji dies after life spreading the joy of puzzles

https://fortune.com/2020/11/01/planes-ships-gps-mediterranean-russia-syria-north-korea/

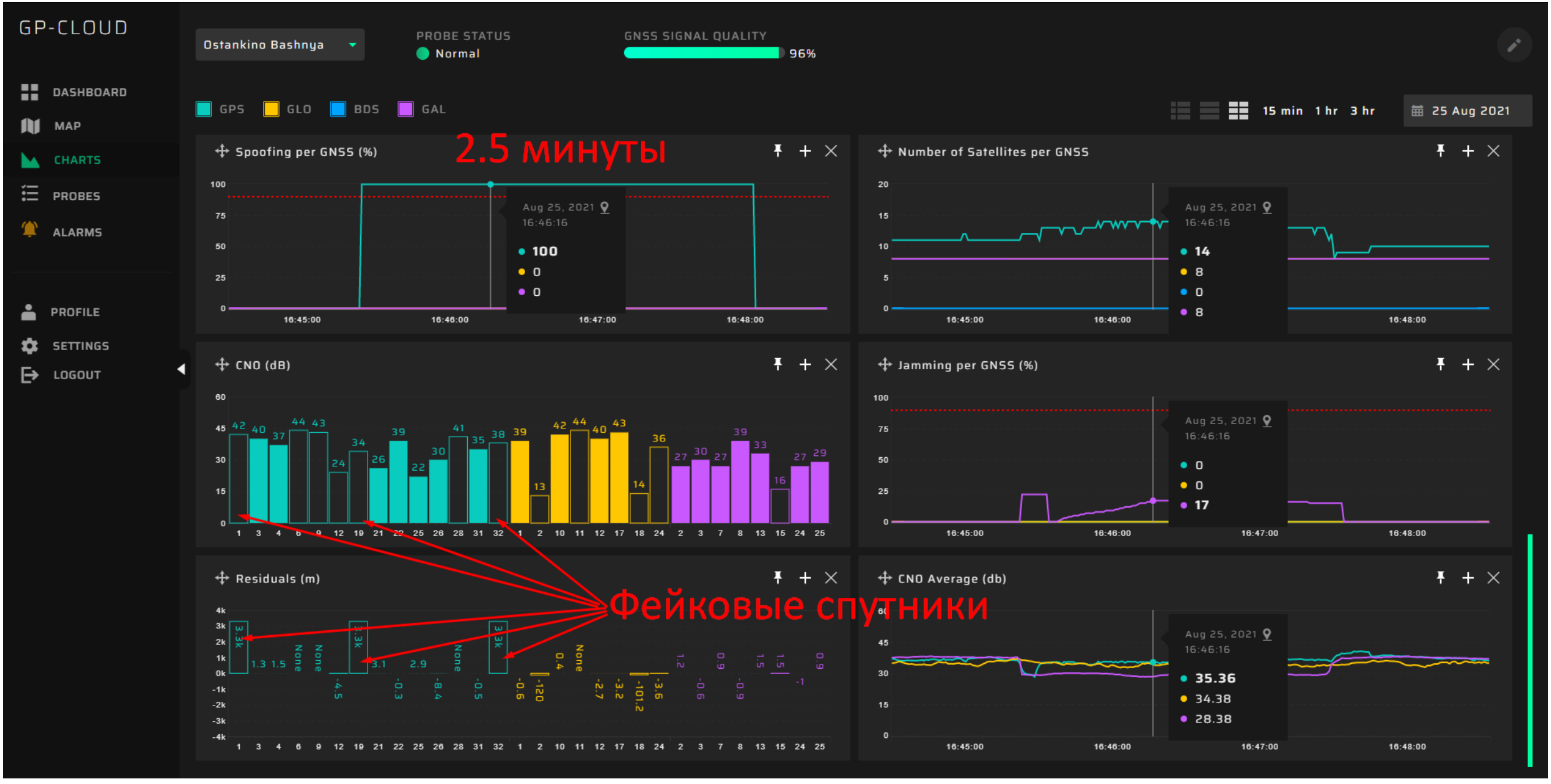
# Минск. Статистика по спуфингу за Август 2021



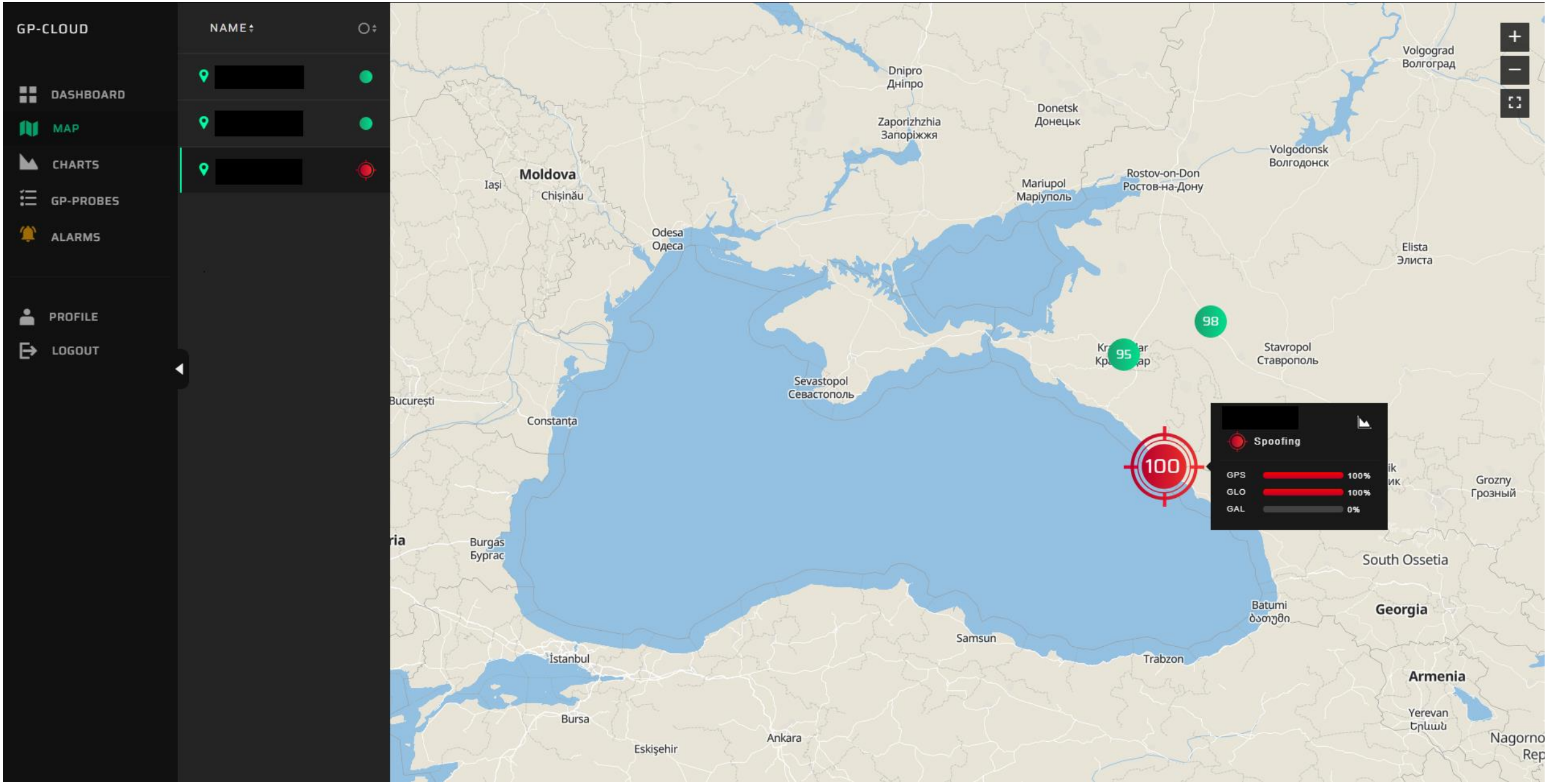
# Москва. Статистика по спуфингу за 25 Августа 2021



# Москва. Инцидент 2.5 минуты

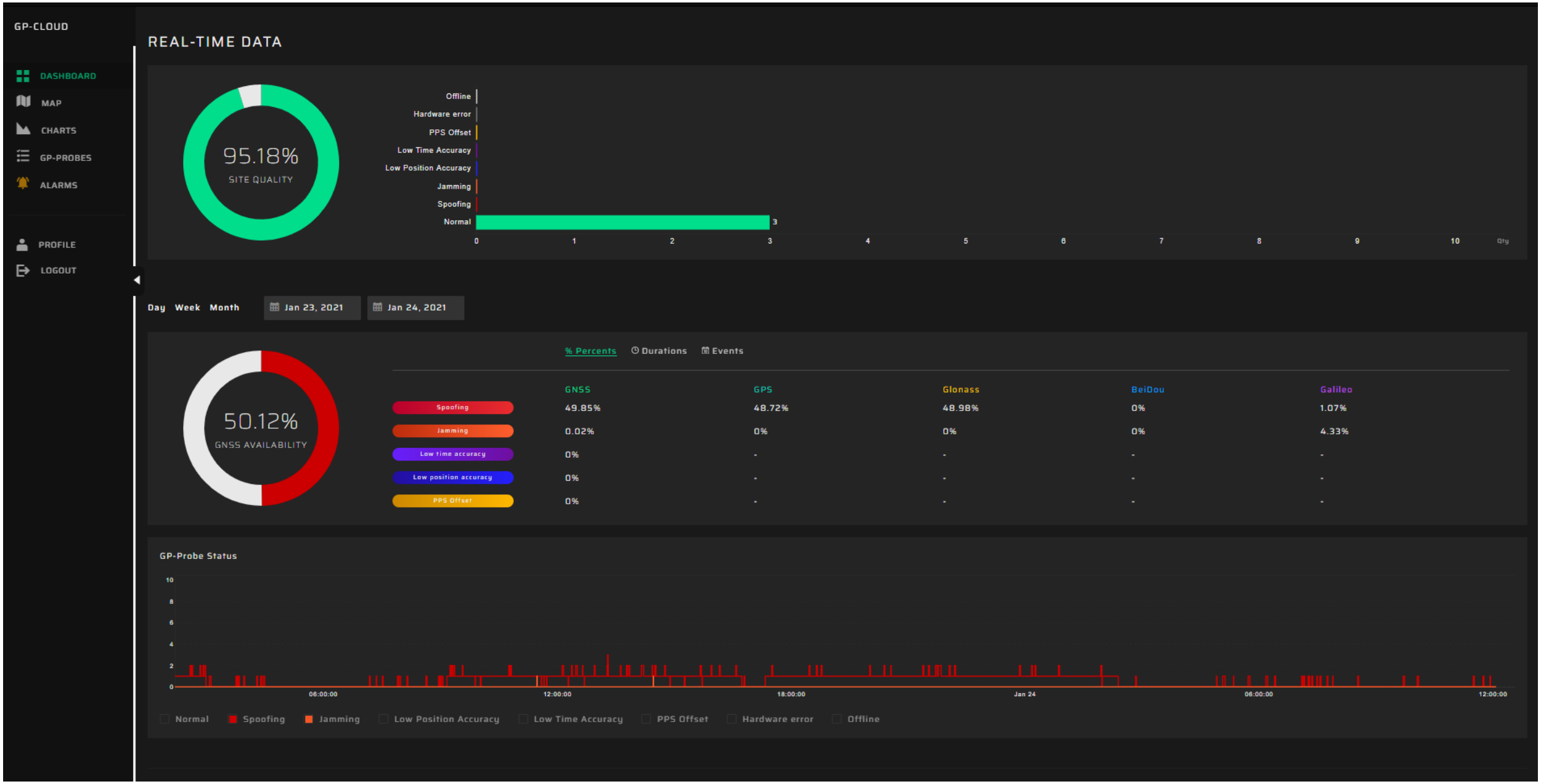


# Краснодар. 30 часов спуфинга за двое суток



# Краснодар. 30 часов спуфинга за двое суток

# Краснодар. 30 часов спуфинга за двое суток



# Регуляции в США. Февраль 2020. Приказ Трампа 13905

"Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing (PNT) Services"

**Sec. 4**. *Implementation*. (a) **Within 1 year** of the date of this order, the Secretary of Commerce, in coordination with the heads of SSAs and in consultation, as appropriate, with the private sector, **shall develop and make available**, to at least the appropriate agencies and private sector users, **PNT profiles**. The PNT profiles will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Once made available, the PNT profiles shall be reviewed every 2 years and, as necessary, updated.

# Регуляции в США. Декабрь 2020. Department of Homeland Security

"Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework"

- Level 1

  - восстановление системы PNT с помощью ручного сброса (после устранения причин сбоя – спуфинга)

- Level 2

  - система PNT должна иметь несколько источников данных (например, GPS и инерциальную систему навигации)
  - система должна определять наличие спуфинга и отключать скомпрометированный источник.
  - разрешается ненормированная деградация точности определения PNT при воздействии спуфинга

- Level 3

  - разрешается нормированная деградация точности под спуфингом

- Level 4

  - наличие множества источников PNT
  - требуется сохранение производительности и точности в присутствии спуфинга

# Регуляции в США. Февраль 2021. NIST

"Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services"

- Цели:
  - идентификация систем зависящих от сервисов PNT
  - выбор источников PNT
  - детектирование искажений и манипуляций PNT
  - управление рисками

- Требования, связанные с ГНСС спуфингом
  - имитация ГНСС спуфинга (и других эффектов, снижающих точность PNT) для тестирования приемника\системы
  - детектирование, классификация, логирование и постанализ аномалий в данных PNT
  - анализ точности\качества PNT
  - определение статистики инцидентов
  - анализ метода атаки
  - анализ спектра в полосах ГНСС
  - локализация источника спуфинга

GPSPATRON

kaspersky

# Спасибо за внимание


Бородько Максим

CEO @ GPSPATRON