



# Статистика работы Wi-Fi сети во время Fortinet Security Day 2019

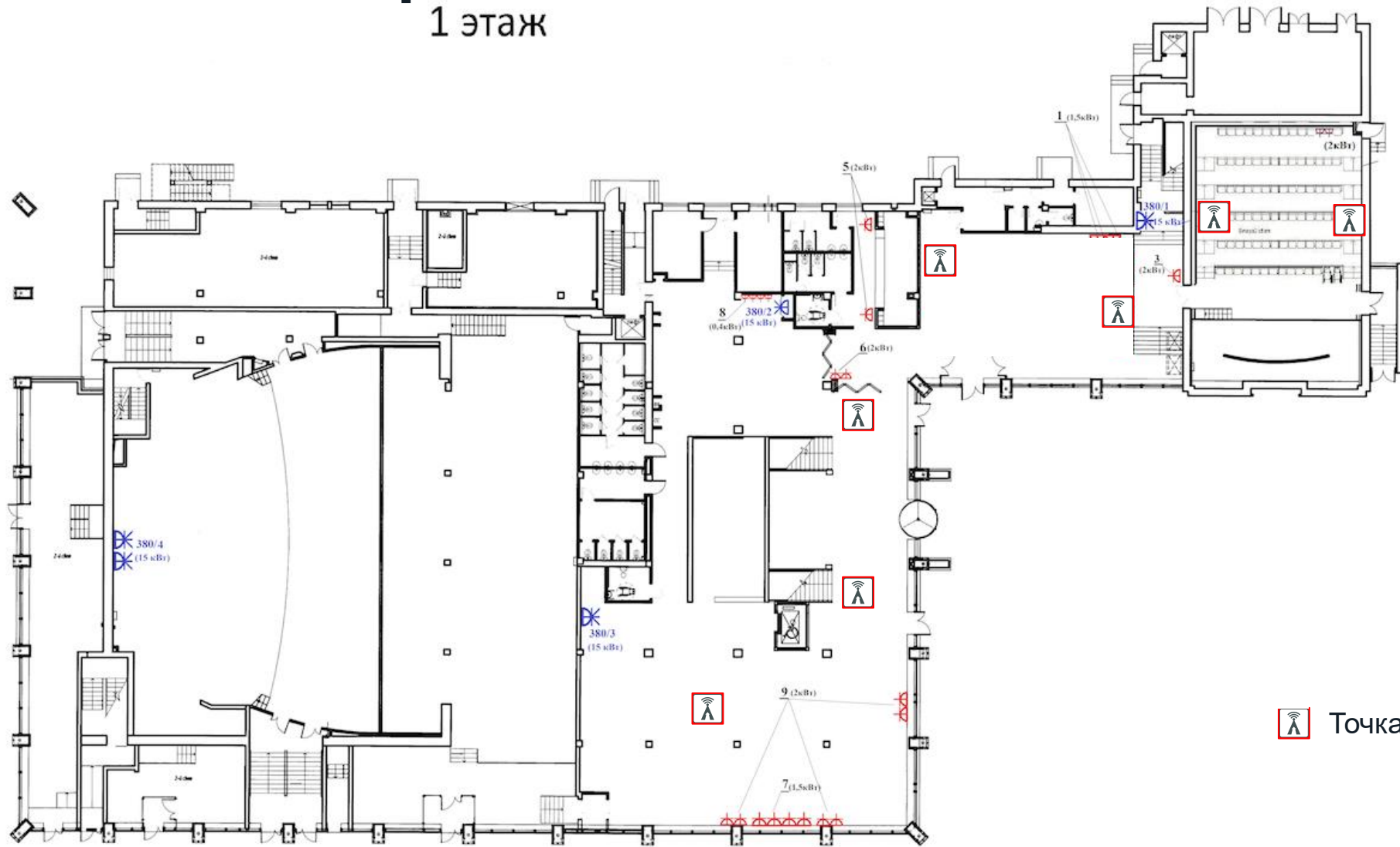
Юрий Захаров, системный инженер


[yzakharov@fortinet.com](mailto:yzakharov@fortinet.com)

12 сентября 2019

# План помещения

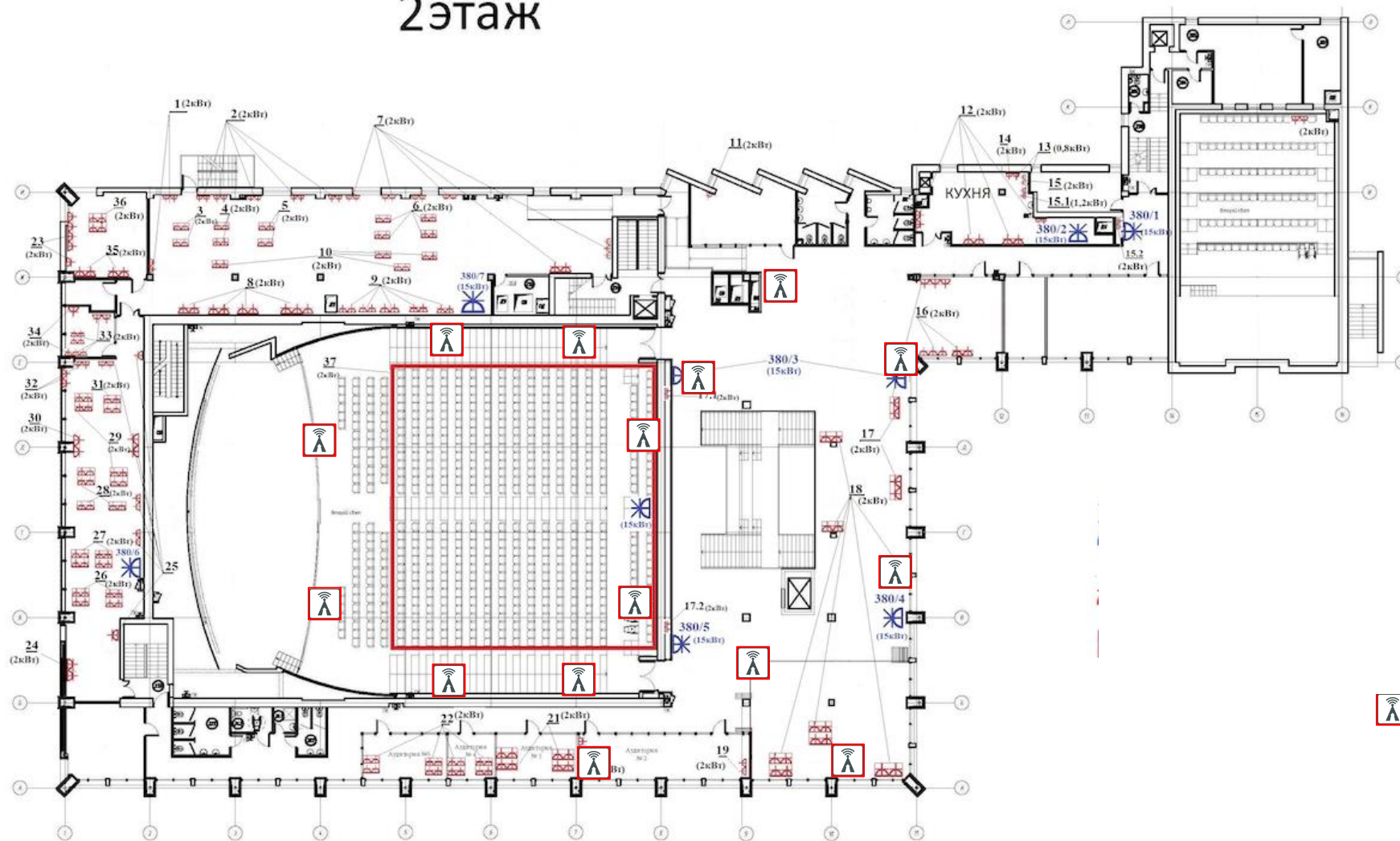
## 1 этаж



 Точка доступа Fortinet AP832e

# План помещения

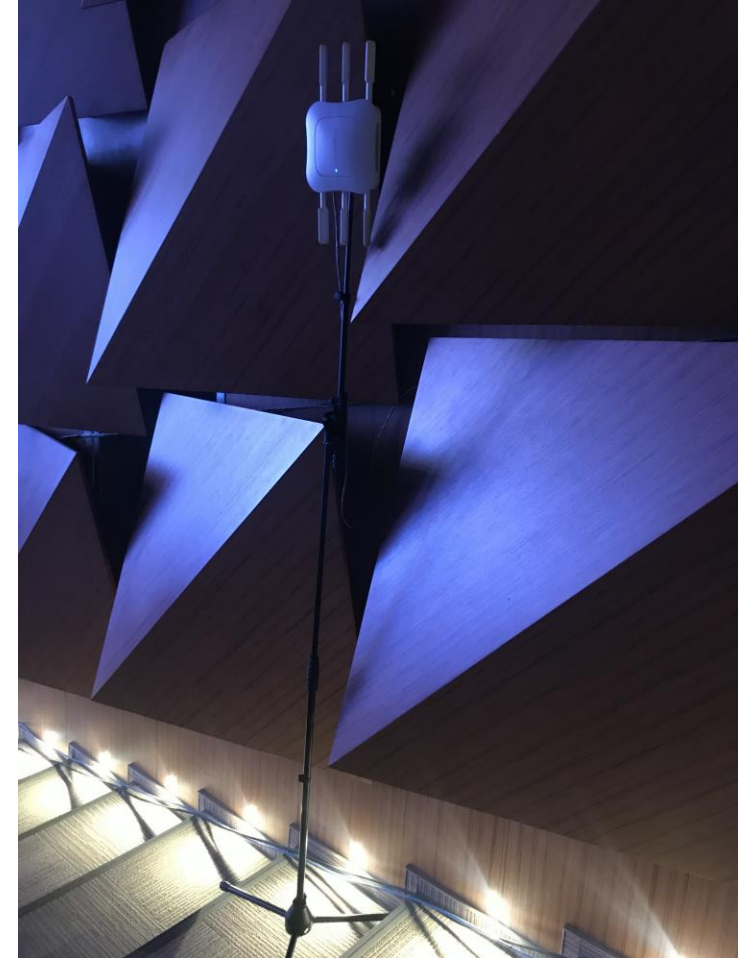
## 2 этаж



 Точка доступа Fortinet AP832e

# Состав оборудования

- 22 точки доступа (802.11ac, 3x3:3ss) – AP832e
- 3 коммутатора с портами PoE – FS-424D-FPOE
- 1км кабеля UTP
- Аппаратный контроллер FWC-500D
- Система управления – FWM-VM
- Система аналитики – FortiPresence
- Шлюз безопасности FortiGate 300E
- Система сбора логов – FortiAnalyzer



# Статистика и результаты

- Общее число посетителей конференции: более 800 человек
- Было одновременно подключено к сети в среднем 300 клиентов
- Канал доступа в Интернет: 200Мбит/с
- Измерения производительности (клиент iPhone 7, 802.11ac, 2ss) :
  - » Download 90Мбит/с,
  - » Upload 110Мбит/с
- Частотные каналы, задействованные в рамках БЛВС:
  - » 2 канала 5GHz, ширина каждого 40MHz: 44+48, 149+153
  - » 2 канала 2.4GHz, ширина каждого 20MHz: 6, 11
- Клиенты распределялись по диапазонам 5/2.4GHz в соотношении 65/35
- Клиенты равномерно распределялись по каналам в рамках одного диапазона
- Качественная работа сервиса у всех абонентов

# Fortinet Security Day 2019

**FORTINET** FortiWLC 8.4-4build-8 | FortiWLC-500D
12:16:48 FWC-500D@10.10.7.110
admin

- Monitor
- Dashboard
- System
- Radio
- Station
- Voice
- WIPS
- Fault Dashboard
- Spectrum Manager
- Diagnostics
- Global Statistics
- Devices
- Statistics
- QoS/Voice
- Topology
- Top 10
- Configuration
- Maintenance
- Wizards

## System Dashboard [Graph Help] ?

System
Service Control
Application

TRENDING
DRAG AND SELECT AN AREA ON CHART TO ZOOM-IN. DOUBLE CLICK TO ZOOM-OUT.

### THROUGHPUT

### STATION

DISTRIBUTION
▼

ALARMS BY SEVERITY (0)

STATIONS BY SSID (286)

STATIONS BY RF BAND (286)

STATIONS BY OS TYPE (286)

WIRELESS CONFIGURATION

SSID	RF Virtualization Mode	Datanlane Mode	Multicast	I2 Security Mode	Captive Portal	MAC Filtering	2.4G Radio	5G Radio

# Fortinet Security Day 2019

FORTINET FortiWLC 8.4-4build-8   FortiWLC-500D														15:08:49	FWC-500D@10.10.7.110	☆	🔍	📄	🔗	admin
Access Points (22 entries)																				
<span>REFRESH</span> <span>ADD</span> <span>EDIT</span> <span>DELETE</span> <span>BULK UPDATE</span> <span>VIEW</span>																				
	AP ID	AP Name	MAC Address	Uptime	Operational State	Availability Status ▲	Runtime Image Version	Connectivity Layer	AP IP Address for L3	AP Model	AP Group Name	Feature Group Name	Operating Mode							
🔍						Online														
🔍	1	3-AP1	00:0c:e6:31:55:d8	00d:16h:02m:34s	Enabled	Online	8.4-4build-8	L3	10.10.100.10	AP832e	-	-	Normal							
🔍	2	3-AP2	00:0c:e6:31:57:2a	00d:15h:56m:00s	Enabled	Online	8.4-4build-8	L3	10.10.100.11	AP832e	-	-	Normal							
🔍	3	3-AP3	00:0c:e6:31:67:22	00d:18h:03m:50s	Enabled	Online	8.4-4build-8	L3	10.10.100.16	AP832e	-	-	Normal							
🔍	4	3-AP4	00:0c:e6:31:56:16	00d:18h:03m:51s	Enabled	Online	8.4-4build-8	L3	10.10.100.17	AP832e	-	-	Normal							
🔍	5	3-AP5	00:0c:e6:31:67:0a	00d:18h:03m:52s	Enabled	Online	8.4-4build-8	L3	10.10.100.18	AP832e	-	-	Normal							
🔍	6	3-AP6	00:0c:e6:31:66:ba	00d:18h:03m:51s	Enabled	Online	8.4-4build-8	L3	10.10.100.19	AP832e	-	-	Normal							
🔍	7	3-AP7	00:0c:e6:31:67:32	00d:18h:03m:53s	Enabled	Online	8.4-4build-8	L3	10.10.100.20	AP832e	-	-	Normal							
🔍	8	3-AP8	00:0c:e6:31:57:32	00d:14h:40m:12s	Enabled	Online	8.4-4build-8	L3	10.10.100.21	AP832e	-	-	Normal							
🔍	9	3-AP9	00:0c:e6:31:67:14	00d:14h:40m:12s	Enabled	Online	8.4-4build-8	L3	10.10.100.22	AP832e	-	-	Normal							
🔍	10	3-AP10	00:0c:e6:31:67:18	00d:14h:40m:11s	Enabled	Online	8.4-4build-8	L3	10.10.100.25	AP832e	-	-	Normal							
🔍	11	3-AP11	00:0c:e6:31:66:fe	00d:14h:40m:09s	Enabled	Online	8.4-4build-8	L3	10.10.100.24	AP832e	-	-	Normal							
🔍	12	3-AP12	00:0c:e6:31:66:c2	00d:14h:40m:10s	Enabled	Online	8.4-4build-8	L3	10.10.100.28	AP832e	-	-	Normal							
🔍	13	3-AP13	00:0c:e6:31:67:36	00d:14h:40m:11s	Enabled	Online	8.4-4build-8	L3	10.10.100.30	AP832e	-	-	Normal							
🔍	14	3-AP14	00:0c:e6:31:64:ac	00d:14h:35m:58s	Enabled	Online	8.4-4build-8	L3	10.10.100.29	AP832e	-	-	Normal							
🔍	15	1-AP1	00:0c:e6:31:65:7c	00d:05h:32m:45s	Enabled	Online	8.4-4build-8	L3	10.10.100.23	AP832e	-	-	Normal							
🔍	16	1-AP3	00:0c:e6:31:58:3a	00d:05h:32m:45s	Enabled	Online	8.4-4build-8	L3	10.10.100.15	AP832e	-	-	Normal							
🔍	17	1-AP5	00:0c:e6:31:58:3e	00d:05h:32m:43s	Enabled	Online	8.4-4build-8	L3	10.10.100.35	AP832e	-	-	Normal							
🔍	18	1-AP7	00:0c:e6:31:58:86	00d:05h:32m:44s	Enabled	Online	8.4-4build-8	L3	10.10.100.36	AP832e	-	-	Normal							
🔍	19	2-AP2	00:0c:e6:31:57:f8	00d:14h:28m:25s	Enabled	Online	8.4-4build-8	L3	10.10.100.38	AP832e	-	-	Normal							
🔍	20	2-AP4	00:0c:e6:31:57:c2	00d:14h:28m:26s	Enabled	Online	8.4-4build-8	L3	10.10.100.39	AP832e	-	-	Normal							
🔍	21	2-AP6	00:0c:e6:31:66:ac	00d:14h:28m:26s	Enabled	Online	8.4-4build-8	L3	10.10.100.42	AP832e	-	-	Normal							

# Fortinet Security Day 2019

- Monitor
- Configuration
  - System Config
  - Security
  - Wireless
    - Radio
    - ARRP
    - Hotspot 2.0
    - ESS
    - Load Balance
    - Mesh
  - Wired
  - Policies
  - Devices
  - Access Control
  - WIPS

ESS-AP Configuration (36 entries) ?

ESS Profile **ESS-AP Table** Security Profiles Hotspot Profiles

REFRESH ADD EDIT DELETE VIEW

	ESS Profile	AP ID	AP Name	Interface Index	Channel	Operating Channel	Admin State	Max Calls	BSSID	Owner
<input type="checkbox"/>									00:0c:e6:02:c3:c3	
<input checked="" type="checkbox"/>	ESS3	9	3-AP9	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	8	3-AP8	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	7	3-AP7	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	6	3-AP6	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	5	3-AP5	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	4	3-AP4	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	3	3-AP3	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	2	3-AP2	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	18	1-AP7	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	17	1-AP5	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	16	1-AP3	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	15	1-AP1	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller
<input checked="" type="checkbox"/>	ESS3	14	3-AP14	2	157	157	Up	0	00:0c:e6:02:c3:c3	controller

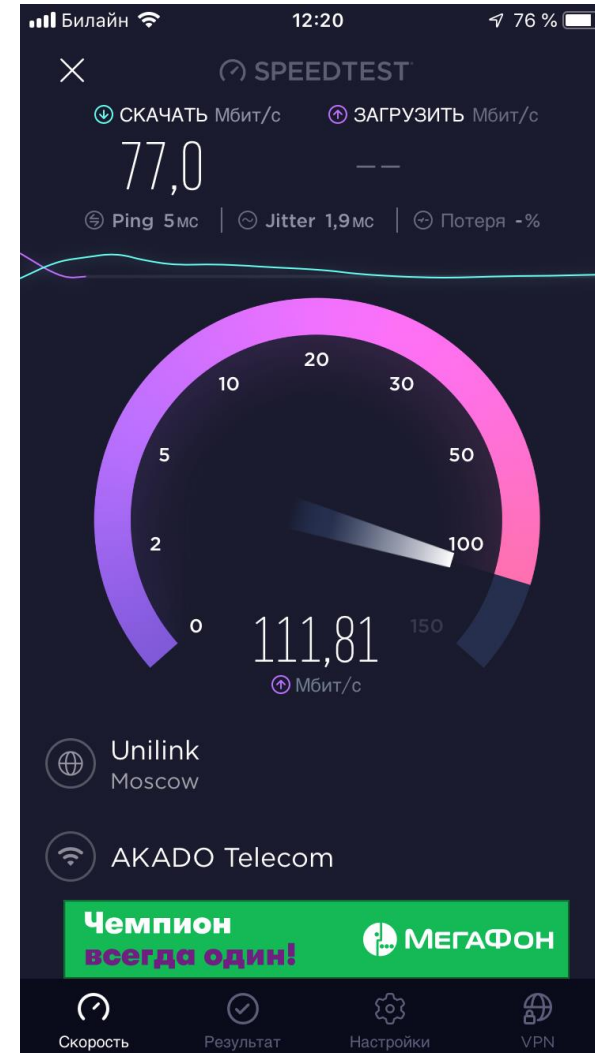
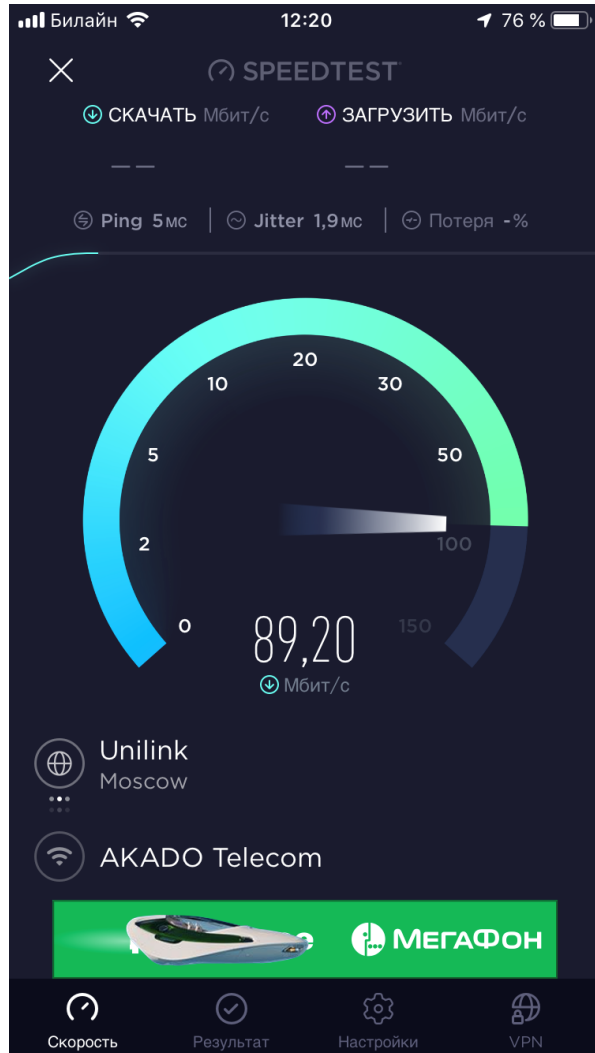
NetSpot - Discover and analyze wireless networks around you

DISCOVER SURVEY EXPORT USER GUIDE ASK A QUESTION UPGRADE NOW

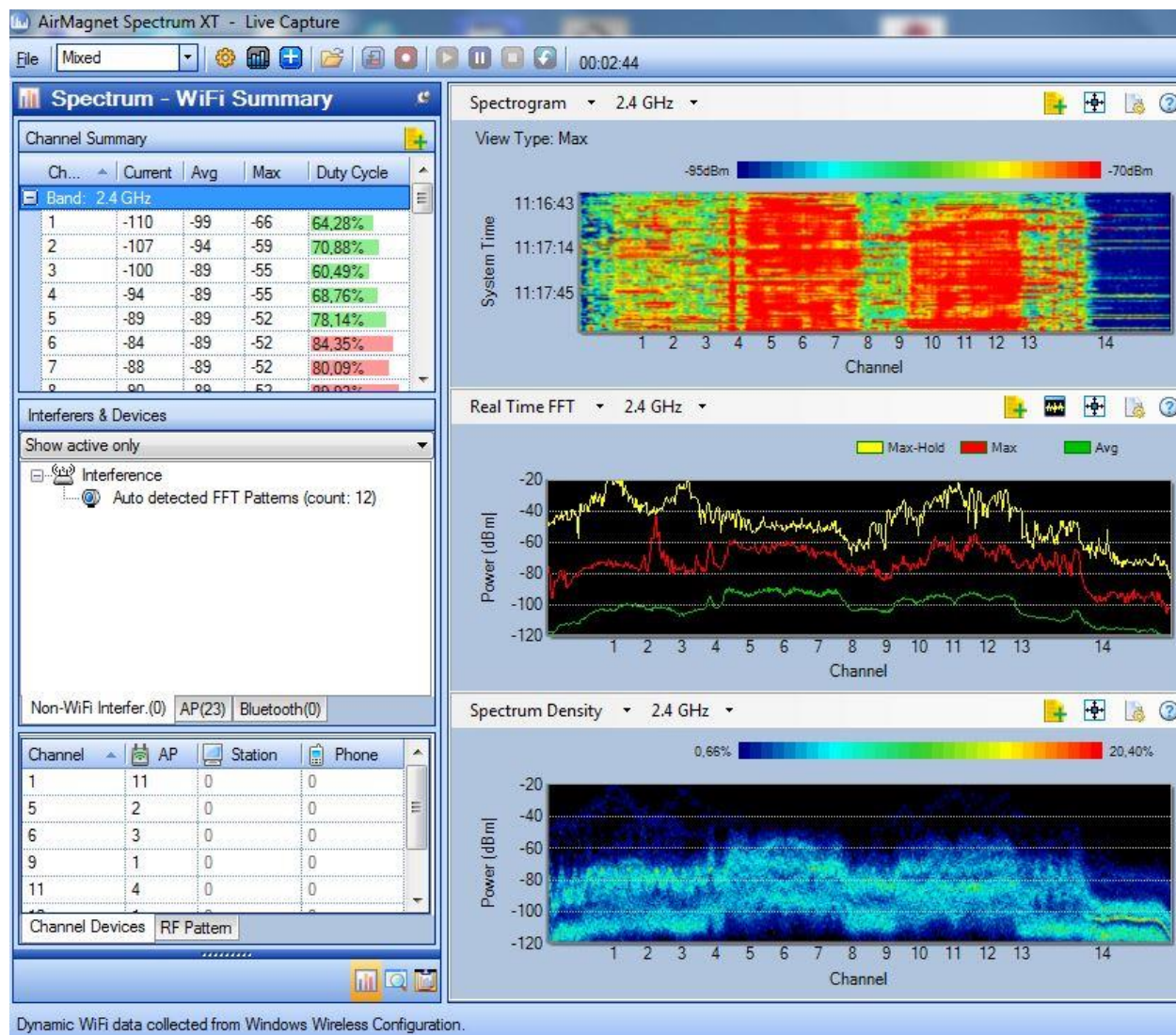
BSSID	Channel	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signal...	Avg	Max	Min	Noise	Nois...	Last seen
<input checked="" type="checkbox"/> SecurityDAY 00:0C:E6:02:C7:82	6	2.4GHz	WPA2 Personal	Meru	g/n	-67	33%	-50	-33	-85	-85	15%	now	
<input checked="" type="checkbox"/> SecurityDAY 00:0C:E6:02:4F:38	11	2.4GHz	WPA2 Personal	Meru	g/n	-54	46%	-66	-34	-81	-85	15%	now	
<input checked="" type="checkbox"/> SecurityDAY 00:0C:E6:02:BE:BB	44,+1	5GHz	WPA2 Personal	Meru	ac	-54	46%	-75	-41	-89	-85	15%	now	
<input checked="" type="checkbox"/> SecurityDAY 00:0C:E6:02:C3:C3	157,+1	5GHz	WPA2 Personal	Meru	ac	-64	36%	-62	-39	-89	-85	15%	now	



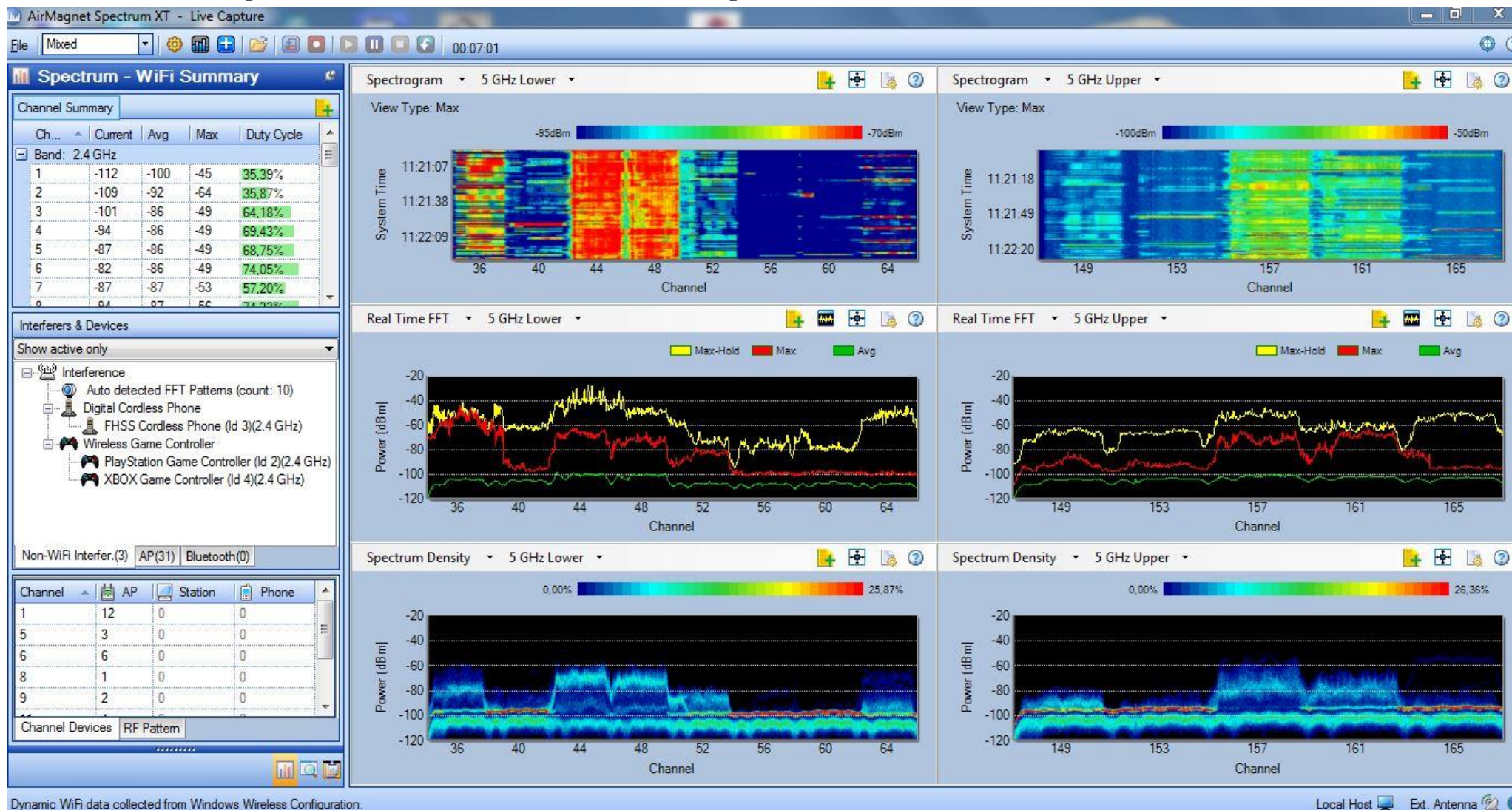
# Fortinet Security Day 2019



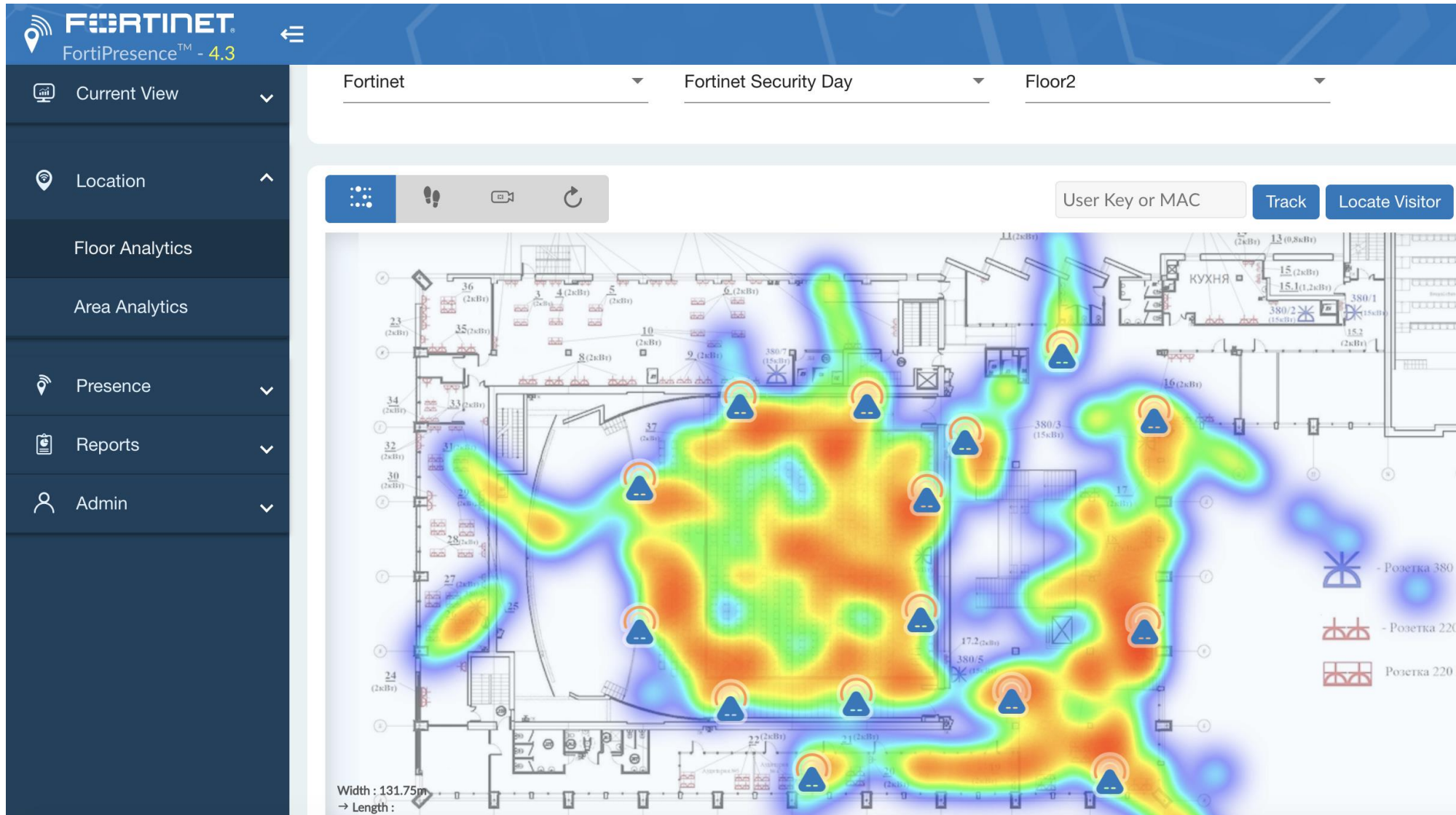
# Fortinet Security Day 2019: замеры анализатором спектра (диапазон 2.4ГГц)



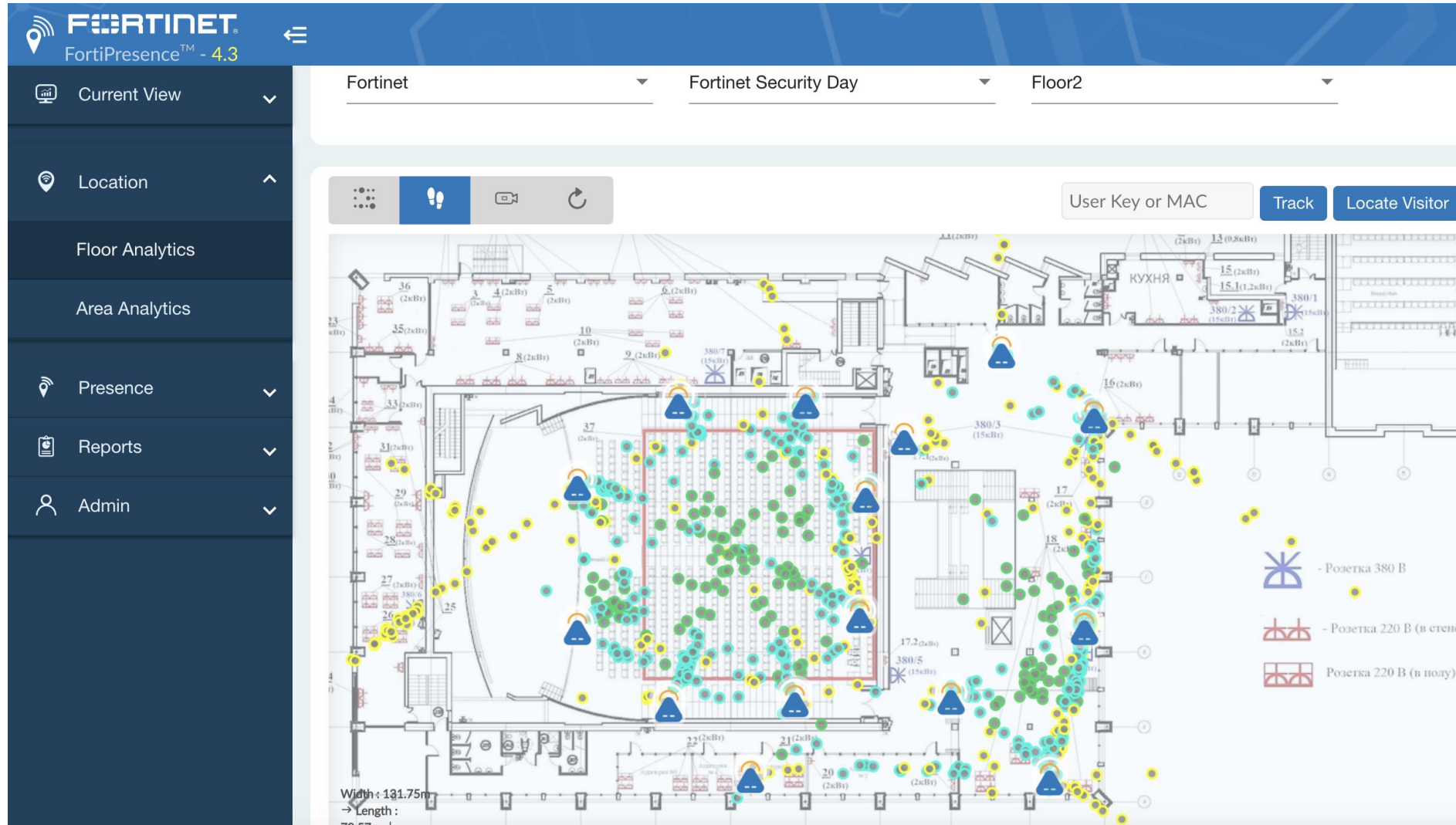
# Fortinet Security Day 2019: замеры анализатором спектра (диапазон 5ГГц)



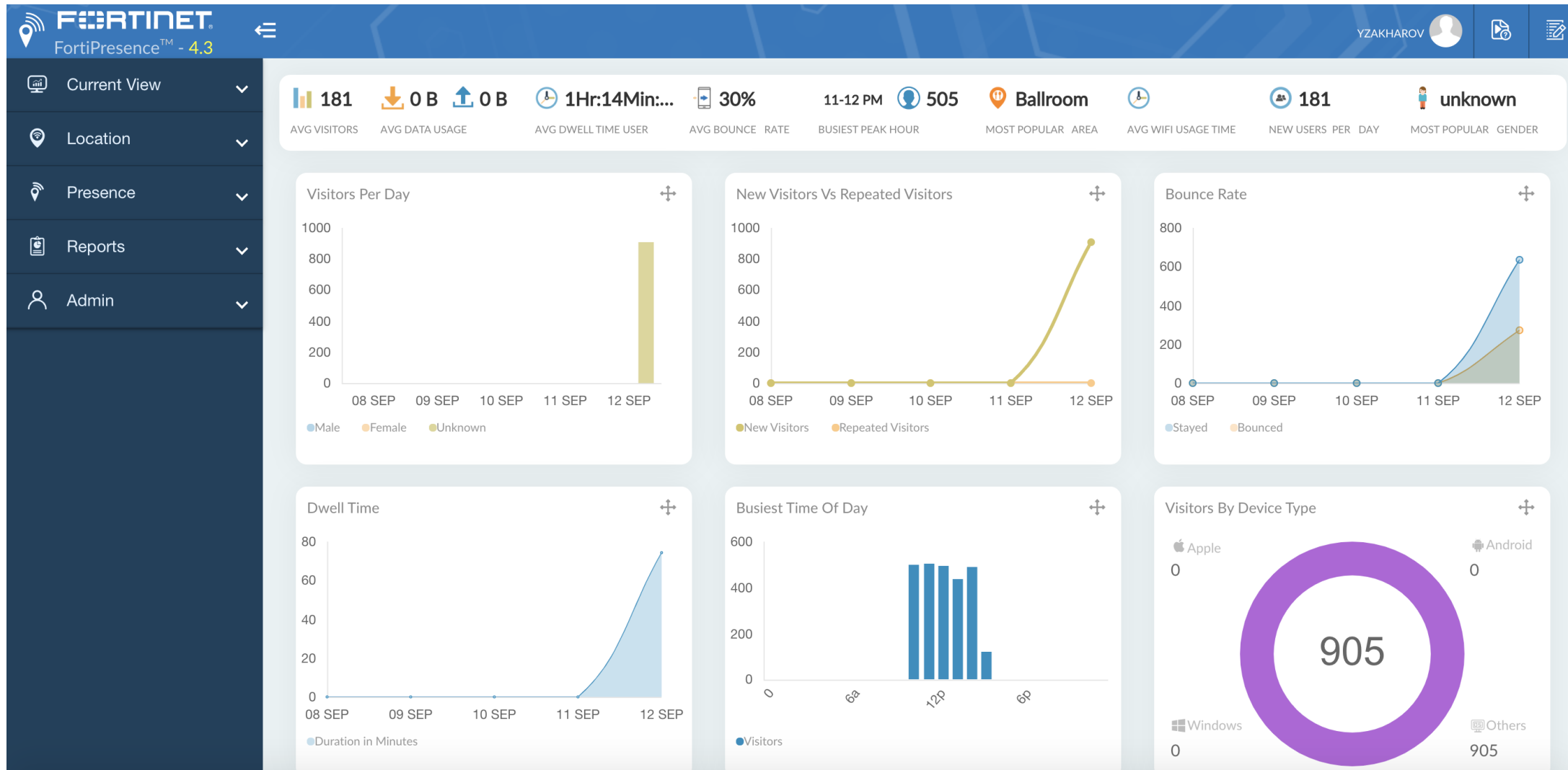
# Fortinet Security Day 2019: FortiPresence Heat Maps



# FortiPresence: местоположение клиентов



# Fortinet Security Day 2019: аналитика FortiPresence

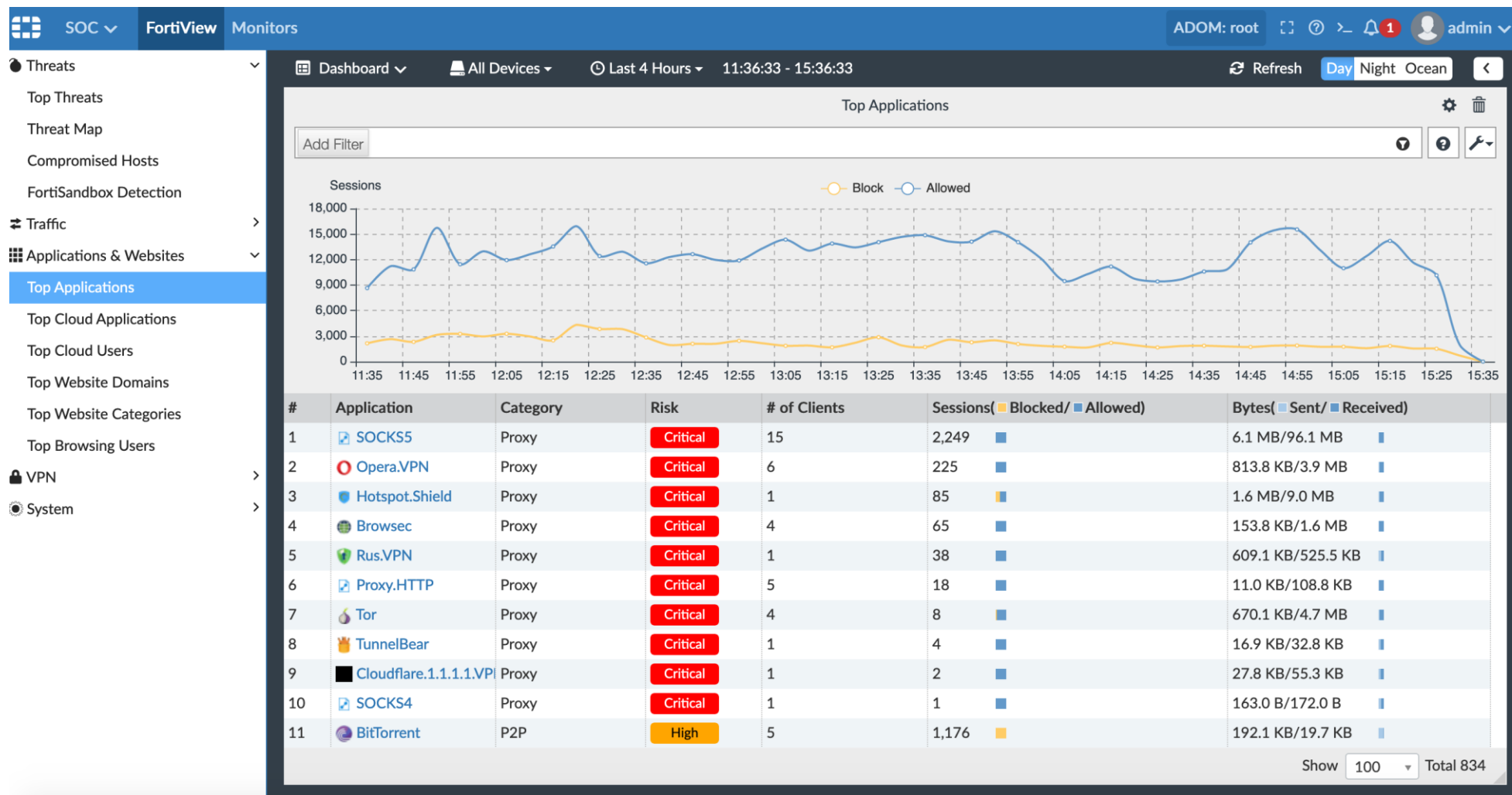


# Fortinet Security Day 2019: пример выявленной угрозы

The screenshot displays the Fortinet FortiView SOC interface. The top navigation bar includes 'SOC', 'FortiView', and 'Monitors'. The user is logged in as 'ADOM: root' and 'admin'. The left sidebar shows navigation options: Threats, Top Threats, Threat Map, Compromised Hosts (selected), FortiSandbox Detection, Traffic, Applications & Websites, VPN, and System. The main content area shows a 'Drilldown Panel' for a threat with 'epid = 1354'. The summary includes: End User (192.168.52.84), Last Detected (09/12/2019), Host Name (192.168.52.84), OS, and Device Name (FortiGate-300E). The verdict is 'Infected' with a '# of Threats' of 1. Below the summary is a table with two tabs: 'Blacklist' and 'Suspicious'. The table lists the following threat:

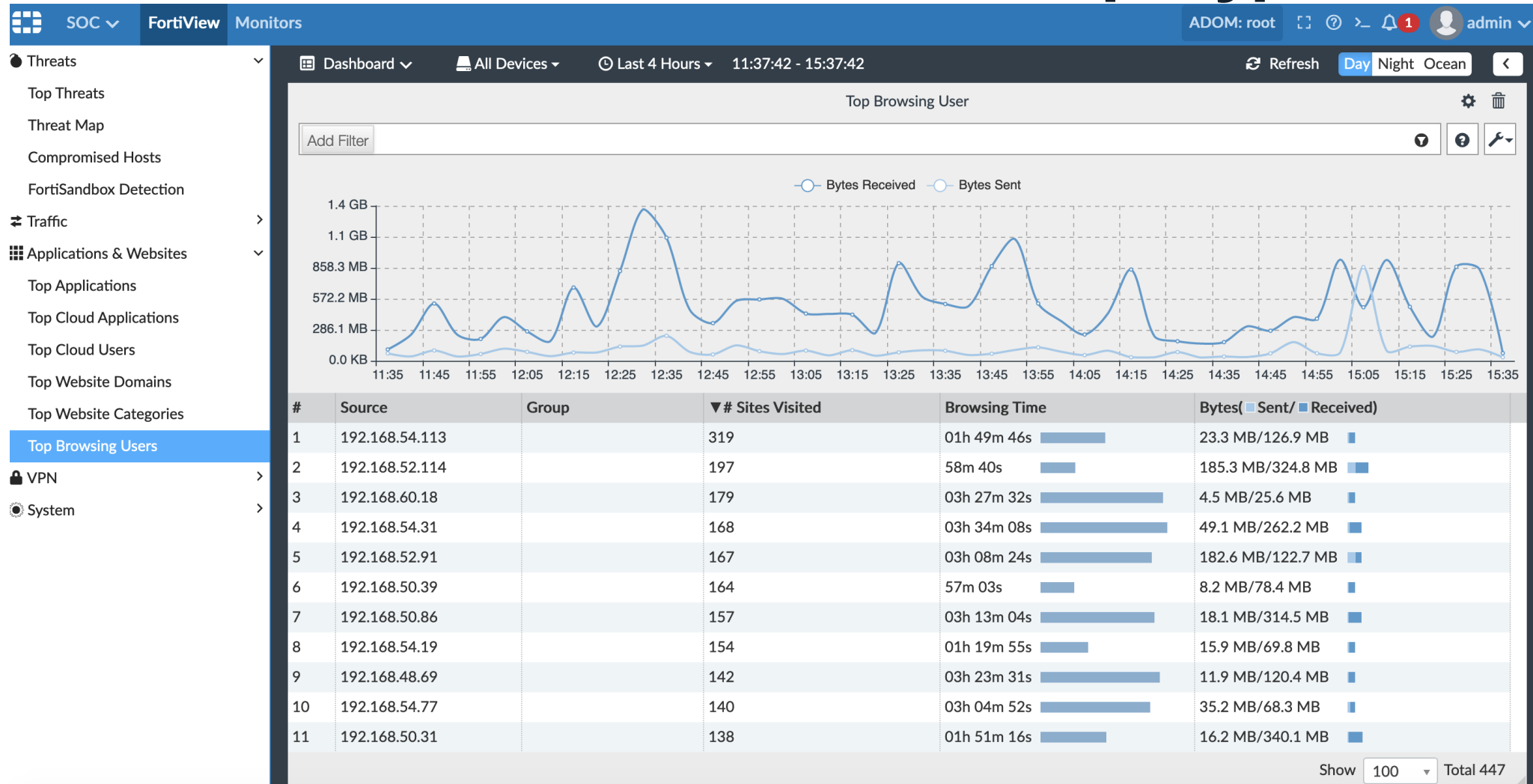
#	Detect Pattern	Threat Type	Threat Name	▲ Category	Detect Method	# of Events	Security Action	Log Type	Device Name
1	195.22.26.248	Malware	Sinkhole	Spyware and Malware	infected-ip	12	server-rst	traffic	FortiGate-300E

# Fortinet Security Day 2019: приложения (в том числе потенциально опасные)





# Fortinet Security Day 2019: статистика по пользователям и посещенным ими ресурсам





**FORTINET**®