

ОмГУ им. Ф. М. Достоевского

**Исследование
беспроводных сетей
стандарта 802.11х**

Докладчик:

Станулевич Дмитрий Антонович

Содокладчик:

Исаенко Александр Олегович

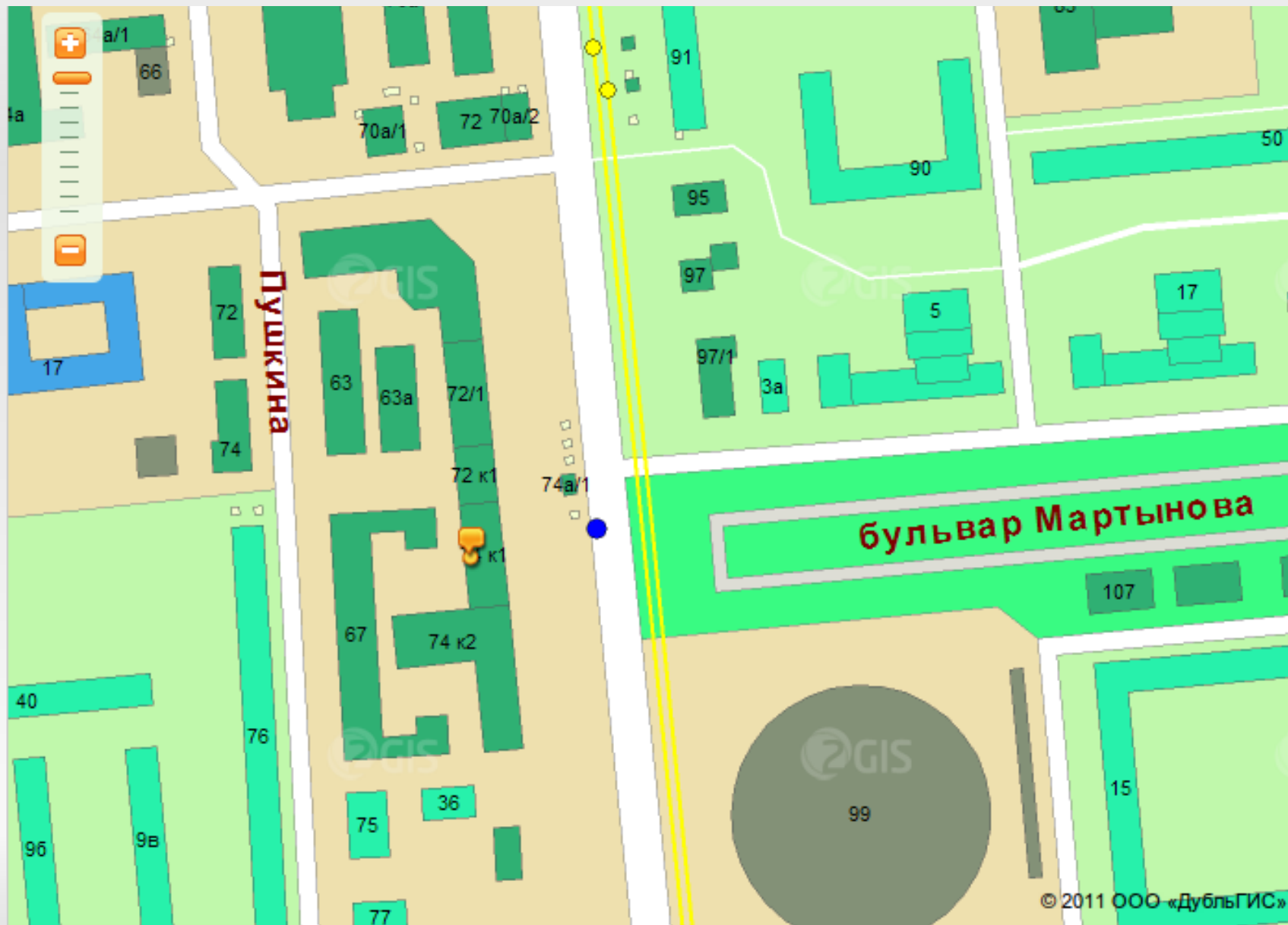
Общие сведения о стандарте

	Год принятия	Частоты	Скорость	Модуляция
a	1999	5 ГГц	54 Мбит/с	ODFM
b	1999	2,4 ГГц	11 Мбит/с	DSSS
g	2002	2,4 ГГц	54 Мбит/с	ODFM/DSSS
n	2009	2,4 ГГц 5 ГГц	4x150 Мбит/с	ODFM/DSSS

Время и место проведения

- Время проведения:
 - 17 марта 2011, 15:00-15:40
 - 24 марта 2011, 15:00-16:00
- Место проведения:
 - ул. Маршала Жукова, 74/1 — ул. Пушкина, 59
 - ул. Маршала Жукова, 74/1 — Бульвар Мартынова
 - территория бизнес-центра Маршала Жукова, 74/1

Карта



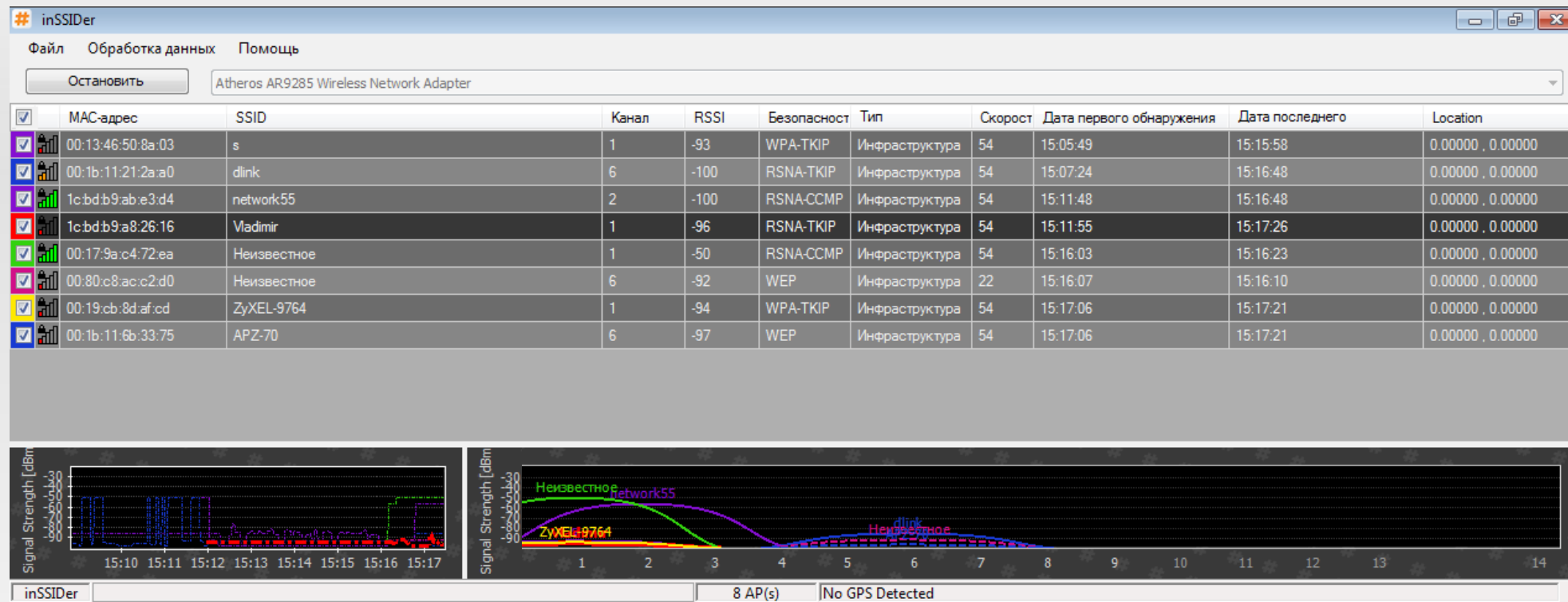
Методика исследования

- Ноутбук DNS 0121597
 - Модуль Wi-Fi Realtek RTL8191SEvB
 - Операционная система Ubuntu 10.10
 - Утилита `iwlist` из пакета `wireless-tools`
- Ноутбук Acer Aspire One
 - Модуль Wi-Fi Atheros AR5B95
 - Операционная система Linux Mint 9.0
 - Утилита `iwlist` из пакета `wireless-tools`
- Ноутбук Lenovo
 - Операционная система Microsoft Windows 7
 - Штатная утилита просмотра беспроводных сетей

Пример работы iwlist

- Cell 04 - Address: 00:14:BF:AA:86:61
- ESSID:"linksys"
- Protocol:IEEE802.11bg
- Mode:Master
- Channel:6
- Encryption key:off
- Bit Rates:54 Mb/s
- Extra: Rates (Mb/s): 1 2 5.5 6 9 11 12 18 24 36 48 54
- Quality=47/100 Signal level=-73 dBm
Noise level=-93 dBm
- Extra: Last beacon: 137ms ago

Пример работы inSSIDer



00:80:c8:ac:c2:d0	Неизвестное	6	-92	WEP	Инфраструктура	22	15:16:07
00:19:cb:8d:af:cd	ZyXEL-9764	1	-94	WPA-TKIP	Инфраструктура	54	15:17:06

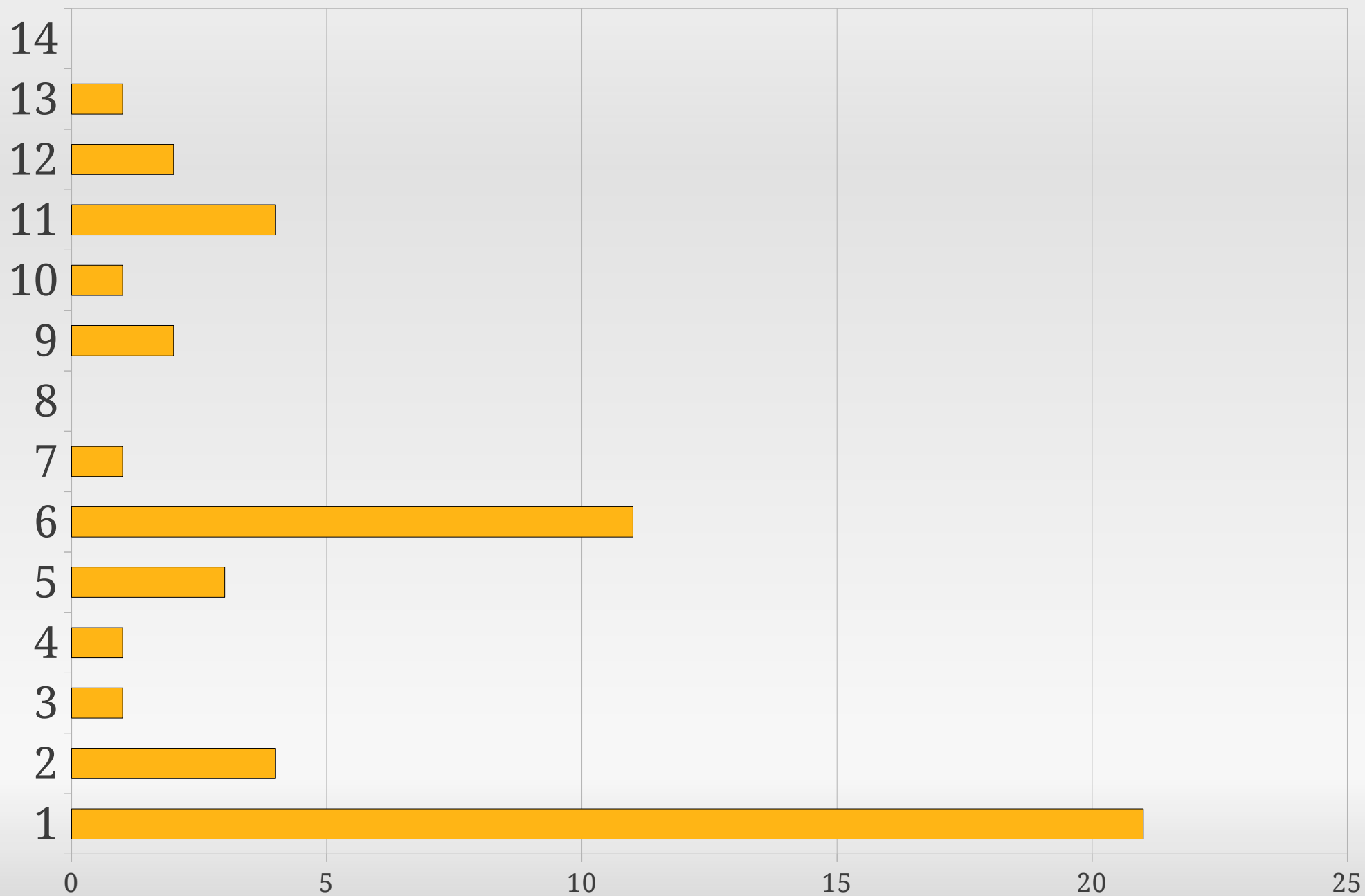
Пример работы конфигуратора Windows



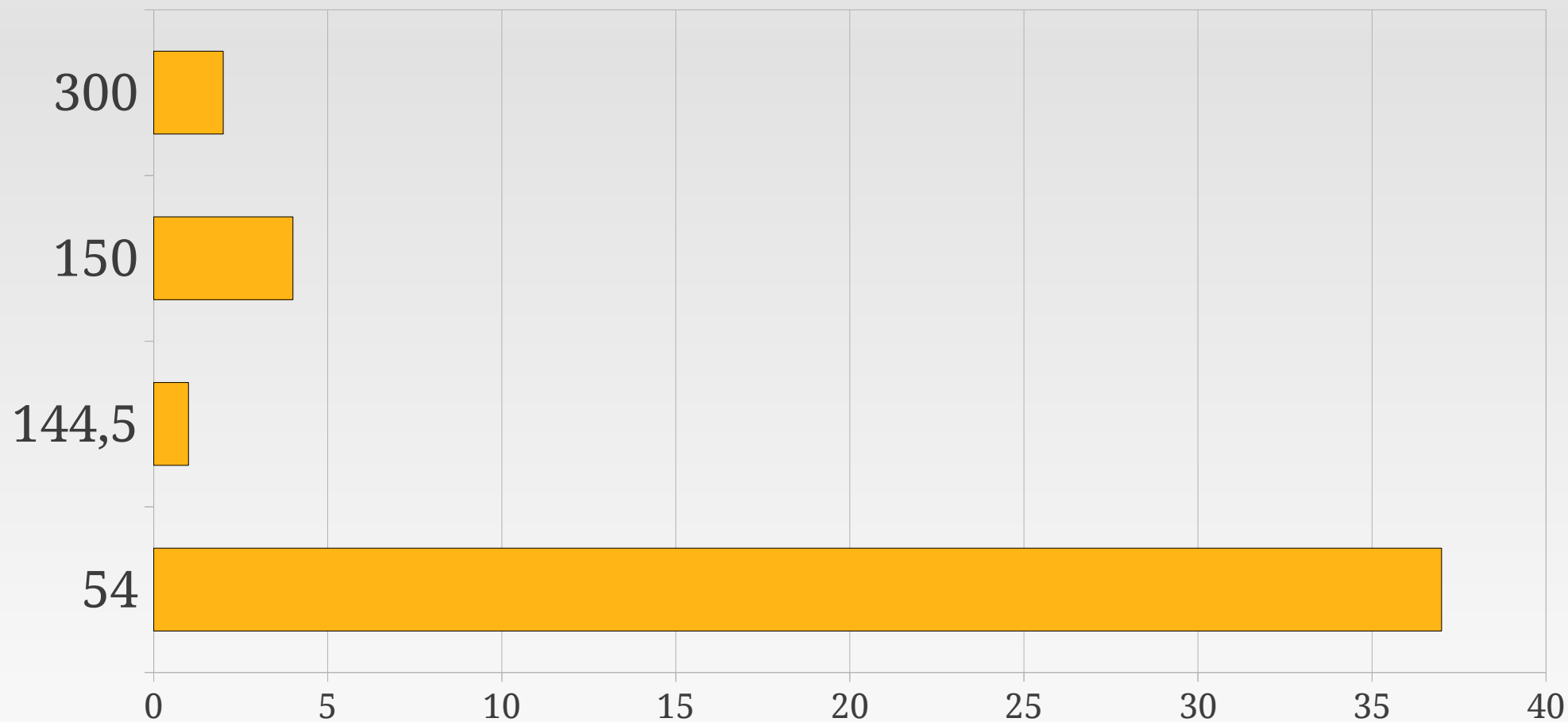
Результаты исследования

- Всего обнаружено 102 сети
- Распределение по стандартам:
 - 802.11g — 98 сетей
 - 802.11n — 14 сетей

Каналы (радиочастоты)



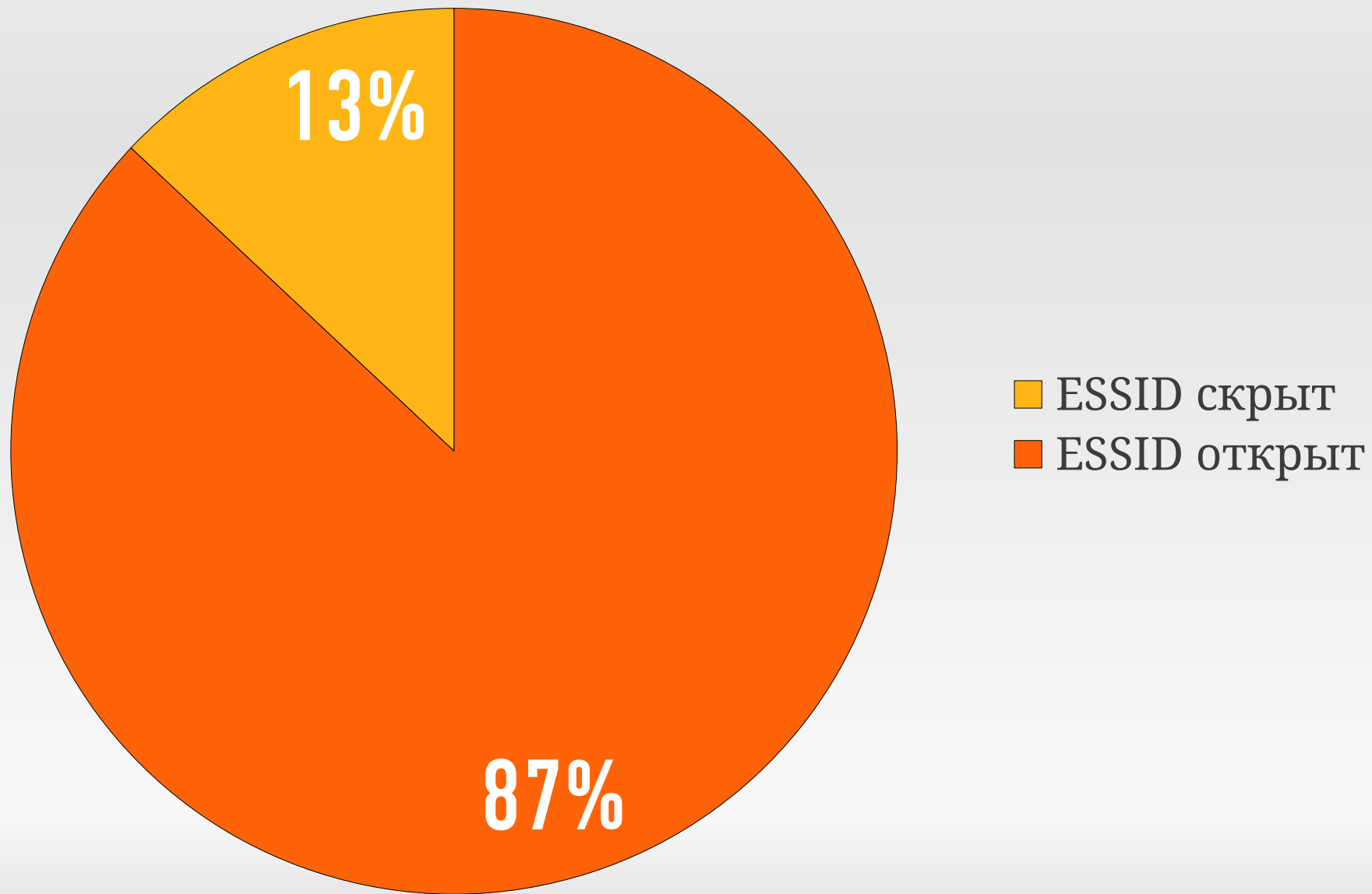
Скорость передачи данных, Мбит/с



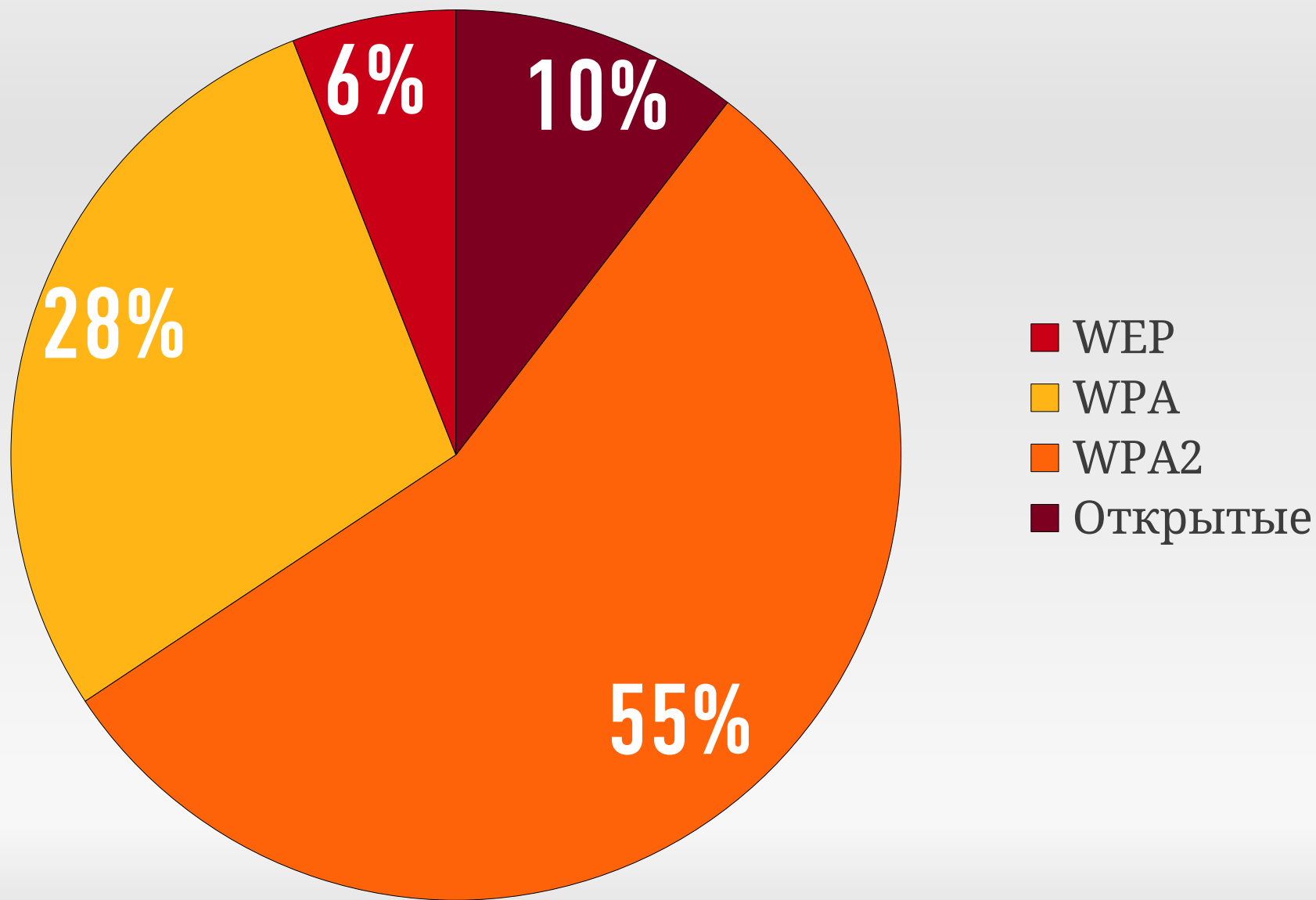
Безопасность сетей Wi-Fi

- WEP
 - алгоритм RC4 (ключ 40/104 бита)
 - уязвим к атакам на коллизию векторов инициализации и инъекции в кадры
 - устарел
- WPA
 - TKIP — Temporal Key Integrity Protocol
 - MIC — Message Integrity Code
- WPA2
 - алгоритм AES

Скрытие ESSID



Защищенность



Итог

- Достаточно высокая популярность Wi-Fi-сетей
- Высокая плотность сетей внутри и вблизи как офисных зданий, так и частных домов
- Использование современных протоколов аутентификации и шифрования (WPA, WPA2)
- Использование радиочастот «по умолчанию»
- Возрастание интереса к новому стандарту 802.11n

Спасибо за внимание!