1 Wi-Fi 7

- номинальная пропускная способность более, чем до 40 Гбит/с в одном частотном канале;
- поддержка приложений реального времени;
- 802.11be;
- 320 МГц (двухкратное увеличение ширины полосы);
- 4KQAM;
- OFDMA;
- MU-MIMO с 16 потоками (двухкратное увеличение числа пространственных потоков) 16x16;
- пропускная способность в 4.8 раз выше, чем у Wi-Fi 7;
- максимальная пропускная способность = 46 Гбит/с;
- комбинированное сочетание канальных полос, с возможностью объединения частотных блоков в несмежных участках спектра;
- SNR для 4096QAM = 40 дБ (засчёт формирования луча);
- изменение метода доступа к каналу – OFDMA;
- одновременное использование нескольких параллельных соединений на различных частотах;
- процедура оценки состояния канала будет пересмотрена;
- гибридный автоматический запрос подтверждения (HARQ);
- полный дуплекс (FD);
- неортогональный множественный доступ (NOMA);
- скоординированная работа точек доступа;
- автоматический частотный координатор (AFC);
- bands 1 – 7.25 ГГц;
- WPA3;
- в России диапазон 6 ГГц разрешён для Wi-Fi.

2 Угрозы и Риски беспроводных сетей

- подслушивание:
  - возможность анонимных атак;
  - перехват радиосигнал, расшифровка данных;
  - вблизи передатчика;
  - невозможно зарегистрировать и помешать;
  - активное подслушивание (неправильное использование ARP);
  - MITM;
  - отказ в обслуживании (DOS).
- глушение клиентской станции;
- глушение базовой станции;
- угрозы криптозащиты;
- восстановление статического ключа после захвата минимального трафика при WEP;
- БСС подвержены перехвату периода контакта;
- анонимность атак;
- физическая защита;
- в 802.11 аппаратная регистрация, а на учётная;
- целостность данных включает безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных.

3 WEP

- Wired Equivallent Privacy – секретность на уровне проводной связи;
- алгоритм RC4 – код Ривеста, симметричное потоковое шифрование;
- ключи шифрования у абонента и точки доступа идентичные;
- ядро алгоритма состоит из функции генерации ключевого потока, которая генерирует последовательность битов, которая XOR с исходным текстом;
- дешифрация состоит из регенерации этого ключевого потока и XOR с шифрограммой;
- вторая часть алгоритма – функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока;
- RC4 это класс алгоритмов, определяемых размером блока;
- достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;
- самосинхронизация для каждого сообщения (ключевое свойство);
- эффективность;
- открытость;
- обязательное использование;
- потоковое (XOR, где ключ и текст одинаковой длины) и блочное (XOR блоков текста соответствующих длине ключа) шифрование;
- метод электронной кодовой книги (ECB);
- вектор инициализации, обратная связь;
- к секретному ключу добавляется вектор инициализации (IV);
- IV длиной 24 бита, совмещается с 40 или 104 битовым ключом (64 и 128 битовые ключи);
- IV в незашифрованном виде в заголовке фрейма в радиоканале, для декодирования фрейма;
- эффетивная длина ключа – 40 или 104 бита;
- обратная связь предотвращает порождение одним и тем же исходным сообщением одного и того же шифротекста;
- обратная связь используется при блочном шифровании (CBC – цепочка шифрованных блоков);
- атаки пассивные и активные;
- уязвимость – метод планирование ключей в RC4;
- нужно усиливать ключ и делать его динамическим;
- нет MIC – контроль (проверка) целостности сообщения;
- ICV (значение проверки целостности) вычисляется с помощью CRC32, который подвержен манипуляции битами;
- Атака – повторное использование вектора инициализации (IV Replay);
- Атака – манипуляция битами (Bit-Flipping);
- поддерживает только статические ключи.

4 WPA