ДИТ

РАБОЧАЯ ТЕТРАДЬ ПО БЕЗОПАСНОСТИ ДОМАШНЕЙ WI-FI СЕТИ

Содержание

1. Угрозы безопасности домашней Wi-Fi сети

Wi-Fi сеть гораздо уязвимее проводной сети, так как доступ к ней может получить любое устройство в радиусе ее действия.

Установка сложного и уникального пароля на Wi-Fi — это далеко не все, что нужно сделать для безопасности.

Защищенная домашняя сеть – это важный аспект интернет-безопасности.

Последствия взлома домашней сети Wi-Fi:

- Риск заражения рабочего устройства при работе из домашней Wi-Fi сети;
- Заражение домашней сети вредоносными программами;
- Кража личной информации;
- Перехват учетных данных;
- Атака на владельца домашней Wi-Fi сети;
- Компрометация личной жизни через сеть интернета вещей[1];
- Несанкционированный доступ к домашней Wi-Fi сети под видом «хозяина»;
- Совершение противоправных действий от имени «хозяина» Wi-Fi сети.

Основные причины взлома домашней Wi-Fi сети:

- Установлен слабый и не уникальный пароль;
- Не изменены названия марки и модели роутера;
- Установлены устаревшие алгоритмы шифрования сети WPA или WEP, которые уязвимы для атак методом перебора пароля или отключены по умолчанию;
- Установлено избыточное покрытие Wi-Fi сети, которое выходит за пределы квартиры:
  - роутер размещен вблизи оконного проема (на рисунке 1 схематично изображен сигнал от Wi-Fi роутера, который выходит на улицу или доходит до соседнего здания через оконный проем);

[1] Сеть интернета вещей то система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека. ГОСТР ИСО/МЭК 29161— 2019 «Информационные технологии. Структура данных. Уникальная идентификация для интернета вещей».

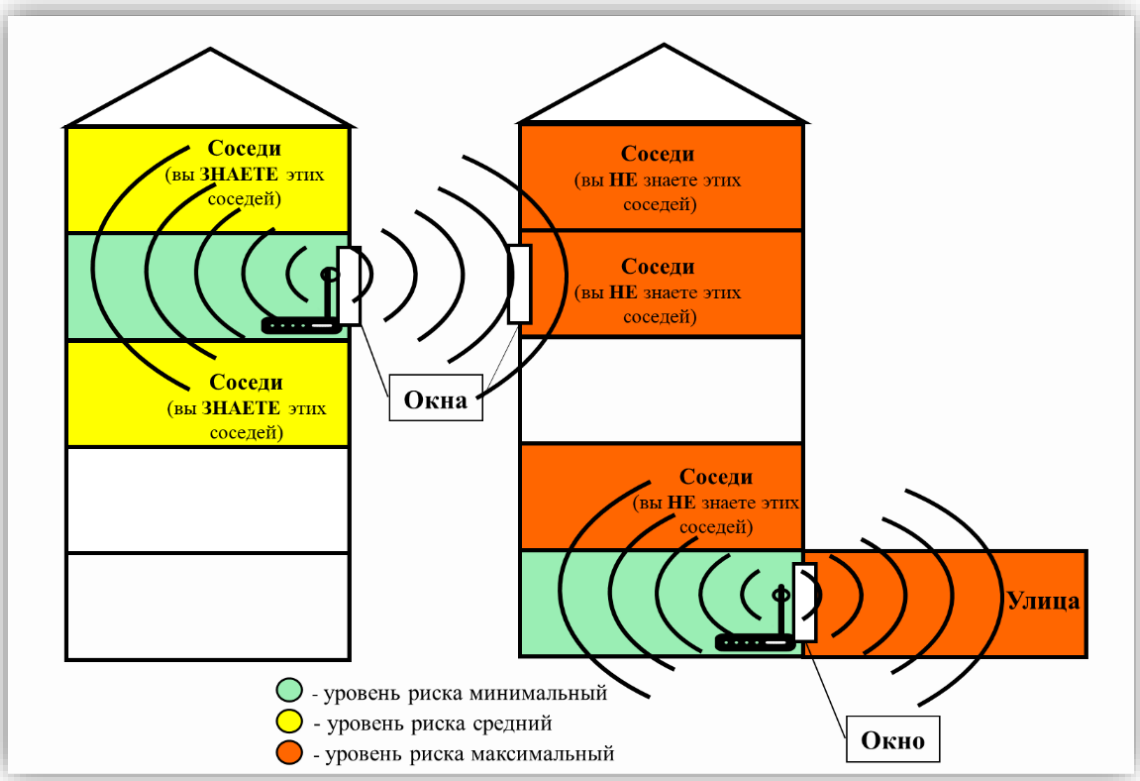


Рис. 1. Схематичное изображение покрытия сигнала от Wi-Fi роутера, который размещен вблизи окна

– роутер размещен вблизи входной двери (на рисунке 2 схематично изображен сигнал, который доходит до соседних квартир, помещения подъезда и других общественных мест);

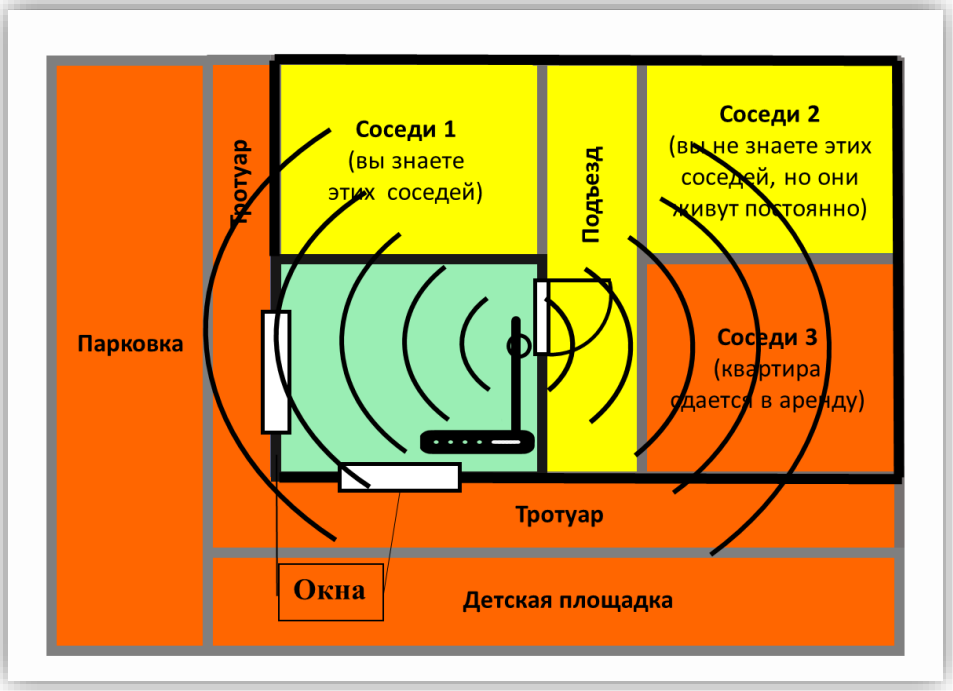


Рис. 2. Схематичное изображение покрытия сигнала от Wi-Fi роутера, который размещен вблизи входной двери или оконного проема

– антенны на Wi-Fi роутере некорректно направлены или высоко размещен высоко под потолком или на полу (на рисунке 3 схематично изображено направление распространения сигнала от Wi-Fi роутера в зависимости от положения его антенн).

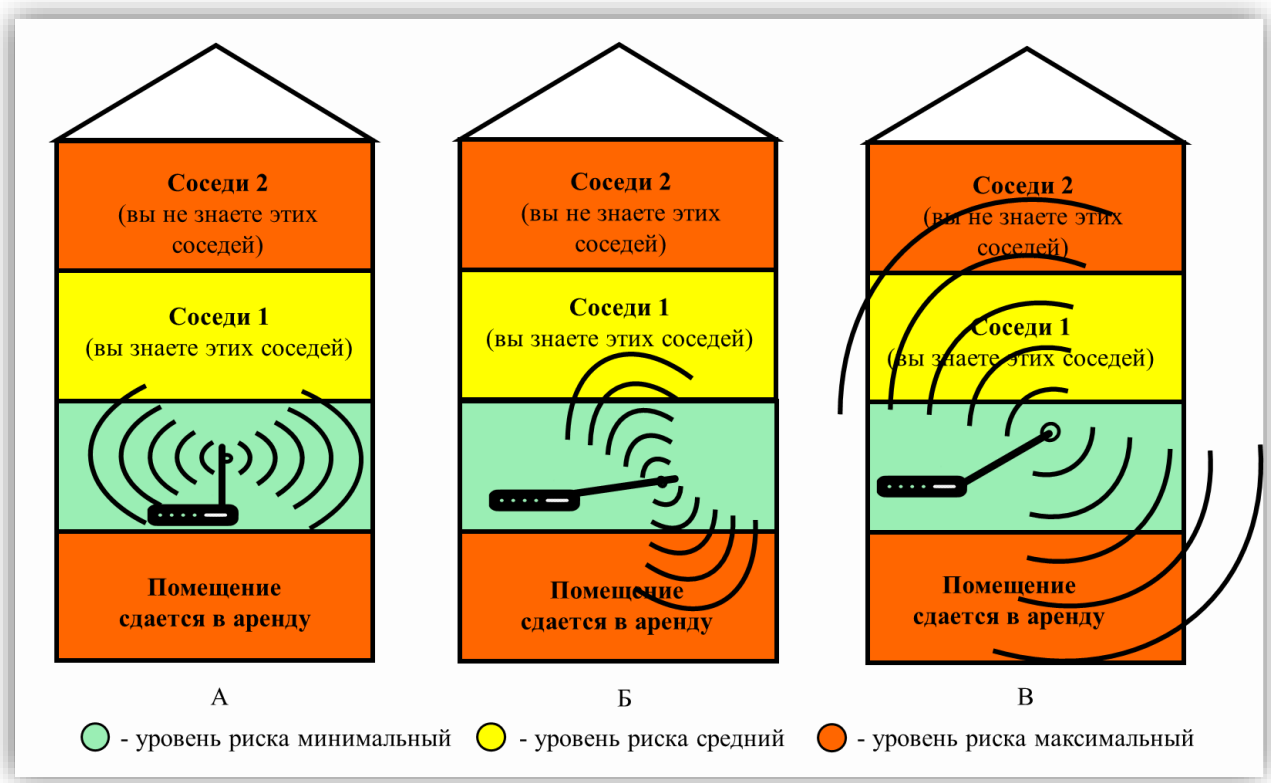


Рис. 3. Условное отображение распределения сигнала от Wi-Fi роутера в зависимости от направления размещенных на нем антенн.
(А – антенна направлена вверх, сигнал распределяется горизонтально и покрывает всю вашу квартиру.
Б – антенна направлена под углом или горизонтально, ее сигнал будет распространяться в вертикальной плоскости, соответственно в вашей квартире будет более слабая зона покрытия Wi-Fi сигналом, а максимальный уровень сигнала уйдет к соседям сверху и(или) снизу.
В – антенна направлена под углом или горизонтально и увеличена мощность сигнала, в вашей квартире улучшился уровень сигнала, но он стал мощнее и по вертикальной плоскости, соответственно увеличивается дальность сигнала за пределами вашей квартиры.)

На рисунке 4 схематично изображено направление распределения сигнала от Wi-Fi роутера по горизонтальной и вертикальным осям.

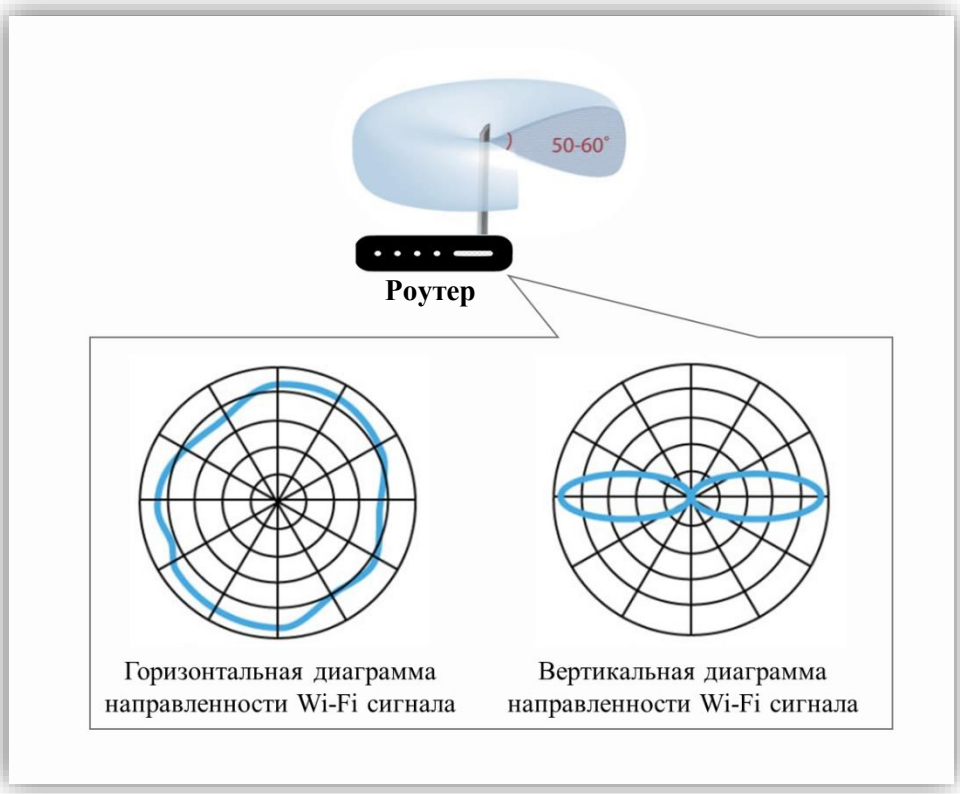


Рис.4. Схематичное изображение направления распределения сигнала от Wi-Fi роутера по горизонтальной и вертикальным осям.

- Установлено устаревшее программное обеспечение Wi-Fi роутера, а следовательно, он уязвим для внешнего воздействия;
- Не настроены отдельные домашний и гостевой Wi-Fi;
- Не настроен запрет на удаленный доступ к настройкам роутера через интернет;
- Несоблюдение правил безопасности сети интернета вещей.

Признаки взлома Wi-Fi сети:

- Регулярное снижение скорости доступа в Интернет;
- Появление неизвестных подключенных устройств в личном кабинете настроек роутера;
- Появление системных предупреждений о подделке пользовательских сертификатов безопасности Wi-Fi.

2. Основные действия по защите домашней Wi-Fi сети

Шаг 1. Изменение названия домашней Wi-Fi сети

Первым шагом в обеспечении безопасности домашней сети является изменение ее имени.

Если злоумышленники узнают производителя вашего роутера, они смогут выяснить уязвимости модели и способы их эксплуатации.

Отличное от используемого по умолчанию имя роутера может отпугнуть злоумышленников, поскольку показывает, что роутер управляется более серьезно, чем если бы для него использовалось заданное по умолчанию имя.

В настройках роутера измените идентификатор SSID так, чтобы в нем не была указана марка или модель роутера (рисунок 5).

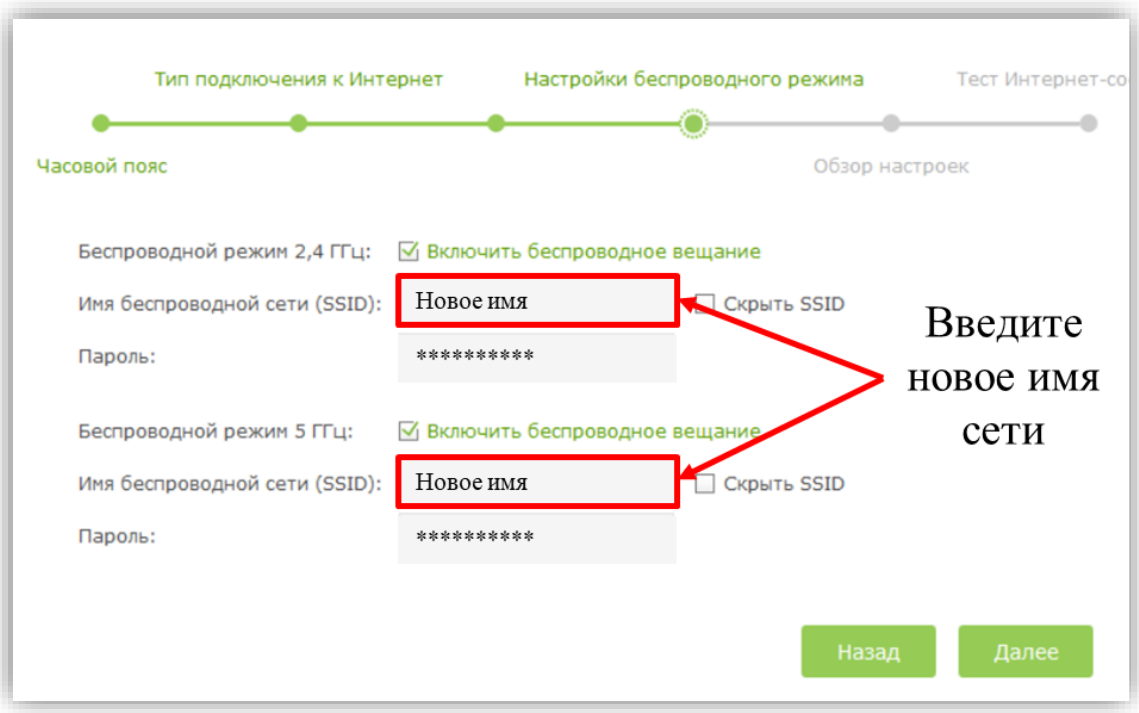


Рис. 5. Изменение названия домашней Wi-Fi сети

Шаг 2. Изменение пароля домашней Wi-Fi сети

Беспроводные роутеры обычно поставляются с предварительно установленными паролями.

Злоумышленники могут подбирать такие пароли, особенно если известен производитель роутера, поэтому изменение пароля поможет обеспечить безопасность домашнего роутера.

Надежный пароль состоит минимум из 8-10 символов, а в идеале – больше, и содержит сочетание заглавных и строчных букв, цифр и специальных символов.

Для безопасности домашней сети рекомендуется регулярно менять пароль, приблизительно каждые шесть месяцев (рисунок 6).

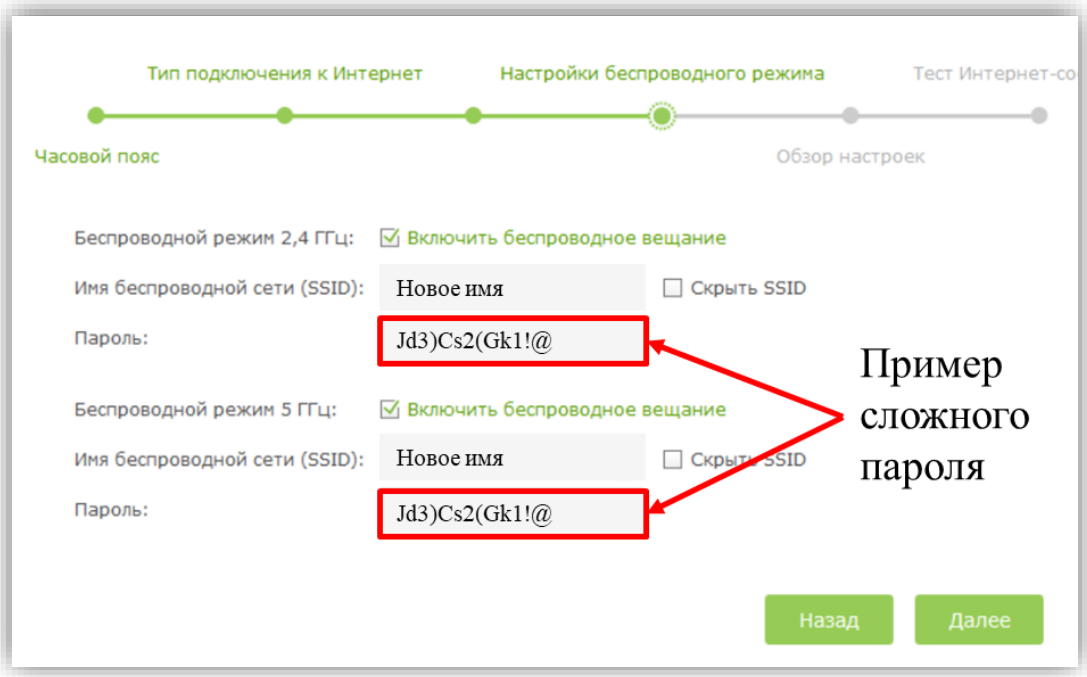


Рис. 6. Изменение пароля домашней Wi-Fi сети

Шаг 3. Настройка шифрования домашней Wi-Fi сети

Шифрование – важный аспект при настройке Wi-Fi сети.

Большинство беспроводных роутеров имеют функцию шифрования, которая часто отключена по умолчанию.

Включение шифрования для домашнего роутера поможет обеспечить защиту сети.

Протоколы WPA2 и WPA3 – оптимальные варианты для защиты Wi-Fi сети, они новее и являются более надежными.

Предыдущие версии WPA и WEP уязвимы для атак методом подбора пароля (рисунок 7).

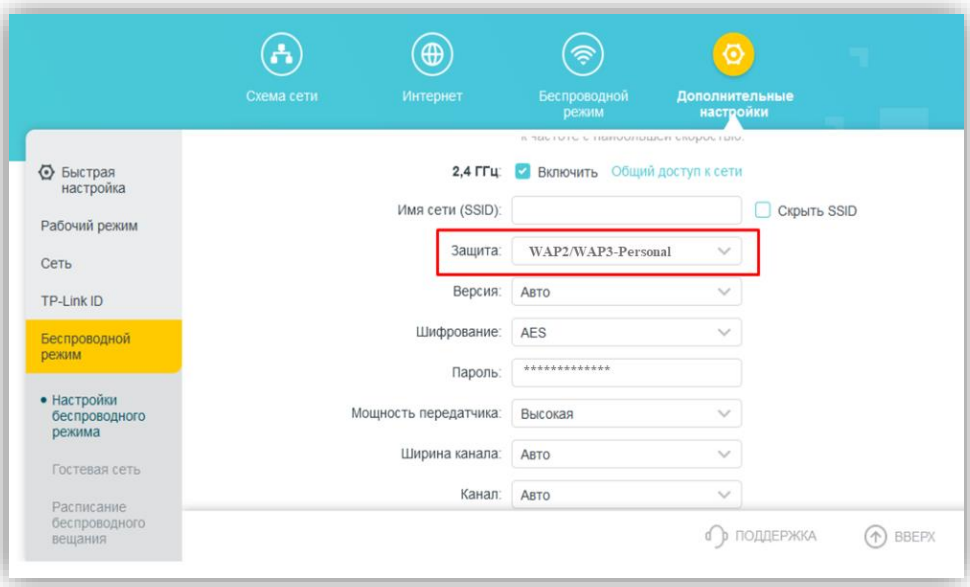


Рис. 7. Настройка шифрования домашней Wi-Fi сети

Шаг 4. Оптимальное размещение Wi-Fi роутера

По возможности размещайте роутер в центре дома или квартиры. Это не только поможет сделать доступ к сети более равномерным, но снизит уровень доступности сети для злоумышленников.

По возможности рекомендуется размещать роутеры подальше от окон, наружных дверей и стен смежных с коридорами, соседними квартирами и лестничными клетками.

Роутеры распространяют излучение сверху и снизу, а также в горизонтальном направлении.

Если у вас двухэтажный дом, размещение роутера на верхней полке нижнего этажа обеспечит покрытие как верхнего, так и нижнего этажа.

Шаг. 5. Настройка оптимальной мощности сигнала Wi-Fi сети

На экране смартфона вы можете видеть все доступные вам сети и их уровень Wi-Fi сигнала, как свой, так и соседей (рисунок 8).

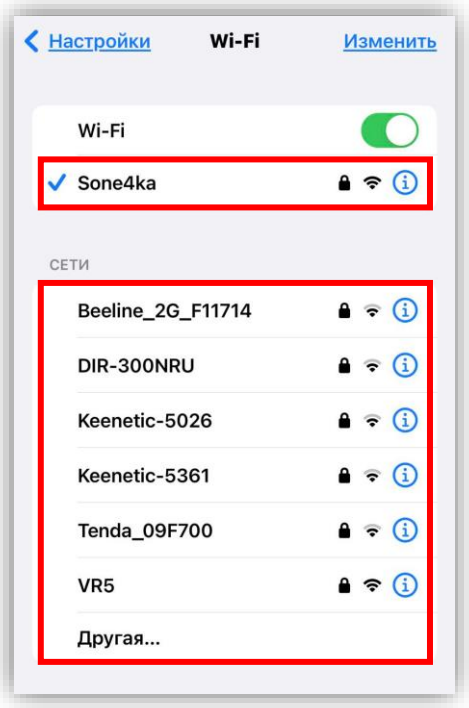


Рис. 8. Скриншот экрана смартфона, в котором показаны доступные Wi-Fi сети и их уровень сигнала

Настроить мощность Wi-Fi роутера, часто бывает необходимо при настройке беспроводной сети.

Это необходимо, чтобы сигнал Wi-Fi не ловил в коридоре, в соседней квартире или на лестничной клетке, и тем самым не провоцировал злоумышленников на попытки взлома вашей Wi-Fi сети (рисунок 9).

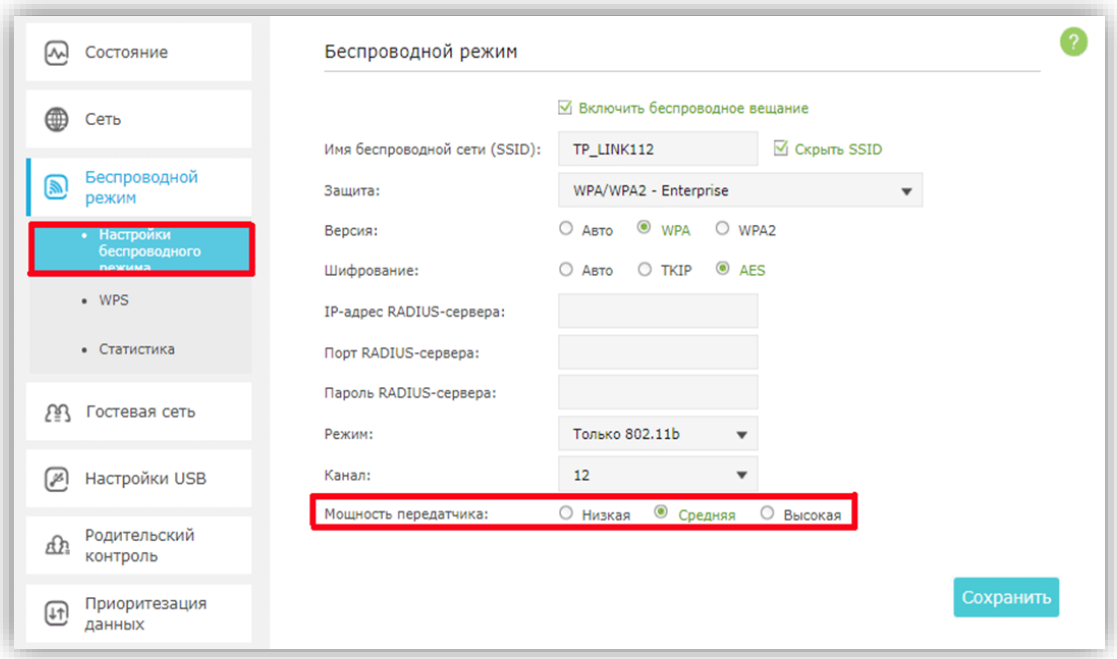


Рис. 9. Настройка мощности сигнала Wi-Fi сети

Алгоритм определения оптимальной мощности сигнала Wi-Fi сети приведен на рисунке 10.

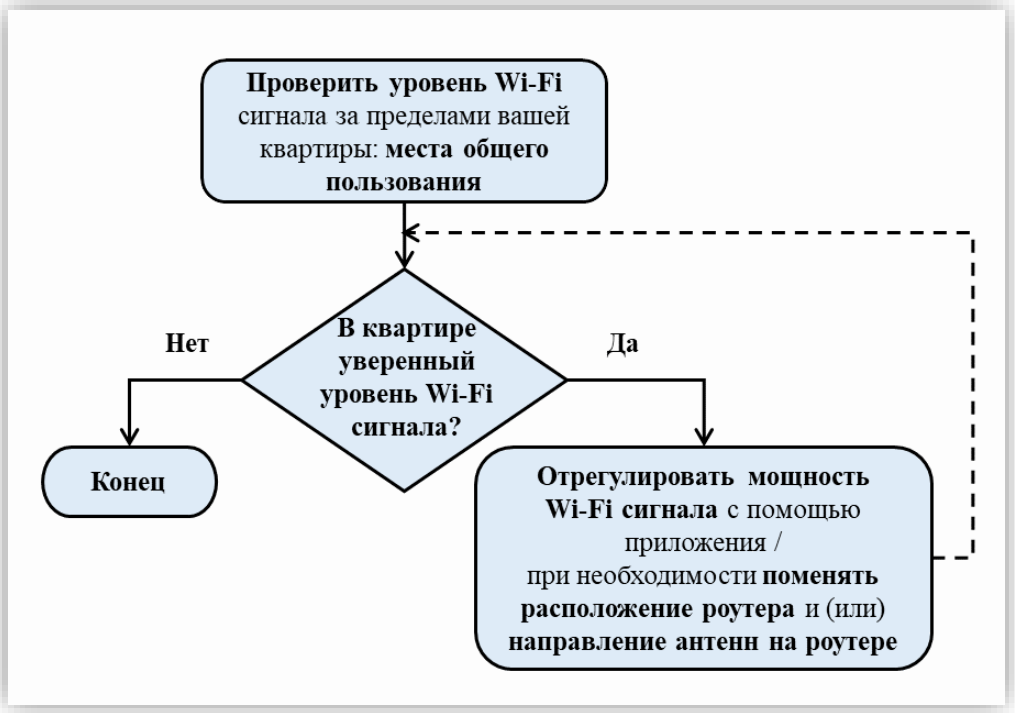


Рис. 10. Алгоритм определения максимальной мощности Wi-Fi сигнала

Шаг 6. Обновление программного обеспечения Wi-Fi роутера

Для обеспечения высокого уровня безопасности рекомендуется регулярно обновлять программное обеспечение роутера.

Некоторые роутеры позволяют проверять, доступны ли обновления прошивки, через интерфейс управления, другие предлагают автоматические обновления (рисунок 11).

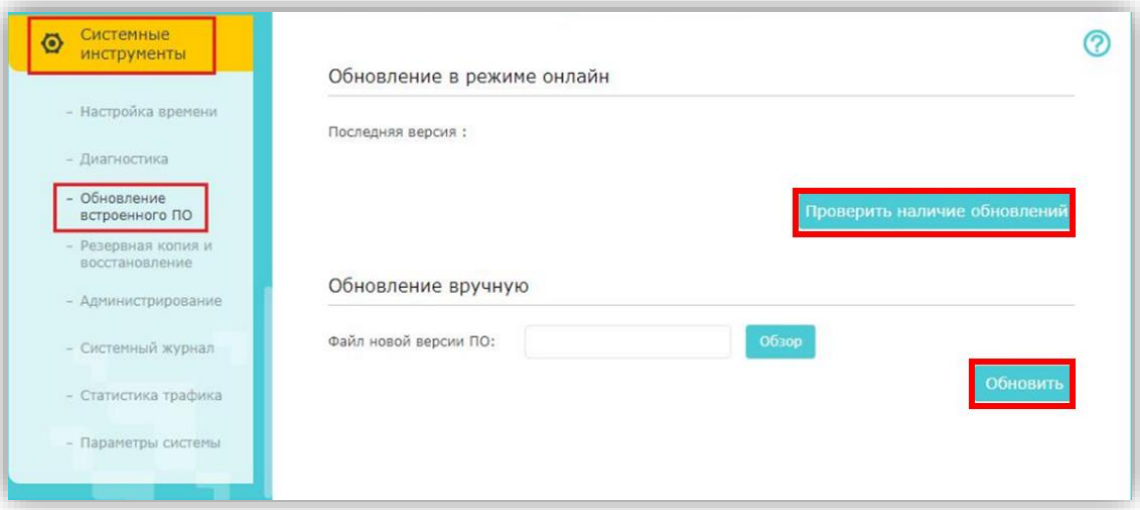


Рис. 11. Обновление программного обеспечения Wi-Fi роутера

Шаг 7. Настройка гостевой Wi-Fi сети

Если позволяет роутер, рекомендуется создать гостевую беспроводную сеть, также использующую протоколы WPA2 или WPA3 и защищенную надежным паролем.

Используйте эту гостевую сеть для друзей и близких.

Друзья и родственники, не будут взламывать вашу сеть, однако до подключения к вашей сети их устройства могли быть скомпрометированы или заражены вредоносными программами.

Использование гостевой сети помогает повысить безопасность домашней сети (рисунок 12).

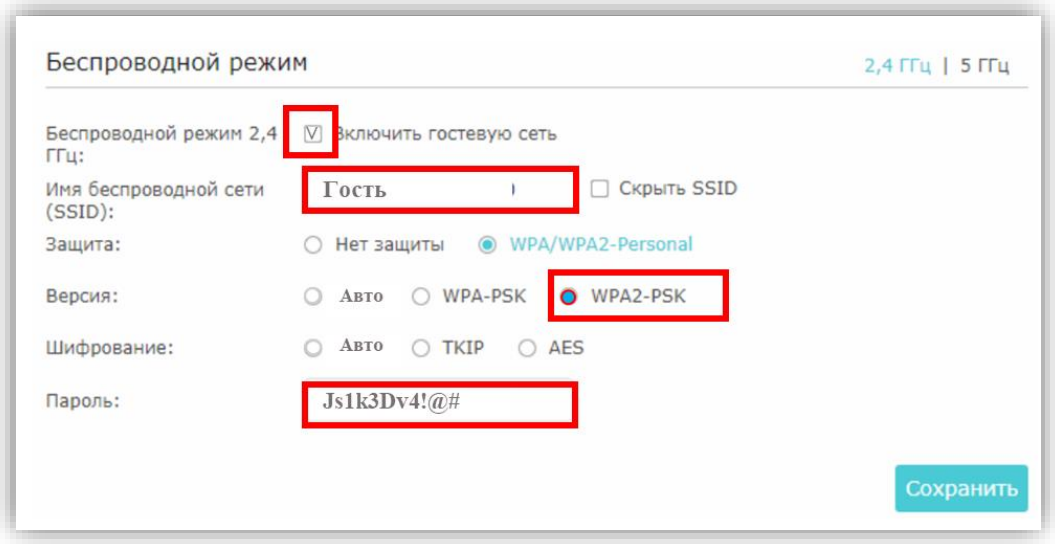


Рис. 12. Настройка гостевой Wi-Fi сети

Шаг 8. Настройка запрета на удаленный доступ к настройкам Wi-Fi роутера через интернет

Многие роутеры оснащены функциями, упрощающими удаленный доступ извне домашней сети.

Однако, если вам не нужен доступ к роутеру на уровне администратора, можно спокойно отключить эти функции на панели настроек роутера. При этом снижается риск удаленного доступа и взлома роутера со стороны злоумышленников.

Для отключения этой функции в веб-интерфейсе роутера найдите «Удаленный доступ», «Удаленное администрирование» или «Удаленное управление», и проверьте, отключена ли эта функция. На многих роутерах она отключена по умолчанию.

Если выяснится, что для отдельных приложений и устройств в вашей сети требуется удаленный доступ, эту функцию всегда можно включить повторно.

Шаг 9. Просмотр всех подключенных к вашей Wi-Fi сети устройств

В Базовых настройках домашнего Wi-Fi можно посмотреть все подключенные устройства, как к локальной сети, так и подключенные к гостевой сети и при необходимости отключить (рисунок 13).

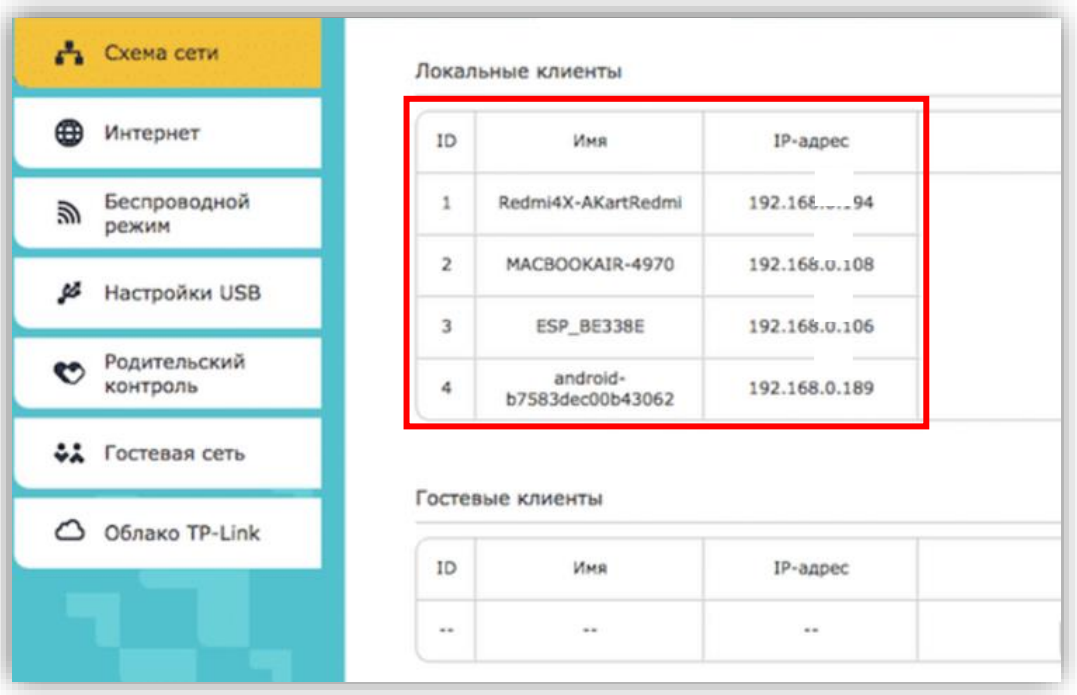


Рис. 13. Просмотр всех подключенных к вашей Wi-Fi сети устройств

Шаг 10. Настройка безопасности интернета вещей

К интернету вещей относят:

- умные фитнес-трекеры, часы, телевизоры,
- гарнитуры виртуальной реальности.
- умные бытовые приборы (холодильники, пылесосы, чайники),
- музыкальные системы,
- интеллектуальные системы освещения,
- жалюзи с электрическим приводом,
- автоматические окна и двери,
- интеллектуальные счетчики коммунальных услуг
- умные автомобили и т.д.

Безопасность Интернета вещей подразумевает защиту Интернет-устройств и сетей, к которым они подключены, от онлайн-угроз и взломов.

Нарушения безопасности систем интернета вещей могут иметь катастрофические последствия. Взлом устройств в «умных домах» может позволить киберпреступникам контролировать сам дом, в котором живут люди.

Рекомендации по обеспечению безопасности Интернета вещей:

- Выясните, какие устройства интернета вещей есть в вашей домашней сети.
- Обеспечьте безопасность вашей Wi-Fi сети.
- Измените установленные по умолчанию пароли на устройствах интернета вещей.

- Регулярно обновляйте программное обеспечение устройств интернета вещей.
- Проверьте политику конфиденциальности устройств интернета вещей.
- Отслеживайте доступные функции устройств и отключайте неиспользуемые.
- По возможности включите многофакторную аутентификацию интернета вещей.
- Соблюдайте осторожность при использовании публичных сетей Wi-Fi (используйте VPN).

Шаг 11. Отключение Wi-Fi роутера, когда никого нет дома

Один из самых простых способов защитить домашнюю сеть – отключить Wi-Fi роутер, когда никого нет дома.

Это снижает вероятность проникновения злоумышленников в вашу домашнюю сеть.

Помимо снижения рисков безопасности, отключение роутера от сети на период вашего отсутствия также предотвращает его повреждение из-за скачков напряжения.

3. Задания для самопроверки

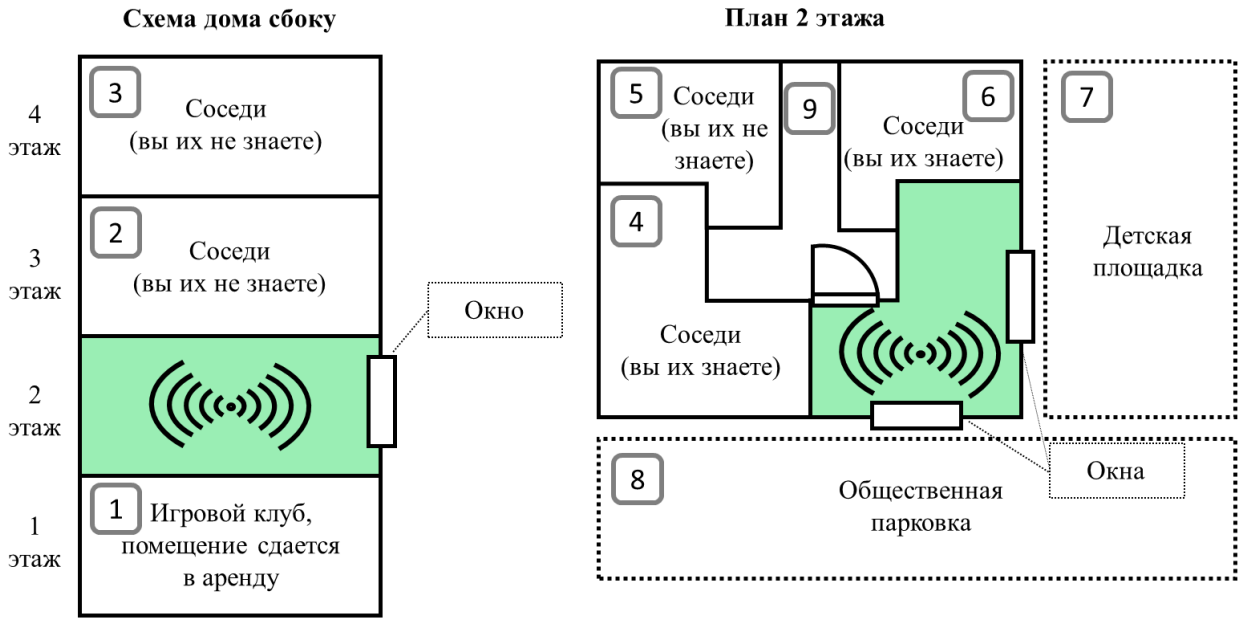
1. В вашей квартире установлен Wi-Fi роутер, как проверить безопасность вашей домашней сети? Отметьте правильные ответы.

- [ ] Проверить в настройках роутера установленную мощность Wi-Fi сигнала
- [ ] Никак
- [ ] Проверить есть ли обновления для вашего роутера
- [ ] Посмотреть как называется ваша Wi-Fi сеть
- [ ] Оценить надежность пароля от Wi-Fi сети
- [ ] Проверить все подключенные устройства к вашей Wi-Fi сети
- [ ] Проверить включенный протокол шифрования
- [ ] Выйти на площадку возле квартиры, подняться на этаж выше или спуститься ниже, выйти на улицу рядом с вашим домом и проверить уровень вашего Wi-Fi сигнала

2. Вы обнаружили, что мощность Wi-Fi сигнала в вашей квартире очень высокая и сигнал выходит за пределы вашей квартиры. Какие шаги вы предпримите?

- [ ] Уменьшу в настройках роутера установленную мощность Wi-Fi сигнала и проверю уровень сигнала в квартире и за ее пределами
- [ ] Скорректирую размещение Wi-Fi роутера (поставлю примерно по центру квартиры, вдали от окон и входной двери)
- [ ] Отрегулирую направление антенн на Wi-Fi роутере таким образом, чтобы уровень сигнала не выходил за пределы квартиры
- [ ] Ничего не буду делать

3. Вы недавно переехали в квартиру на 2 этаже в многоэтажном доме. Посмотрите на рисунок, какие номера квартир или общественных мест будут иметь максимальный уровень риска для вашей квартиры с точки зрения угроз безопасности при размещении Wi-Fi роутера.



1	2	3	4	5	6	7	8	9
☐	☐	☐	☐	☐	☐	☐	☐	☐