

А.А. Гумерова, студент
Р.Р. Шарипов, кандидат технических наук, доцент
кафедра «Систем Информационной Безопасности»
«Казанский национальный исследовательский технический университет им.
А.Н.Туполева – КАИ» (КНИТУ-КАИ),

A.A. Gumerova, student
R.R. Sharipov, PhD in Engineering, Associate Professor
Department of Information Security Systems
Kazan National Research Technical University named after A.N.Tupolev

Моделирование защищённых беспроводных сетей Wi-Fi

Simulation of secure Wi-Fi wireless networks

В данной статье рассматриваются современные подходы к моделированию защищённых беспроводных сетей Wi-Fi, с акцентом на методы обеспечения безопасности передачи данных и защиты от несанкционированного доступа. В работе представлены результаты моделирования различных сценариев использования Wi-Fi сетей, что позволяет оценить эффективность предложенных решений, также особое внимание уделяется внедрению современных протоколов шифрования и аутентификации.

This article discusses modern approaches to modeling secure wireless Wi-Fi networks, with an emphasis on methods for ensuring data transmission security and protection against unauthorized access. The paper presents the results of modeling various scenarios for using Wi-Fi networks, which makes it possible to evaluate the effectiveness of the proposed solutions, and special attention is paid to the implementation of modern encryption and authentication protocols.

Ключевые слова: беспроводные сети, Wi-Fi, моделирование, безопасность, шифрование, аутентификация, уязвимости, защита данных, сетевой трафик.

Keywords: wireless networks, Wi-Fi, modeling, security, encryption, authentication, vulnerabilities, data protection, network traffic.

Wi-Fi (Wireless Fidelity) — это технология беспроводной связи, основанная на стандартах IEEE 802.11 [1-6]. С момента своего появления в 1997 году Wi-Fi прошёл несколько этапов развития, включая стандарты 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac и 802.11ax. Каждый из этих стандартов предлагает различные скорости передачи данных, диапазоны частот и возможности подключения.

802.11b: Работает на частоте 2.4 ГГц и обеспечивает скорость до 11 Мбит/с.

802.11g: Также использует 2.4 ГГц, но поддерживает скорость до 54 Мбит/с.

802.11n: Работает на 2.4 и 5 ГГц, обеспечивая скорость до 600 Мбит/с благодаря технологии MIMO (Multiple Input Multiple Output).

802.11ac: Использует только 5 ГГц и поддерживает скорости до 1.3 Гбит/с.

802.11ax: Новый стандарт, который улучшает производительность в многопользовательских средах и обеспечивает более высокую скорость передачи данных.

Беспроводные сети Wi-Fi, основанные на стандартах IEEE 802.11, обеспечивают высокоскоростную передачу данных без проводов, но обладают рядом уязвимостей, таких как ограниченная зона покрытия, подверженность помехам и риски кибербезопасности, включая перехват трафика. Для защиты данных используются протоколы WEP, WPA и WPA2/WPA3,

причём WEP, использующий слабое RC4-шифрование, считается устаревшим и ненадёжным, тогда как WPA2 с AES-шифрованием обеспечивает высокий уровень безопасности [7-9].

Рассмотрим вариант моделирования в среде эмуляции Cisco Packet Tracer, который позволяет настроить параметры защиты, включая выбор режима безопасности (WEP, WPA, WPA2), тип шифрования (TKIP, AES) и сложные пароли, что подтверждает необходимость использования современных протоколов для минимизации рисков взлома. В данной среде проектирования можно создать виртуальную домашнюю сеть с Wi-Fi-роутером, включающую маршрутизатор провайдера и клиентские устройства, например, такие как ноутбук и персональный компьютер (рис.1).

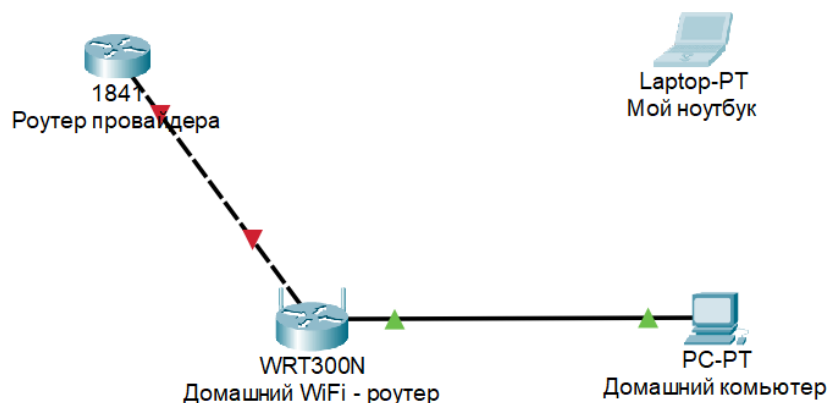


Рис. 1 – Сеть с WiFi-устройствами

После настройки параметров домашней сети, можно будет настроить различные протоколы защиты беспроводного соединения.

Рассмотрим настройку протокола защищённой передачи – WEP. Для этого на домашнем роутере войдите в раздел GUI – Wireless – Wireless Security. Выберите протокол WEP и задайте статический ключ: 1234567890, затем сохраните настройки, нажав внизу кнопку сохранения.

После этого незащищённое беспроводное соединение между точкой и ноутбуком разрывается. Это связано с тем, что зашифрованный трафик не принимается ноутбуком, и точка доступа не видит ноутбук. Далее, настройте протокол WEP и на ноутбуке и подключите его к точке доступа. Для этого зайдите на рабочий стол ноутбука и перейдите в приложение беспроводной сетевой карты: Desktop – PC Wireless, затем в раздел Connect (Рис.2).

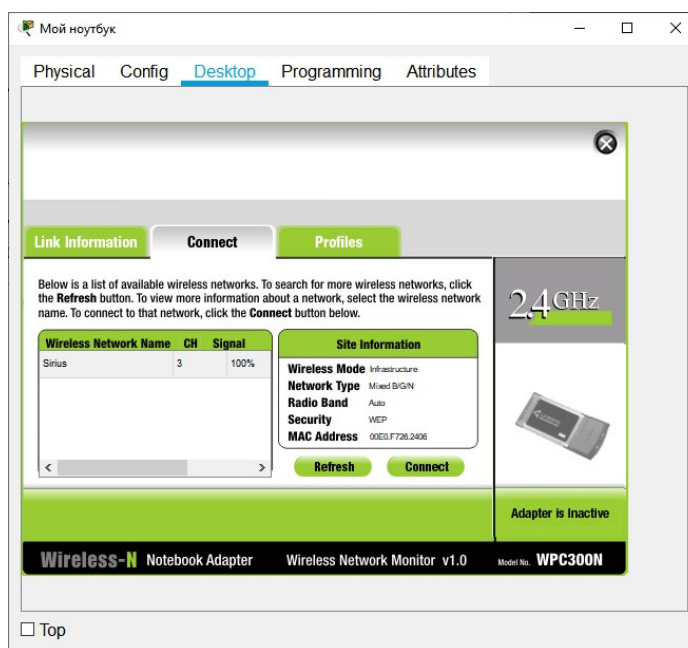


Рис. 2 – Приложение беспроводного адаптера

Обратите внимание, приложение нашло точку доступа – Sirius на 3м канале. Далее, подключитесь к этой точке доступа (Connect) и перейдите в меню настройки соединения (Рис.3).



Рис. 3 – Настройка подключения WEP

Выберите протокол подключения WEP и введите WEP-ключ точки доступа: 1234567890. Обратите внимание что ключи должны быть идентичны на устройства. После этого выйдите из приложения и посмотрите статус соединения (Рис.4). При всех настройках, указанных выше не забывайте сохранять изменения.

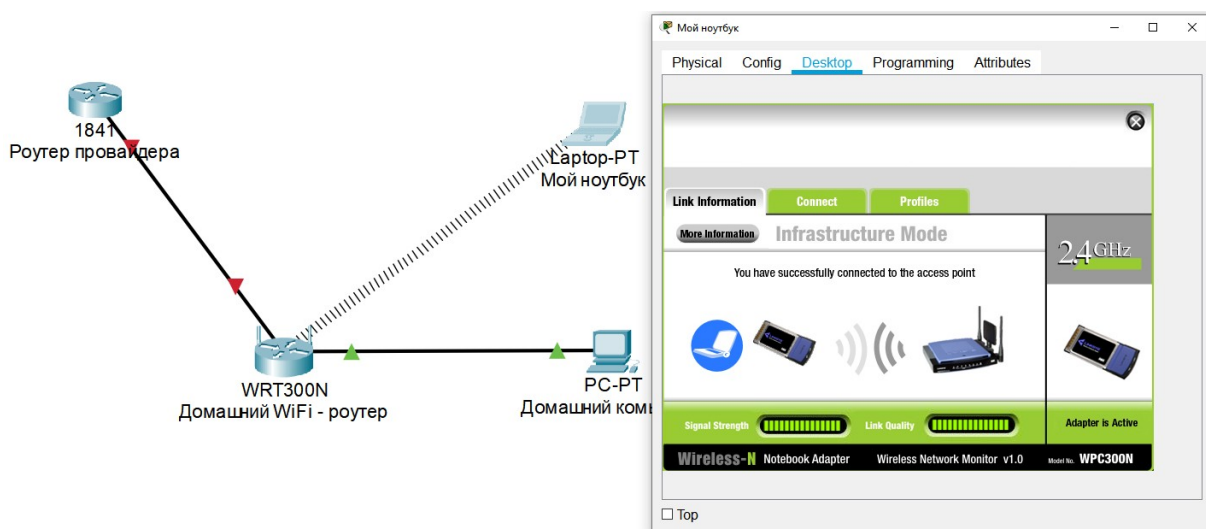


Рис. 4 – Установка соединения по протоколу WEP и статус сети

Следующим этапом будет настройка протокола безопасности WPA между WiFi-точкой и ноутбуком. Как и в предыдущем разделе, сначала необходимо настроить точку доступа и задать пароль безопасности. Для этого на точке доступа перейдите в раздел GUI – Wireless – Wireless Security. Выберите режим персональный WPA (WPA Personal) и метод шифрования AES, затем

задайте секретную фразу: 1234567890 и не забудьте сохранить изменения (Рис.5). Далее, перейдите на рабочий стол ноутбука, в приложение беспроводной сетевой карты: Desktop – PC Wireless, в раздел Connect [10].

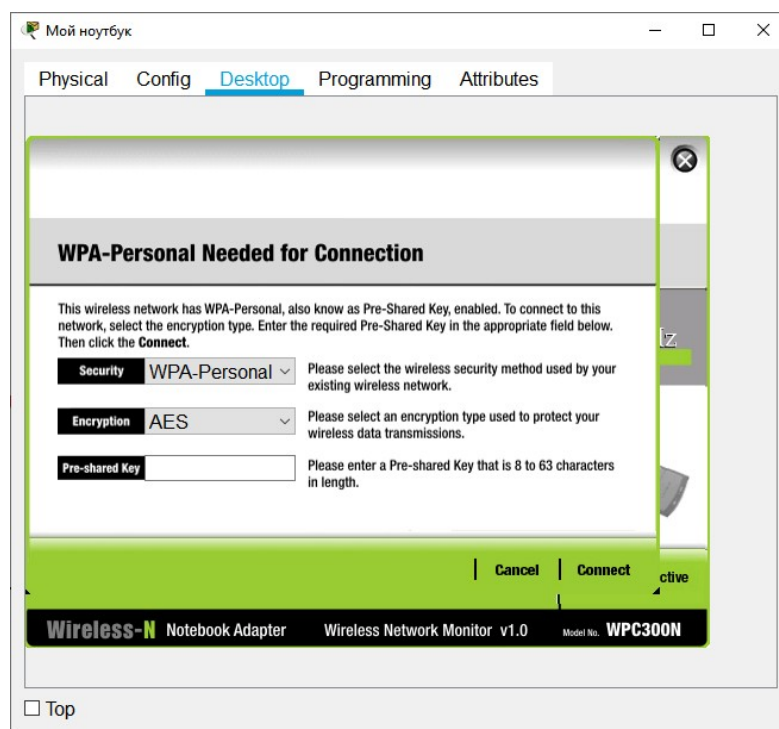


Рис. 5 – Настройка протокола WPA на ноутбуке

Подключитесь к точке Sirius и выберите настройки WPA. Введите ключевую фразу: 1234567890 и после этого проверьте установку соединения и статус подключения (Рис.6).

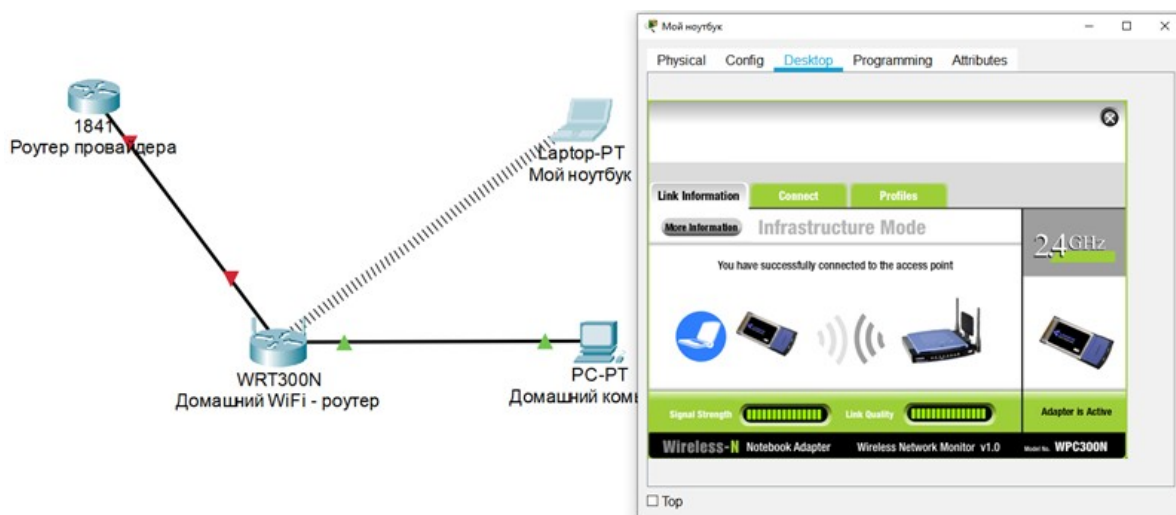


Рис. 6 – Установка соединения по протоколу WPA и статус сети

Соединение успешно установлено (Рис. 6). Обратите внимание при этом методе используется блочное шифрование AES, которое на сегодняшний день является очень распространённым и криптостойким алгоритмом [11,12] и не было не одного известного случая взлома данного шифра.

Далее, перенастройте беспроводное подключение по протоколу WPA2. Аналогично, как и в предыдущих двух разделах, сначала настройте точку доступа и сохраните настройки.

И так же перенастройте приложение беспроводной карты. Результаты настройки предоставлено на рисунке 7.

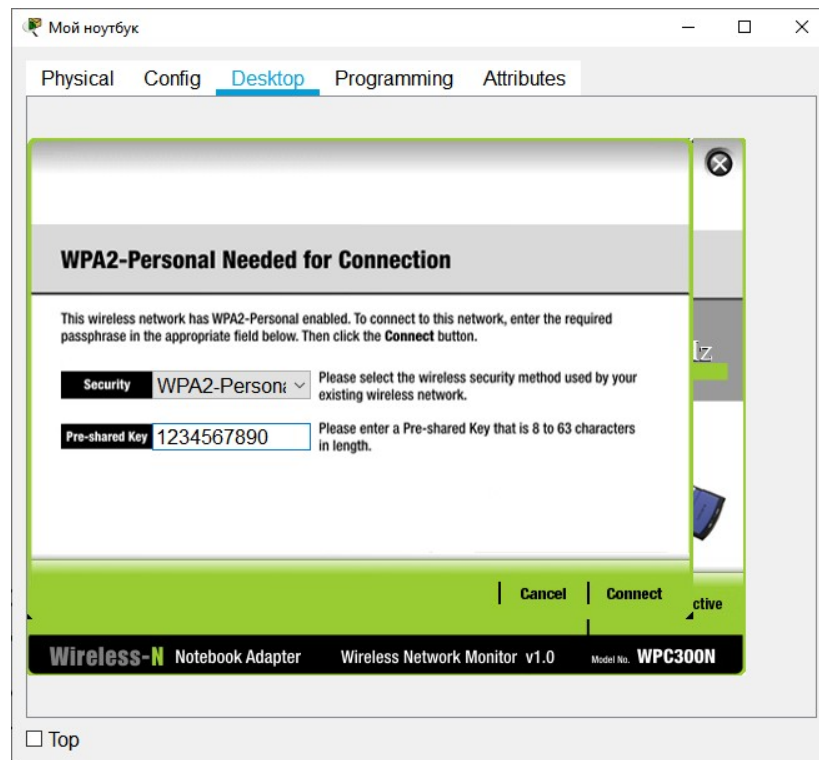


Рис. 7 – Настройка WPA2 в приложение беспроводной карты

Обратите внимание соединение по протоколы WPA2 установлено. В этом режиме также существует шифрование AES.

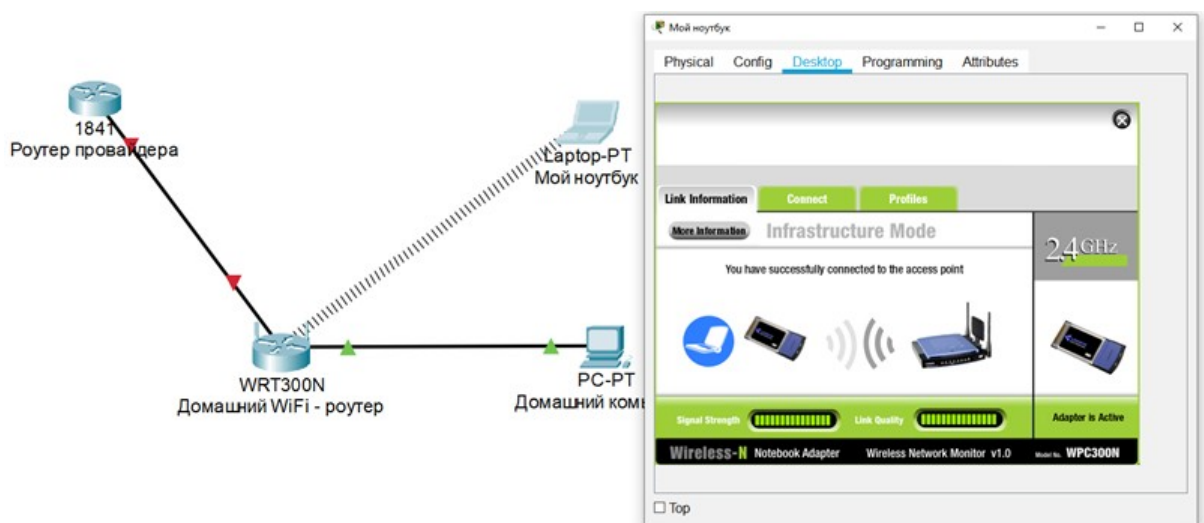


Рис. 8 – Установка соединения и статус сети

После того когда защищённое соединение установлено, между точкой доступа и ноутбуком должно осуществляться передача данных. Для проверки соединения можно с ноутбука подать команду ping на точку доступа и если пришел ответ, то защищённое соединение успешно установлено.

В данной статье рассмотрены основные аспекты моделирования защищённых беспроводных сетей Wi-Fi. Протоколы безопасности, такие как WEP, WPA и WPA2, играют ключевую роль в обеспечении защиты данных и предотвращении несанкционированного доступа. Моделирование с использованием программного обеспечения Cisco позволяет визуализировать и тестировать различные сценарии, что способствует лучшему пониманию принципов работы и защиты беспроводных сетей, а также может быть использовано в учебном

процессе. В работах [13-16] представлены результаты, используемые в учебном процессе с целью повышения компетенций обучающихся.

Список литературы:

1. WEP/WPA/WPA2 и методы борьбы с ними / Б. А. Ахметова [и др.] // Вестник современных исследований. – 2020. – № 8-1(38). – С. 4–7.
2. Олин, Р. А. Влияние автономных агентов с искусственным интеллектом на инновационные процессы в корпоративной среде / Р. А. Олин // Актуальные тренды в развитии науки, экономики, образования : сборник научных статей Всероссийской научно-практической конференции, Самара, 17 июня 2024 года. – Самара : Самарский государственный экономический университет, 2024. – С. 18–23.
3. Белетова, Д. У. Использование стандарта IEEE 802.1x для защиты от НСД / Д. У. Белетова // Электронный журнал: наука, техника и образование. – 2017. – № 1(10). – С. 6–15.
4. Шарипов, Р. Р. Методы анализа клавиатурного почерка пользователей с использованием эталонных гауссовских сигналов / Р. Р. Шарипов, А. С. Катасев, А. П. Кирпичников // Вестник Технологического университета. – 2016. – Т. 19, № 13. – С. 157–160.
5. Кухта, А. И. Анализ методов защиты беспроводной сети Wi-Fi / А. И. Кухта // Молодой исследователь Дона. – 2020. – № 2(23). – С. 41–48.
6. Шарипов, Р. Р. Проблемы при разработке систем распознавания пользователей по клавиатурному почерку / Р. Р. Шарипов, А. Н. Ситников // Вестник Технологического университета. – 2019. – Т. 22, № 10. – С. 143–147.7
7. Ковалев, Д. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 / Д. Ковалев // Первая миля. – 2014. – № 3(42). – С. 72–77.
8. Шарипов, Р. Р. Аппаратурный анализ клавиатурного почерка с использованием эталонных гауссовских сигналов / Р. Р. Шарипов, Н. З. Сафиуллин // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2006. – № 2. – С. 21–23.
9. IEEE Std 802.11-2020 – IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks—Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – 2020.
10. Шнайер, Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер ; пер. с англ. – Москва : Триумф, 2002. – 816 с.
11. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Санкт-Петербург : Питер, 2019. – 992 с.
12. Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3™ Security // Wi-Fi Alliance. – 2018. – URL: <https://www.wi-fi.org/discover-wi-fi/security> (дата обращения: 10.04.2025).
13. Cisco Systems. CCNA Security Course Book / Cisco Networking Academy. – 3rd ed. – Cisco Press, 2021. – 600 p.
14. Шарипов, Р. Р. Исследование электрических параметров пороговых извещателей / Р. Р. Шарипов, Б. З. Юсупов // Программные системы и вычислительные методы. – 2023. – № 3. – С. 29–47. – DOI: 10.7256/2454-0714.2023.3.43682.
15. Шарипов, Р. Р. Система распознавания клавиатурного почерка пользователей на основе полигауссового алгоритма / Р. Р. Шарипов, А. С. Катасев // Вестник Казанского государственного энергетического университета. – 2016. – № 4(32). – С. 45–59.
16. Олин, Р. А. Формирование инновационной среды предприятия с использованием средств искусственного интеллекта / Р. А. Олин, Е. С. Шатрова // Журнал монетарной экономики и менеджмента. – 2024. – № 3. – С. 213–217. – DOI: 10.26118/2782-4586.2024.99.23.032.