

**РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ НЕАВТОРИЗОВАННОГО ДОСТУПА В  
БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ С ПОМОЩЬЮ МИКРОКОНТРОЛЛЕРА  
ESP32**

**Семенов В.Д.** (Университет ИТМО)

**Научный руководитель – кандидат технических наук, доцент Попов И.Ю.**  
(Университет ИТМО)

**Введение.** Беспроводные сети уже используются практически во всех сферах деятельности. Ежедневно количество точек доступа Wi-Fi неуклонно растет, но несмотря на этот положительный аспект, количество уязвимостей, связанных с ними, также увеличивается. Несанкционированный доступ к беспроводному каналу передачи данных, используемый Wi-Fi, влечет угрозу конфиденциальности, доступности, целостности информации. Эта работа может быть полезна для всех сфер деятельности, где востребованы Wi-Fi сети: на производственных и промышленных предприятиях, в офисных центрах, в компаниях по оптовой и розничной торговле, гостиничных комплексах, транспортных предприятиях.

**Основная часть.** Целью данной работы является повышение точности определения несанкционированного доступа в беспроводную сеть Wi-Fi за счет использования микроконтроллера ESP32. Для достижения цели работы были решены следующие задачи:

- 1) Обоснована актуальность задачи защиты беспроводной сети Wi-Fi от несанкционированного доступа;
- 2) Выполнен анализ литературы в области защиты беспроводных сетей;
- 3) Разработана модель угроз безопасности беспроводной сети Wi-Fi;
- 4) Разработана структурную схему системы обнаружения несанкционированного доступа в беспроводную сеть Wi-Fi;
- 5) Проведена оценка эффективности разработанного метода.

**Выводы.** В процессе выполнения работы был разработан метод, позволяющий выявить неавторизованный доступ в беспроводную локальную сеть. Предложено решение по повышению точности определения несанкционированного доступа в беспроводную сеть Wi-Fi.

**Список использованных источников:**

1. Банк данных угроз безопасности информации [Электронный ресурс]. – URL: <https://bdu.fstec.ru>
2. IEEE 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. – URL: <https://standards.ieee.org/ieee/802.11/7028/>
3. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // Computer and Communications Security: In Proceedings of the 2017 ACM SIGSAC Conference – URL: <https://dl.acm.org/doi/10.1145/3133956.3134027>