

МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

## **ИНТЕРНЕТ/WI-FI ТЕХНОЛОГИИ**

### **РЕФЕРАТ**

студента 2 курса 251 группы  
направления 09.03.04 — Программная инженерия  
факультета КНиИТ  
Григорьева Даниила Евгеньевича

Проверено:

доцент, к. ф.-м. н.

\_\_\_\_\_

Черкасова О. А.

## СОДЕРЖАНИЕ

1 Введение .....	2
1 Принцип работы беспроводной коммуникации .....	4
1.1 Технология Wi-Fi .....	4
2 Стандарты Wi-Fi .....	5
2.1 Некоторые юридические аспекты .....	5
3 Атаки на беспроводные сети .....	6
3.1 Атаки отказа в обслуживании (DoS и DDoS) .....	6
3.2 Разведка и перехваты пакетов .....	6
3.2.1 Перехват пакетов .....	6
3.3 Атака получения доступа .....	6
3.4 Принудительная смена алгоритма шифрования .....	6
3.5 Атаки человека посередине .....	6
3.6 Атаки подмены ARP записей .....	6
4 Способы защиты от атак на Wi-Fi сети .....	7
4.1 Идентификация устройства, атакующего на отказ в обслуживании ..	7
4.2 Секретность на уровне проводной сети (WEP) .....	7
4.2.1 WEPCrack .....	7
5 Заключение .....	8
5 Список использованных источников .....	9

## ВВЕДЕНИЕ

На заре развития компьютерных сетей, когда встала необходимость обеспечения обмена разнообразными данными между различными сетевыми устройствами, для задания единообразного способа передачи информации возникли различные соглашения интерфейса — протоколы передачи данных — а Международная организация по стандартизации (ИСО) представила модель сетевых протоколов OSI/ISO (также OSI), которая разделила различные уровни взаимодействия систем и, таким образом, стала путеводной звездой при разработке будущих протоколов, эталонной моделью взаимосвязи открытых систем. Она состоит из семи уровней, каждый из которых выполняет определённые задачи. Эти уровни, начиная с нижнего, самого низкоуровневого, включают:

1. Физический уровень (У1)
2. Канальный уровень (У2)
3. Сетевой уровень (У3)
4. Транспортный уровень (У4)
5. Сеансовый уровень (У5)
6. Представительский уровень (У6)
7. Прикладной уровень (У7)

Каждый уровень модели OSI отвечает за свою часть процесса передачи данных, обеспечивая абстракцию и независимость от конкретных технологий.

Физический уровень является первым и самым низким уровнем модели OSI. Он отвечает за передачу необработанных битов данных по физическим носителям, таким как кабели и радиоволны. Он определяет способы передачи битов по физическим носителям, включая медные и оптоволоконные кабели, беспроводные каналы. Также У1 описывает электрические, механические и функциональные характеристики для активации и поддержания соединений между устройствами связи. Собственно, здесь определяются и сами физические носители, коих немало количество от коаксиального кабеля до оптоволокна и любой беспроводной среды.

Следующий за ним канальный уровень обеспечивает контроль стабильности физического канала связи и непосредственно общение между узлами одного сегмента локальной сети. На втором уровне модели OSI данные делятся на кадры, содержащие полезную нагрузку —

данные — и служебную информацию — метаданные (это, в частности, могут быть сетевые адреса отправителя и получателя). Для обнаружения и даже по мере возможности исправления ошибок передачи, как правило, используются контрольные суммы. Также канальным уровнем определяются правила доступа к физическому носителю, что предотвращает коллизии.

Общепринятые и наиболее распространённые на текущий момент времени стандарты обоих уровней разработаны Институтом инженеров электротехники и электроники США (IEEE). В первую очередь это группа IEEE 802, одним из наборов которой является IEEE 802.11. В нём описаны нормы и правила работы беспроводных компьютерных с использованием радиоволн и видимого света, а сам этот набор известен под торговой маркой Wi-Fi.

В рамках своей работы мною рассмотрен как сам стандарт, так и принцип его работы с физической точки зрения, а, кроме того, мною затронуты некоторые аспекты компьютерной безопасности, связанные с атакой и защитой беспроводных сетей на физическом уровне.

# **1 Принцип работы беспроводной коммуникации**

## **1.1 Технология Wi-Fi**

## **2 Стандарты Wi-Fi**

### **2.1 Некоторые юридические аспекты**

### **3 Атаки на беспроводные сети**

#### **3.1 Атаки отказа в обслуживании (DoS и DDoS)**

Создание широкополосных помех с помощью радио-джаммеров. Это эквивалент DoS-атаки, но только на физическом уровне радиосреды. Противостоять подобного рода атаке средствами инфраструктуры Wi-Fi практически невозможно, если мощность излучения высока

#### **3.2 Разведка и перехваты пакетов**

##### **3.2.1 Перехват пакетов**

Самый универсальный способ атаки на точку доступа — вычисление ее ключа WPA2 по отдельным сообщениям (M1-M4) из перехваченных хендшейков. Он срабатывает практически всегда, но требует больших затрат (особенно времени). Перехват «рукопожатий» всегда выполняется в режиме мониторинга, который поддерживает далеко не каждый Wi-Fi-чип и драйвер. Для ускорения сбора хендшейков потребуется функция инъекта пакетов, которая деавторизует подключенных к AP клиентов и заставляет их чаще отправлять «рукопожатия». Она и вовсе встречается у единичных Wi-Fi-модулей.

#### **3.3 Атака получения доступа**

#### **3.4 Принудительная смена алгоритма шифрования**

#### **3.5 Атаки человека посередине**

#### **3.6 Атаки подмены ARP записей**

## **4 Способы защиты от атак на Wi-Fi сети**

### **4.1 Идентификация устройства, атакующего на отказ в обслуживании**

использовать специальные технологии для идентификации типа устройства, создающего помехи и определения его физического местоположения в зоне покрытия. Например, это может быть выполнено с большой эффективностью в случае, если сеть построена на оборудовании Cisco Systems и Точки Доступа WiFi поддерживают технологию CleanAir (модельные ряды Cisco 3700, 3600, 2700, 1550 и тд). После обнаружения местоположения излучателя, в данную точку могут быть направлены сотрудники службы безопасности для физического устранения проблемы.

### **4.2 Секретность на уровне проводной сети (WEP)**

#### **4.2.1 WEPCrack**



## **ЗАКЛЮЧЕНИЕ**

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Линь Лай Тхи, Дык Буй Минь, Хуи Нгуен Нгок, Чыонг Нгуен Динь, Хю Нгуен Ба, Хыонг Лыу Чан Сетевая модель OSI // Научные исследования. 2017. №1 (12). URL: <https://cyberleninka.ru/article/n/setevaya-model-osi> (дата обращения: 29.10.2024).
2. Сложно о простом. Физический уровень (L1) модели OSI <https://habr.com/ru/companies/timeweb/articles/825344/>