

Министерство образования и науки, молодёжи  
и спорта Украины

## Анализ безопасности протокола WEP в компьютерных сетях стандарта 802.11 WLAN

Выполнил  
ст.гр. БИКС-08-2  
Фролов В.В.

Руководитель  
ст.преп. Олешко О.И.

# Задачи

- ▶ Изучить протокол WEP, процесс обмена пакетами и обеспечение аутентификации и конфиденциальности в сетях стандарта 802.11 WLAN.
- ▶ Исследовать возможные атаки и реализовать атаку с фрагментацией на WEP.
- ▶ Провести анализ безопасности WEP.
- ▶ Рассмотреть условия работы труда на рабочем месте и рассчитать КЕО для города Харькова.

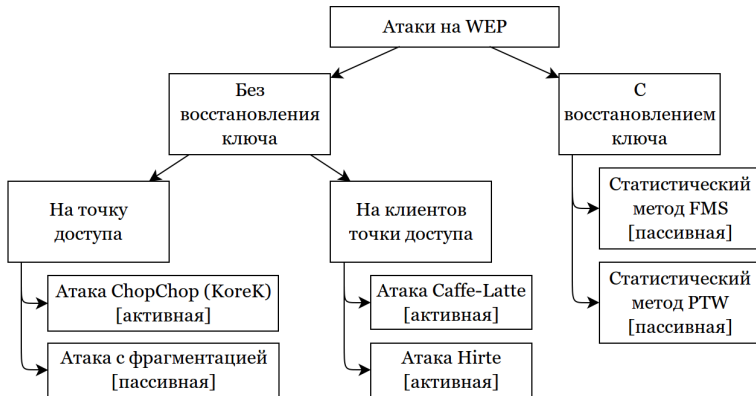
# Передача пакетов в сетях стандарта 802.11 WLAN



# Нарушитель в сетях стандарта 802.11 WLAN



# Классификация атак на протокол WEP

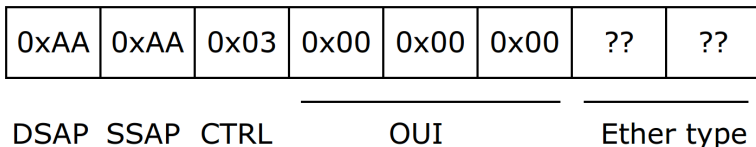


# Атака с фрагментацией

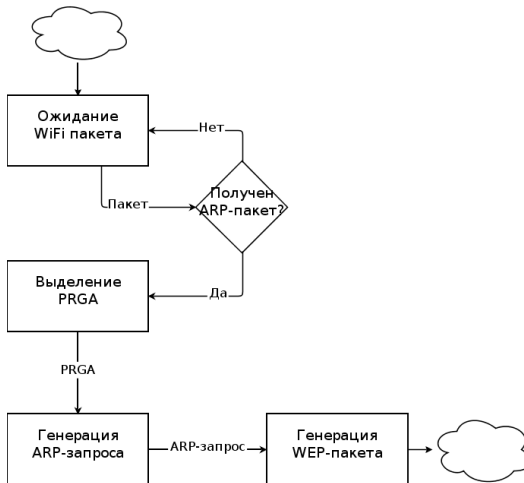
- ▶ Вычисление ключа PRGA (шифрующей гаммы)



- ▶ Стандартный заголовок LLC



# Алгоритм атаки с фрагментацией



# Анализ безопасности протокола WEP

- ▶ PTW атака (атака с восстановлением ключа) позволяет вычислить ключ в течение нескольких минут.
- ▶ Атака с фрагментацией (атака без восстановления ключа) позволяет вычислить гамму шифрования, что позволяет создавать легитимные пакеты, принимаемые точкой доступа.



# Охрана труда

- ▶ Разработаны меры по охране труда в НИЛ с углублённой обработкой вопроса расчёта КЕО для города Харькова.
- ▶ Коэффициент естественного освещения для города Харькова составил 1,8%.

# Выводы

- ▶ Исследован процесс обмена пакетами и обеспечение безопасности в сетях стандарта 802.11 WLAN.
- ▶ Рассмотрены возможные атаки на протокол WEP.
- ▶ Реализована атака с фрагментацией.
- ▶ Проведен анализ безопасности WEP.
- ▶ Расчитан коэффициент естественного освещения для города Харькова.

Спасибо за внимание.