

Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені К. Д. УШИНСЬКОГО»



ОДЕСЬКИЙ
НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ТРЕТЯ ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ
СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

24 квітня 2026 р.

Одеса – 2026

Інформатика, інформаційні системи та технології: тези доповідей двадцять третьої всеукраїнської конференції студентів і молодих науковців. Одеса, 24 квітня 2026 р. - Одеса, 2026. – 208 с.

Друкується за рішенням Вченої Ради
Університету Ушинського
(протокол № 13 від 30.04.2026 р.)

Організатори конференції продовжують традицію обміну досвідом у сфері освіти та використання інформаційних технологій. У конференції приймають участь студенти, аспіранти та молоді науковці вищих навчальних закладів України.

Тематика конференції охоплює наступне коло питань: сучасні інформаційні технології; інтелектуальні системи; методика викладання інформатики; інформаційні технології в освіті; психолого-педагогічне забезпечення інформатизації навчальної діяльності; дистанційна освіта і глобальні телекомунікаційні мережі; математичне моделювання й інформаційні технології; інформатизація системи керування освітою; інформаційні технології в менеджменті.

Наукові керівники:

завідувачка кафедри прикладної математики та інформатики навчально-наукового інституту природничо-математичних наук, інформатики та менеджменту, д. т. н., проф. Т. Л. Мазурок,
завідувач кафедри математичного забезпечення комп'ютерних систем факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. т. н., проф. Є. В. Малахов

Оргкомітет:

Голова:

Ректор Університету Ушинського,
д. і. наук, доц. А. В. Красножон

Заступники голови:

Проректор з наукової роботи Університету Ушинського, д. політ. н., проф. Г.В. Музиченко,
Директор навчально-наукового інституту природничо-математичних наук, інформатики та менеджменту, д. пед.н., проф. О. І. Ордановська,
Декан факультету математики, фізики та інформаційних технологій
ОНУ імені І. І. Мечникова, д. ф-м. н., проф. Ю. А. Ніцук

Члени оргкомітету:

д. т. н., проф.	Є. В. Малахов	д. т. н., проф.	Т. Л. Мазурок
д. т. н., проф.	Ю. О. Гунченко	к. п. н., доц.	А. О. Яновський
ст. викладач	І. М. Лісіцина	викладач	О. Я. Рубанська
ст. викладач	Н. Ф. Трубіна	к. ф.-м. н.	О. П. Бойко
ст. викладач	В. А. Корабльов	PhD, associated prof. (Poland)	A. Rychlik

© Навчально-науковий інститут природничо-математичних наук, інформатики та менеджменту Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», кафедра прикладної математики та інформатики, 2026

© Факультет математики, фізики та інформаційних технологій Одеського національного університету імені І. І. Мечникова, кафедра математичного забезпечення комп'ютерних систем, 2026

ПРОБЛЕМИ ПЕРЕВІРКИ ПОХОДЖЕННЯ ПРОГРАМНИХ АРТЕФАКТІВ.....	115
Паталашко П. Ю., Антоненко О. С.....	115
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КЕРУВАННЯ РУХОМИМ ОБ'ЄКТОМ.....	117
Борщ А. О., Рачинська А. Л.....	117
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ІНТЕГРАЦІЇ ДАНИХ У ГЕТЕРОГЕННІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ	118
Гавинський І. А., Малахов Є. В.	118
ХМАРНА ІНФОРМАЦІЙНА ПІДСИСТЕМА ТРАНСКРИБАЦІЇ І АНАЛІЗУ ТЕЛЕФОННИХ ДЗВІНКІВ.....	120
Гайдук Д. І., Волощук Л. А.	120
ДОСЛІДЖЕННЯ МЕТОДІВ ПОБУДОВИ ХМАРНИХ СИСТЕМ У ПАРАДИГМІ ІНФРАСТРУКТУРА ЯК КОД	122
Гудевич В. С., Антоненко О. С.	122
ROLLUPS AND DATA AVAILABILITY FOR INCREASING THE EFFICIENCY OF BLOCKCHAIN TRANSACTIONS PROCESSING	124
Dvorchuk D., Shpinareva I.....	124
РОЗПОДІЛЕНА ПЛАТФОРМА ДЛЯ УПРАВЛІННЯ НАУКОВИМИ КОНФЕРЕНЦІЯМИ У ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ	126
Денисенко О. В., Лісіцина І. М.	126
ПРОБЛЕМА ДЕВІАНТНОЇ ПОВЕДІНКИ ШІ В КРИТИЧНИХ СИТУАЦІЯХ	129
Жар М. Ю., Малахов Є. В.....	129
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РОЗРАХУНКУ НАПРУЖЕННЯ ПРИ ПОПЕРЕЧНОМУ ЗГІНІ БАЛОК.....	130
Земляний О. О., Іщенко О. В.....	130
ОГЛЯД АЛГОРИТМІВ ПОШУКУ НАЙКОРОТШОГО МАРШРУТА ДЛЯ КЕРУВАННЯ БЕЗПЛОТНИМ ТРАНСПОРТОМ	132
Коба В. В., Шпінарева І. М.....	132
РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ ВПЛИВУ ПАРАМЕТРІВ ПОПЕРЕЧНОГО ПЕРЕРІЗУ НА ЖОРСТКІСТЬ КОНСТРУКЦІЙНИХ ЕЛЕМЕНТІВ	134
Ісмаїлова А. Ш., Рачинська А. Л.....	134
ІНФОРМАЦІЙНА СИСТЕМА ОПЕРАТИВНОГО ОБМІНУ ТЕКСТОВИМИ ТА ПОТОКОВИМИ ДАНИМИ НА МАЛИХ ТА СЕРЕДНІХ ДИСТАНЦІЯХ	135
Ковальчук М. О., Малахов Є. В.	135
АКТИВНО-ПАСИВНИЙ ШІФЕР AIRCRACK-NG ДЛЯ РОБОТИ З ПРОТОКОЛАМИ СІМЕЙСТВА IEEE 802.11	138
Косоруков Є. Є., Шпінарева І. М.....	138
ПОРІВНЯЛЬНИЙ АНАЛІЗ СТРАТЕГІЙ ЗБЕРЕЖЕННЯ ДАНИХ У СИСТЕМАХ КОНТРОЛЮ ВЕРСІЙ ПРИ РОБОТІ З ВЕЛИКИМИ ФАЙЛАМИ.....	140
Костенко Д. Р., Іщенко О. В.	140

АКТИВНО-ПАСИВНИЙ СНІФЕР AIRCRACK-NG ДЛЯ РОБОТИ З ПРОТОКОЛАМИ СІМЕЙСТВА IEEE 802.11

Косоруков Є. Є., Шпінарева І. М.

Одеський національний університет імені І. І. Мечникова

Анотація. Ця робота розглядає можливості використання пакету інструментів AirCrack-ng для проведення інформаційно-безпекового аудиту бездротових мереж розроблених за стандартом IEEE 802.11.

Ключові слова: сніфер, бездротові мережі, захист бездротових мереж, IEEE 802.11, каналний рівень, радіозв'язок.

Бездротові технології прийому та передачі інформації посідають важливе місце в сучасному світі. Високий рівень загроз зумовлює необхідність пошуку методів захисту, які дозволяють системно вирішувати завдання інформаційної безпеки. Моніторинг бездротового середовища за допомогою сніферів дозволяє своєчасно виявляти приховані загрози для систем.

Aircrack-ng є потужним пакетом програм, які відносяться до вузькоспеціалізованих бездротових сніферів для аналізу радіомереж стандарту IEEE 802.11[1,**Помилка! Джерело посилання не знайдено.**]. Утиліта надає можливість працювати на каналному рівні з кадрами (eng. frame), маяками (eng. beacons), запитами на зондування (eng. probe request), а також рукоштовками (eng. handshakes). Сніфер Aircrack-ng дозволяє аналізувати безпеку бездротових мереж, комбінуючи пасивне прослуховування радіоефіру та активні атаки. До основних векторів атак відносяться:

- перехоплення та злом 4-етапного рукоштовання;
- пасивне перехоплення трафіку (сніфінг);
- підміна MAC-адрес та Deauth attacks.

На даний час значну частину цих вразливостей усуває новий стандарт протоколу безпеки WPA3[2]. Проте значна частина роутерів ще не підтримують цей протокол і тому багато користувачів та компаній продовжують використовувати старий WPA2-PSK. Хоча WPA2 надійно шифрує користувацький трафік, він залишається вразливим до перехоплення процесу авторизації[**Помилка! Джерело посилання не знайдено.**], що дозволяє зловмиснику підібрати пароль доступу до мережі.

Критичною проблемою WPA2 є відсутність захисту кадрів керування (англ. Management frames) [3]. Оскільки ці кадри не шифруються і не засвідчуються цифровим підписом, зловмисник може підробити MAC-адресу точки доступу та розсилати пакети на деавтентифікацію клієнтських пристроїв. Ні клієнт, ні точка доступу при цьому не зможуть розпізнати справжнього відправника, що змусить пристрій перепідключитися і дозволить хакеру перехопити нове

«рукостискання». При цьому пересічний користувач мережі залишається майже безсилим проти такого втручання, оскільки виявити пасивний збір інформації практично неможливо [3]. На відміну від активних атак, мережева карта хакера в режимі моніторингу не відправляє жодних запитів у мережу; вона лише «слухає» радіохвилі заданої частоти, фіксуючи абсолютно всі пакети, що потрапляють у радіоефір».

Типовий сценарій атаки виглядає наступним чином:

- 1) перевести мережеву карту у режим монітору за допомогою Airmon-ng;
- 2) почати прослуховування всіх доступних бездротових мереж за допомогою Airodump-ng;
- 3) отримати MAC-адресу та канал потрібної бездротової мережі;
- 4) відправити пакети на деавтентифікацію всіх клієнтів за допомогою Aireplay-ng;
- 5) почати прослуховування заданої мережі на заданому каналі до моменту, поки клієнт ні під'єднається наново;
- 6) отримати рукостискання клієнта та точки доступу;
- 7) методом грубої сили утилітою Airodump-ng знайти пароль бездротової мережі (рис.1).

```
Aircrack-ng 1.6
[00:00:01] 4934/10303715 keys tested (4616.34 k/s)
Time left: 37 minutes, 11 seconds                                0.05%
KEY FOUND! [ hellohello ]

Master Key      : 42 F5 71 13 82 7D A3 BE 84 C2 AD C0 D7 DA 53 54
                  D1 E6 0F 86 C2 66 A9 48 98 0E 7E 8C 51 94 7C A3

Transient Key   : 92 1C 0E 6B 64 3B F7 26 15 E5 BD 16 35 4B 5E 5C
                  29 E8 94 19 4A 9F F2 86 37 E0 5C DC 5D 65 B3 01
                  DC 74 81 D5 A8 93 46 B3 55 82 40 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 93 54 6E 80 15 25 3B 5F 91 25 21 61 17 F8 EE 3B
```

Рисунок 1– Результат роботи Airodump-ng

Найкращим захистом від подібного роду атак є наявність складного пароля, який має складатися не менш як з 12 символів, серед яких: малі та великі літери, цифри, спеціальні символи.

Література

1. Aircrack-ng [Електронний ресурс] – Режим доступу: <https://www.aircrack-ng.org/>.

2. Vanhoef, M., & Ronen, E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. // Conference: 2020 IEEE Symposium on Security and Privacy (SP) DOI:10.1109/SP40000.2020.00031
3. Wright, J. Detecting Wireless LAN MAC Address Spoofing.// Computer Science, Engineering. 2003.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТРАТЕГІЙ ЗБЕРЕЖЕННЯ ДАНИХ У СИСТЕМАХ КОНТРОЛЮ ВЕРСІЙ ПРИ РОБОТІ З ВЕЛИКИМИ ФАЙЛАМИ

Костенко Д. Р., Іщенко О. В.

Одеський національний університет імені І.І. Мечникова

Анотація. У роботі проведено порівняльний аналіз стратегій збереження даних у системах контролю версій при роботі з великими файлами та визначено їх ефективність за ключовими критеріями продуктивності.

Ключові слова: системи контролю версій, великі файли, стратегії збереження даних, управління версіями.

Зростання обсягів цифрових даних підвищує вимоги до систем контролю версій, зокрема в частині роботи з великими файлами, тобто мультимедійними матеріалами, архівами, програмними збірками та іншими подібними об'єктами. У межах даної роботи великими вважаються файли обсягом понад 50 МБ, що зазнають часткових змін між версіями. Неefективна стратегія збереження таких файлів призводить до надмірного зростання репозиторію та зниження швидкодії системи.

У сучасних системах контролю версій застосовуються три основні підходи: збереження повних копій файлів, збереження лише змін між версіями (дельта-кодування) та комбіновані методи. Вибір стратегії визначає обсяг дискового простору, швидкість фіксації змін і час відновлення попередніх версій.

Збереження повних копій забезпечує просте і швидке відновлення будь-якої версії, однак призводить до значного зростання обсягу репозиторію при частих оновленнях. Дельта-кодування мінімізує використання дискового простору, але збільшує обчислювальне навантаження при відновленні, оскільки потребує послідовного застосування ланцюжка змін. Комбіновані підходи поєднують переваги обох методів: повні копії зберігаються з певною періодичністю, тоді як проміжні версії фіксуються у вигляді дельт.

Для об'єктивного порівняння стратегій збереження даних доцільно використовувати низку ключових показників ефективності. До них належать швидкість виконання операцій фіксації змін, обсяг даних, що накопичується у репозиторії, а також час відновлення попередніх версій файлів. Зазначені

Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені К. Д. УШИНСЬКОГО»



ОДЕСЬКИЙ
НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ТРЕТЯ ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ
СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ
СИСТЕМИ ТА ТЕХНОЛОГІЇ

Збірник робіт

Збірник робіт надрукований в авторській редакції
без внесення суттєвих змін оргкомітетом

Підписано до друку 24.04.2026
Здано у виробництво 24.04.2026
Формат 60x84/16. Папір офсетний. Друк офсетний.
Тираж 50 примірників

Надруковано з готового оригінал-макета