**Силабус освітнього компонента**
Програма навчальної дисципліни

# Реверсне програмування

Шифр та назва спеціальності
123 – Комп'ютерна інженерія

Інститут
ННІ комп'ютерних наук та інформаційних технологій

Освітня програма
Сучасне програмування, мобільні пристрої та комп'ютерні ігри (інноваційний кампус/ Прикладна комп'ютерна інженерія)

Кафедра
Комп'ютерна інженерія та програмування (326)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка

Семестр
6

Мова викладання
Українська

## Викладачі, розробники

**Рисований Олександр Миколайович**

Oleksandr.Rysovanyi@khpi.edu.ua
кандидат технічних наук, доцент, професор кафедри комп'ютерної інженерії та програмування НТУ «ХПІ». Має більше 400 публікацій, з них 6 підручників та 2 навчальні посібники з грифами міністерства освіти і науки України, більш 50 навчальні посібники, більш 100 винаходів, оформлених у вигляді авторських свідоцтв, патентів, патентів на корисні моделі та ін. Викладає курси: «Системне програмування», «Реверсне програмування», «Низькорівневе програмування апаратних засобів».
Детальніше про викладача на сайті кафедри https://web.kpi.kharkov.ua/cep/2022/05/15/rysovannyj-oleksandr-mykolajovych/ та на особистому сайті http://blogs.kpi.kharkov.ua/v2/asm/

## Загальна інформація

### Анотація

Дисципліна спрямована на розгляд широкого кола питань, починаючи з антиналагоджувальних прийомів, дослідження формату PE-файлів, втручання в різні секції коду та даних, в тому числі з використанням нової точки входу в програму, збільшення розміру секцій, дослідження

динамічних бібліотек та закінчуючи реверсом програм з запитом паролю, шифруванням програми. Крім того, розглядаються питання перекриття коду, самомодифікації коду при виконанні та реверсингом програм з використанням перевірки дати та часу, з розміщенням даних в різних типах секцій, з перетворенням логічних операцій та різних варіантів виклику функцій. Використовується віконний інтерфейс в операційній системі x64. Теоретичний матеріал підкріплюється прикладами програмного коду – від простих програм до програм професійного рівня, таких як пакувальники та протектори, виконаних в макроасемблері.

### Мета та цілі дисципліни

Забезпечення теоретичної підготовки для дослідження та виправлення програмного коду, яке знаходиться в експлуатації; набуття практичних навичок впровадження в виконавчий файл прийомів виправлення помилок в програмному забезпеченні, яке знаходиться в експлуатації; використання заходів, спрямованих на запобігання появі та усунення вразливостей програми; створення нової функціональності, використовуючи неявне в експлуатації програмне забезпечення платформ x64 для професійного та системного програмного використання..

### Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – екзамен.

### Компетентності

ФК 2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення. .

### Результати навчання

ПРН 6. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.
ПРН 8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей..

### Обсяг дисципліни

Загальний обсяг дисципліни 120 (4 кредитів ECTS, 6 семестр): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно знати: лінійну алгебру, системне програмування.

### Особливості дисципліни, методи та технології навчання

Презентація, лекція-бесіда, лекція-візуалізація, навчальна дискусія, мозкова атака, кейс-метод, демонстрування, самостійна робота, метод порівняння, метод узагальнення, метод конкретизації, метод виокремлення основного, обговорення, робота над помилками.
Лекції проводяться з використанням мультимедійних технологій, в тому числі, проектора, персонального комп'ютера..

## Програма навчальної дисципліни

### Теми лекційних занять

Тема 1. Антиналагоджувальні прийоми. Ч.1.
Антиналагоджувальні прийоми. Загальні відомості. Обробка винятків. Трасування за часом виконання інструкцій. Функції роботи з мультимедійними таймерами.
Тема 2. Антиналагоджувальні прийоми. Ч.2.
API-функції виявлення наладчика. Налагоджувальні регістри. Прапори налагодження, пам'ять додатків.
Тема 3. Дослідження PE-формату.
Загальні відомості про PE-формат. DOS MZ-заголовок. PE-заголовок. Секції PE-файлу. Дослідження PE-файлу.
Тема 4. Впровадження в exe-файл в кінець секції коду без додавання API-функцій.
агальні відомості щодо алгоритму впровадження коду. Послідовність застосування без додавання API-функцій. Безпосереднє використання коду. Впровадження коду у діалогову програму.

Тема 5. Впровадження в exe-файл в кінець секції коду з додаванняя API-функцій.
Загальні відомості. Послідовність впровадження з додаванням API-функцій.
Тема 6. Впровадження коду. Додавання нової секції коду.
Основний алгоритм додавання нової секції. Додавання нової секції.
Тема 7. Впровадження коду в різні секції даних.
Макроси, написані користувачем. Системні макроси. Загальні відомості. Алгоритм впровадження коду у секції даних. Створення програми з трьома діалоговими вікнами.
Тема 8. Впровадження коду. Зміна точки входу в програму.
Основний алгоритм зміни точки входу до програми. Приклад зміни точки входу до програми.
Тема 9. Впровадження коду. Збільшення розміру секції.
Загальні відомості. Основний алгоритм збільшення розміру секції. Приклад збільшення розміру секції.
Тема 10. Реверсинг простих програм з запитом паролю.
Узагальнена послідовність пошуку пароля. Реверсинг консольної програми з консольним запитом пароля та використанням API-функції lstrcmp. Реверсинг діалогової програми з консольним запитом пароля та використанням API-функції lstrcmp.
Тема 11. Реверсинг програми з парольним захистом з використанням API-функції Lstcmp.
Реверсинг консольної програми з парольним захистом та використанням базових команд. Реверсинг діалогової програми з парольним захистом та використанням базових команд.
Тема 12. Реверсинг програми з парольним захистом з використанням базових команд.
Реверсинг консольної програми з парольним захистом та використанням рядкових команд. Створення програми із двома діалоговими вікнами.
Тема 13. Реверсинг програми з парольним захистом з використанням рядкових команд.
Обробка повідомлень від дочірніх вікон. Обробка повідомлень в діалоговій програмі.
Тема 14. Реверсинг програми з шифруванням паролю.
Захист вихідного програмного коду. Основні відомості. Прийоми обфускації. Поворотне шифрування. Програма вилучення частини пароля (без шифрування). Реверсинг програм із шифруванням коду.
Тема 15. Перекриття коду.
Алгоритм перекриття коду. Перекриття коду з переходом назад за програмним кодом. Перекриття коду з переходом уперед за програмним кодом.
Тема 16. Самомодифікація коду.
Загальні відомості. Проста програма перевірки пароля. Самомодируючі програми перевірки пароля. Самодифікуюча діалогова програма з кількома діалоговими вікнами. Реверсинг програми, що самодифікується.
Тема 17. Реверсинг програм з перевіркою датита часу.
Фіксована кількість запусків програми. Реверс програми перевірки дати закінчення запуску програми. Реверс програми запису кількості запусків програми у файл. Реверс програми запуску програми певну кількість разів. Реверс програми запису кількості запусків програми до реєстру. Послідовність реверсингу.
Тема 18. Реверсинг програм з розміщенням даних у секції коду.
Організація реєстру. Програмування задач з використанням реєстру.
Тема 19. Реверсинг програм з з перетворенням логічних операцій.
Організація реєстру. Програмування задач з використанням реєстру.
Тема 20. Реверсинг програм з різними варіантами виклику функцій.
Організація реєстру. Програмування задач з використанням реєстру.

## Теми практичних занять

## Теми лабораторних робіт

Тема 1. Антиналагоджувальні прийоми. Ч.1.
Антиналагоджувальні прийоми. Загальні відомості. Обробка винятків. Трасування за часом виконання інструкцій. Функції роботи з мультимедійними таймерами.
Тема 2. Антиналагоджувальні прийоми. Ч.2.

API-функції виявлення наладчика. Налагоджувальні регістри. Прапори налагодження, пам'ять додатків.

Тема 3. Дослідження PE-формату.

Загальні відомості про PE-формат. DOS MZ-заголовок. PE-заголовок. Секції PE-файлу. Дослідження PE-файлу.

Тема 4. Впровадження в exe-файл в кінець секції коду без додавання API-функцій.

агальні відомості щодо алгоритму впровадження коду. Послідовність застосування без додавання API-функцій. Безпосереднє використання коду. Впровадження коду у діалогову програму.

Тема 5. Впровадження в exe-файл в кінець секції коду з додаванняя API-функцій.

Загальні відомості. Послідовність впровадження з додаванням API-функцій.

Тема 6. Впровадження коду. Додавання нової секції коду.

Основний алгоритм додавання нової секції. Додавання нової секції.

Тема 7. Впровадження коду в різні секції даних.

Макроси, напсані користувачем. Системні макр Загальні відомості. Алгоритм впровадження коду у секції даних. Створення програми з трьома діалоговими вікнами.

Тема 8. Впровадження коду. Зміна точки входу в програму.

Основний алгоритм зміни точки входу до програми. Приклад зміни точки входу до програми.

Тема 9. Впровадження коду. Збільшення розміру секції.

Загальні відомості. Основний алгоритм збільшення розміру секції. Приклад збільшення розміру секції.

Тема 10. Реверсинг простих програм з запитом паролю.

Узагальнена послідовність пошуку пароля. Реверсинг консольної програми з консольним запитом пароля та використанням API-функції lstrcmp. Реверсинг діалогової програми з консольним запитом пароля та використанням API-функції lstrcmp.

Тема 11. Реверсинг програми з парольним захистом з використанням API-функції Lstcmp.

Реверсинг консольної програми з парольним захистом та використанням базових команд. Реверсинг діалогової програми з парольним захистом та використанням базових команд.

Тема 12. Реверсинг програми з парольним захистом з використанням базових команд.

Реверсинг консольної програми з парольним захистом та використанням рядкових команд. Створення програми із двома діалоговими вікнами.

Тема 13. Реверсинг програми з парольним захистом з використанням рядкових команд.

Обробка повідомлень від дочірніх вікон. Обробка повідомлень в діалоговій програмі.

Тема 14. Реверсинг програми з шифруванням паролю.

Захист вихідного програмного коду. Основні відомості. Прийоми обфускації. Поворотне шифрування. Програма вилучення частини пароля (без шифрування). Реверсинг програм із шифруванням коду.

Тема 15. Перекриття коду.

Алгоритм перекриття коду. Перекриття коду з переходом назад за програмним кодом. Перекриття коду з переходом уперед за програмним кодом.

Тема 16. Самомодифікація коду.

Загальні відомості. Проста програма перевірки пароля. Самомодируючі програми перевірки пароля. Самодифікуюча діалогова програма з кількома діалоговими вікнами. Реверсинг програми, що самодифікується.

Тема 17. Реверсинг програм з перевіркою датита часу.

Фіксована кількість запусків програми. Реверс програми перевірки дати закінчення запуску програми. Реверс програми запису кількості запусків програми у файл. Реверс програми запуску програми певну кількість разів. Реверс програми запису кількості запусків програми до реєстру. Послідовність реверсингу.

Тема 18. Реверсинг програм з розміщенням даних у секції коду.

Організація реєстру. Програмування задач з використанням реєстру.

Тема 19. Реверсинг програм з з перетворенням логічних операцій.

Організація реєстру. Програмування задач з використанням реєстру.

Тема 20. Реверсинг програм з різними варіантами виклику функцій.

Організація реєстру. Програмування задач з використанням реєстру.

**Самостійна робота**

Для самостійної роботи студентам рекомендується тема:
Реверсинг зашифрованої програми. Шифрування файлу з будь-яким розширенням відповідно до варіанта;  навести послідовність ручного розшифрування (знаходження ключа); - написати програму розшифровки відповідно до знайденого ключа.
Результат оформлюється у вигляді пояснювальної записки. Студентам також рекомендуються додаткові матеріали (відео, статті, підручники) для самостійного вивчення та аналізу, підготовки до лекційних, практичних та лабораторних занять.

## Література та навчальні матеріали

ОСНОВНА ЛІТЕРАТУРА

1. Рисований О.М. Реверсне програмування. Використання коду. Середовище програмування masm64 : навчальний посібник для студентів спеціальностей 123 «Комп'ютерна інженерія», 125 «Кібербезпека» [електронне видання] /О.М. Рисований. – Харків: НТУ «ХПІ», 2021. - 250 с.
- посилання будуть пізніше ?????
2.  Рисований О.М. Реверсне програмування. Крекінг. Середовище  програмування masm64  : навчальний посібник для студентів спеціальності: 123 – «Комп’ютерна інженерія» » [електронне видання] /О.М. Рисований. – Харків: НТУ «ХПІ», 2024. -
- посилання будуть до 01.07.24 ?????
3. Методичні вказівки для виконання лабораторних робіт з курсу "Низькорівневе програмування апаратних засобів", "Розроблення та застосування маніфесту додатка Win32. Середовище програмування masm64" для студентів спеціальності: 123 - "Комп'ютерна інженерія" усіх форм навчання [електронне видання] /упорядник О.М. Рисований. - Х. : НТУ "ХПІ", 2024. - 64 с.
- посилання будуть пізніше ?????
4. Методичні вказівки до виконання практичних та  лабораторних робіт з курсу «Низькорівневе програмування апаратних засобів. Управління комп'ютером. Командна оболонка» для студентів спеціальності: 123 - "Комп'ютерна інженерія" всіх форм навчання [електронне видання] /упорядник О.М. Рисований. - Х.: НТУ "ХПІ", 2024. - 64 с.
- посилання будуть пізніше ?????
5. Методичні вказівки до виконання практичних та лабораторних робіт з курсу «Системне програмування. Графічний інтерфейс користувача (GUI)  для студентів спеціальності *:* 123 – «Комп’ютерна інженерія» всіх форм навчання [електронне видання] / упорядник О.М. Рисований. - Х.: НТУ "ХПІ", 2024
- посилання будуть пізніше ?????
6. Методичні вказівки для виконання практичних та лабораторних робіт з курсу «Реверсне програмування. Антиналагоджувальні прийоми захисту від реверсу. Середовище програмування masm64 : для студентів спеціальності: 123 - "Комп'ютерна інженерія" всіх форм навчання [електронне видання] / укладач О.М. Рисований. - Х.: НТУ "ХПІ", 2024
- посилання будуть пізніше ?????

ДОДАТКОВА ЛІТЕРАТУРА

7. Ришковець Ю. В., Висоцька В. А. Алгоритмізація та програмування. Частина 1: навчальний посібник - Львів: Видавництво «Новий Світ - 2000», 2020. - 337 с.
http://library.kpi.kharkov.ua/files/new_postupleniya/atprc1.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

Тематичні бази даних https://ufn.ru/en/articles.
Закордонні електронні наукові інформаційні ресурси: European Library. Вільний доступ до ресурсів 47 Національних бібліотек Європи, Австралії, Білорусії, Великої Британії, Німеччини, бібліотека коледжу Лондонського університету.

## Система оцінювання

### Критерії оцінювання успішності студента та розподіл балів

Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
модульні контролі - 40 балів; практичні заняття - 30 балів; залік - 30 балів.

### Шкала оцінювання

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

| | | |
|---|---|---|
| Силабус погоджено | Дата погодження, підпис<br>22.04.2024 | Завідувач кафедри<br>Олександр ЗАКОВОРОТНИЙ |
| | Дата погодження, підпис<br>22.04.2024 | Гарант ОП<br>Олександр ЗАКОВОРОТНИЙ |