Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

[RE-83] ЗАХИСТ ДАНИХ


Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

| | |
|---|---|
| Рівень вищої освіти | Другий (магістерський) |
| Галузь знань | 17 Електроніка, автоматизація та електронні комунікації |
| Спеціальність | 172 Електронні комунікації та радіотехніка |
| Освітня програма | 172Мн РОС - Радіозв'язок і оброблення сигналів (ЄДЕБО id: 31175)172Мн ІТР - Інтелектуальні технології радіоелектронної техніки (ЄДЕБО id: 49263)172Мп РОС - Радіозв'язок і оброблення сигналів (ЄДЕБО id: 4857)172Мп ІТР - Інтелектуальні технології радіоелектронної техніки (ЄДЕБО id: 49262)172Мн РЕІ - Радіоелектронна інженерія (ЄДЕБО id: 53272), |
| Статус дисципліни | Нормативна |
| Форма здобуття вищої освіти | Очна (денна) |
| Рік підготовки, семестр | 1 курс, осінній семестр |

| | |
|---|---|
| Обсяг дисципліни | 5 кредитів ЄКТС /150 годин (Лекц. 36 год, Практ. год, Лаб. 36 год, СРС. 78 год ) |
| Семестровий контроль/контрольні заходи | Семестровий контроль: екзамен<br>Контрольні заходи: МКР, ДКР |
| Розклад занять | https://rozklad.kpi.ua |
| Мова викладання | Українська |
| Інформація про керівника курсу / викладачів | Лекц.: Навроцький Д. О. (navrotskyi@nau.edu.ua)<br>Лаб.: Навроцький Д. О.,<br>СРС.: Навроцький Д. О. |
| Розміщення курсу | Дистанційний курс в Google Classroom: https://classroom.google.com/u/3/c/NjIwNDA0NDQwMzUw |

Програма навчальної дисципліни

**1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання**

*Чому це цікаво/треба вивчати?*

Корисна інформація, завжди становить цінність, яку необхідно оберігати. На цьому курсі вивчимо основи криптографії для захисту каналів зв'язку і для захисту даних у сховищах.

*Чому можна навчитися (результати навчання)?*

- Навчитись основам симетричної і асиметричної криптографії.
- Навчитись використовувати існуючі шифратори для захисту різних програм/пристроїв.
- Навчитись створювати власні шифратори.

*Як можна користуватися набутими знаннями і уміннями (компетентності)?*

- Набуті знання дозволять використовувати існуючі шифратори, наприклад, AES256, RSA для захисту даних на комп'ютері і у мікроконтролері.
- Використовувати криптографію для захисту каналу зв'язку між різними пристроями

Метою викладання дисципліни є формування у студентів таких фахових компетентностей:

- ФК 21 Здатність до аналізу основних принципів передачі інформації;
- ФК 22 Здатність обирати та використовувати способи кодування інформації, принципи криптографії та шифрування даних.

Програмних результатів навчання:

- ПРН 23 Синтезувати та моделювати поведінку систем;
- ПРН 24 Обирати та оптимізувати канал передачі інформації, тип раціонального кодування інформації для передачі в каналах зв'язку. Вміти обирати та використовувати програмне забезпечення для надійного захисту інформації.

**2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)**

Бажане володіння мовами програмування низького і високого рівня.

Такими як C/C++, C#, Python.

Але, можна навчитись програмуванню і під час проходження курсу.

Дана дисципліна буде корисною для  практики

**3. Зміст навчальної дисципліни**

Тема 1. "Вступ до захисту даних. Цілі криптографії і стеганографії"

Тема 2. "Основи криптографії. Симетрична, асиметрична, гібридна, квантова криптографії"

Тема 3. "Криптографічні примітиви, функції перетворення"

Тема 4. "Незвідні та примітивні поліноми, Абелеві групи, поля, кільця, побудова S-Box (таблиця замін)"

Тема 5. "Потокові шифри"

Тема 6. "Блокові шифри"

Тема 7. "Режими шифрування"

Тема 8. "Порівняння AES подібних шифрів"

Тема 9. "Генератори псевдо-випадкових послідовностей"

Тема 10. "Цифровий підпис. Геш-функції".

Тема 11. "Аналіз шифрограми. Тести NIST STS, цифрова ентропія, тести Diehard"

Тема 12. "RSA шифри"

Тема 13. "Розробка власного шифру"

Тема 14. "Криптологія. Вразливості алгоритму і реалізації"

**4. Навчальні матеріали та ресурси**

Інформаційні ресурси:

1. Тести NIST STS [Електронний ресурс]. – Режим доступу:  https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

2. Тести Dieharder [Електронний ресурс]. – Режим доступу: https://webhome.phy.duke.edu/~rgb/General/dieharder.php

*3. І. Н. Войцехівська*. Криптографія// Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. — К. : Наукова думка, 2009. — Т. 5 : Кон — Кю. — С. 390. — 560 с. : іл. — ISBN 978-966-00-0855-4.

*4. О. В. Гомонай*. Криптографія // Енциклопедія сучасної України : у 30 т. / ред. кол. І. М. Дзюба [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2001–2020. — ISBN 944-02-3354-X.

5. Криптографія // Літературознавча енциклопедія : у 2 т. / авт.-уклад. Ю. І. Ковалів. — Київ : ВЦ «Академія», 2007. — Т. 1 : А — Л. — С. 532.

Навчальний контент

**5. Методика опанування навчальної дисципліни (освітнього компонента)**

Лабораторні роботи:

1. Створення форми авторизації для користувача (поле для вводу логіна і пароля);
2. Шифрування чисел за допомогою операції XOR (вона ж “складання за модулем 2”);
3. Шифрування тексту, одноразовим ключем, коли довжина тексту і ключа однакові.;
4. Шифрування файлу одноразовим ключем, коли довжина файлу значно більша за довжину ключа;
5. Створення цифрового підпису, використання HASH-функції;
6. Розширення ключа шифрування, створення “гами” довільної довжини. Стандарт PBKDF2.
7. Розрахунок інформаційної ентропії, аналіз шифрограми;
8. Режими симетричного блочного шифрування AES, 3DES;
9. Асиметричне шифрування RSA;
10. Розробка власного потокового шифру;
11. Стеганографія;
12. Криптологія.

Альтернативні лабораторні роботи:

1. Encryption/Decryption of Enigma Machine

2. Frequency-Based Decryption

3. Hacking at RobberCity

4. Crack the PIN

5. Error correction #1 - Hamming Code

6. Decode the QR-Code

7. Discrete Log Problem

8. Elliptic curve cryptography

Альтернативні лабораторні роботи рекомендовано проходити на сайтах https://www.codewars.com/ та https://www.codingame.com/ , https://leetcode.com/ Оскільки ці сайти мають вбудовані тести перевірки виконаних завдань. Також, іноді при наймі на роботу просять виконати одну з задач на такому сайті. Бажано, щоб студент був готовий до такої ситуації і мав вже певний рейтиг на цих сайтах

**6. Самостійна робота студента**

Домашня контрольна робота:

Розрахувати власну таблицю замін (S-Box) за вказаним незвідним поліномом і утворюючим елементом. Таблиця містить 256 унікальних елементів (числа від 0 до 255), розмір таблиці 16x16. Приклад S-Box для AES.

Політика та контроль

**7. Політика навчальної дисципліни (освітнього компонента)**

1. Пояснювально-ілюстративний метод, дискусійний метод, метод проблемного навчання
2. Методи навчання за джерелом передачі навчальної інформації: словесні, наочні, практичні
3. Максимум практичних занять, мінімум теорії (тільки необхідне)

**8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)**

Рейтинг студента складається із балів, які він отримує за:

1. Виконання лабораторних робіт (48 балів)

2. Тест (4 бали)

3. Модульна контрольна робота (6 балів)

4. Домашня контрольна робота (12 балів)

5. Екзамен (30 балів)

1. Виконання лабораторних робіт:

Виконання лабораторних робіт передбачає оформлення результатів у формі протоколу.

При оформленні протоколу необхідно надавати коментарі та висновки, а також надати відповіді на контрольні питання та забезпечити пояснення ходу виконання лабораторної роботи та отриманих результатів.

Форма зарахування/захисту лабораторних робіт передбачає два варіанти:

Перший варіант захисту лабораторних робіт проводиться у формі співбесіди шляхом надання відповідей на запитання викладача. Така форма захисту передбачає наступну градацію нарахування балів за одну лабораторну роботу:

— виконання всіх пунктів завдання, повне володіння матеріалом (не менше 90% ), наявність звіту, проведення тестування алгоритму реалізації моделі, аналіз результатів, наявність висновків — 4.00 балів

— виконання переважної більшості завдання, добре володіння матеріалом (не менше 75% ) — 3.00...3.90 балів

— часткове виконання завдання, достатнє володіння матеріалом (не менше 60% ) — 2.40...2.90 балів

— повністю неправильне виконання завдання або відсутність наданих результатів виконання завдання або недостатнє володіння матеріалом (менше 60%) — 0 балів.

Другий варіант захисту передбачає надання на перевірку оформленого протоколу виконання лабораторних робіт із наданими письмовими відповідями, розрахунками, коментарями тощо, без проведення співбесіди. При цьому максимальний бал, який може бути нарахований за захист лабораторної роботи становить 64% від максимального балу, що може бути отриманий при умові проведення захисту у формі співбесіди. Градація балів за одну лабораторну роботу згідно другого варіанту проведення здачі лабораторної роботи має наступний вид:

— «достатньо» (виконано всі пункти лабораторної роботи, надані письмові коментарі щодо отриманих результатів, надані письмові відповіді на перелік питань, надані висновки) — 2.40...2.56 балів

— «незадовільно» (відсутні відповіді на окремі контрольні питання, відсутні коментарі щодо отриманих результатів, етапів виконання роботи, відсутні висновки або лабораторна робота не виконана в повному обсязі або не виконана загалом або відсутній протокол) — 0 балів

Всього пропонується для виконання 12 лабораторних робіт. Максимальна кількість балів, яку можна отримати за успішне виконання всіх лабораторних роботі становить 48 балів.

2. Тест.

У формі надання письмових відповідей на перелік питань

• «відмінно» (надано не менше 90% потрібно інформації) — 4.00 бали

• «добре» (надано не менше 75% потрібно інформації) — 3.00...3.95 балів

• «достатньо» (надано не менше 60% потрібно інформації) — 2.40...2.95 балів

• «незадовільно» (надано менше 60% потрібно інформації) — 0 балів

3. Модульна контрольна робота

Модульна контрольна пишеться в кінці семестру і передбачає контроль успішності засвоєння головних тем, які були розглянуті в кредитному модулі та вміння використовувати набуті знання для

вирішення практичних завдань.

• «відмінно», правильне виконання всіх пунктів завдання, (надано не менше 90% потрібно інформації) – 6.00 балів.

• «добре», правильно виконано 75%-90% завдань. Правильність ходу виконання завдань, наявність незначних похибок в чисельних обрахунках – 3.50…4.95 балів.

• «достатньо», правильно виконано 60%-74% завдань. Існують окремі суттєві помилки або відсутні обґрунтовані відповіді на деякі пункти завдань — 2.00…3.45 балів.

• «незадовільно», наявні грубі помилки, надано менше 60% потрібно інформації, відсутність правильного ходу рішення завдань, відсутність завдання — 0 балів

Максимальна кількість балів, яку можна отримати за модульну контрольну роботу становить 10 балів.

4. Домашня контрольна робота

оцінена за такою шкалою:

незадовільно – 0 балів;

достатньо 1-3;

задовільно – 4-6 бали;

добре – 7-8 балів;

дуже добре – 9-10;

відмінно – 11-12 балів.

У випадку відсутності студента на захисті домашньої контрольної роботи без поважної причини, йому зараховується 0 балів. У випадку відсутності студента на захисті домашньої контрольної роботи з поважної причини, йому зараховується 0 балів з наданням можливості повторного захисту роботи

5. Екзамен

Мінімальний бал для допуску до екзамену становить 30 балів.

Студенти у яких менше 30 балів до екзамену не допускаються і мають доздати відповідні роботи або написати контрольну роботу для допуску на екзамен.

Екзаменаційний білет складається із 3 завдань. Бали за нараховуються так:

Завдання 1:

— «відмінно» (надано не менше 90% потрібно інформації) — 10.00 балів

— «добре» (надано не менше 75% потрібно інформації) — 7.50...9.95 бали

— «достатньо» (надано не менше 60% потрібно інформації) — 6.00...7.45 бали

— «незадовільно» (надано менше 60% потрібно інформації) — 0 балів

Завдання 2:

— «відмінно» (надано не менше 90% потрібно інформації) — 10.00 балів

— «добре» (надано не менше 75% потрібно інформації) — 7.50...9.95 бали

— «достатньо» (надано не менше 60% потрібно інформації) — 6.00...7.45 бали

— «незадовільно» (надано менше 60% потрібно інформації) — 0 балів

Завдання 3:

— «відмінно» (надано не менше 90% потрібно інформації) — 10.00 балів

— «добре» (надано не менше 75% потрібно інформації) — 7.50...9.95 бали

— «достатньо» (надано не менше 60% потрібно інформації) — 6.00...7.45 бали

— «незадовільно» (надано менше 60% потрібно інформації) — 0 балів

Максимальна кількість балів, яку можна отримати за екзамен становить 30 балів.

Студенти, які не виконали лабораторні роботи, до екзамену не допускаються

*Таблиця відповідності рейтингових балів оцінкам за університетською шкалою*

| **Кількість балів** | **Оцінка** |
|---|---|
| 100-95 | Відмінно |
| 94-85 | Дуже добре |
| 84-75 | Добре |
| 74-65 | Задовільно |
| 64-60 | Достатньо |
| Менше 60 | Незадовільно |
| Не виконані умови допуску | Не допущено |

**9. Додаткова інформація з дисципліни (освітнього компонента)**

Приклади екзаменаційних запитань:

1. Що таке семерична криптографія?
2. Що таке асиметрична криптографія?

3. Коли використовують відкритий ключ шифрування?
4. Коли використовують секретний ключ шифрування?
5. Що таке інформаційна ентропія?
6. Що таке гамування?
7. Що таке шифрограма?
8. Коли використовують блочні шифри?
9. Коли використовують потокові шифри?
10. Основні криптографічні примітиви?
11. Які популярні стандарти шифрування?
12. Чим відрізняється практична від теоретичної криптостійкості шифру?
13. Що таке вразливість реалізації шифру?
14. Які бувають режими шифрування?

*Опис матеріально-технічного та інформаційного забезпечення дисципліни*

IDE Visual Studio для Python, C#, C/C++

Робочу програму навчальної дисципліни (силабус):
**Складено** Навроцький Д. О.;

**Ухвалено** кафедрою ПРЕ (протокол № 06/2023 від 22.06.2023 )

**Погоджено** методичною комісією факультету/ННІ (протокол № 06-2023 від 29.06.2023 )

**Погоджено** методичною комісією факультету електроніки (протокол № 06\23 від 29.06.2023 р.)