Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра «Інженерії програмного забезпечення» (№ 603)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ І.В. Шевченко
(підпис) (ініціали та прізвище)

«_30_» ___08_____ 2024 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних

(назва навчальної дисципліни)

Галузь знань: 12 Інформаційні технології
(шифр і найменування галузі знань)

Спеціальність: 121 Інженерія програмного забезпечення
(код та найменування спеціальності)

Освітня програма: Інженерія програмного забезпечення
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2024 року

Харків – 2024 р.

Розробник: Дем’яненко В.А., ст.викладач . кафедри №603
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри інженерії програмного забезпечення (№ 603)

Протокол № 1 від « 30 » серпня 2024 р.

Завідувач кафедри д-р техн.наук., проф. І.Б. Туркін
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Погоджено з представником здобувачів освіти:
Представник студентського самоврядування Дикун Д.В.
(підпис) (ініціали та прізвище)

1. Загальна інформація про викладача

Дем’яненко Владислав Анатолійович, старший викладач кафедри. З 2001 р викладає в Національному аерокосмічному університеті ім. Н.Є. Жуковського «ХАІ».

Має 9 наукових і навчально-методичних публікацій. Викладає дисципліни «Моделі і методи захисту інформації та ПО», «Безпека програм та даних», «Об’єктно орієнтоване програмування», «Криптовалюти і блокчейн технології», «Проектування розподілених систем ЕОМ.

Напрями наукових досліджень: Криптовалюти та блокчейн технології, криптографія та безпека програмного забезпечення, інтернет речей та розумний дім.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 7 семестр.

Обсяг дисципліни:

4,5 кредита ЄКТС (135 годин), у тому числі аудиторних – 64 годин, самостійної роботи здобувачів **–** 71 години.

Форми здобуття освіти

Денна, дистанційна, заочна.

Дисципліна – обов’язкова.

Види навчальної діяльності – лекції, практичні (семінарські) заняття, розрахункова робота (РР), самостійна робота здобувача.

Види контролю – поточний, модульний та підсумковий (семестровий) контроль (іспит).

Мова викладання – українська.

Необхідні обов’язкові попередні дисципліни (пререквізити) –

ОК36. Фізика

ОК03. Алгоритми систем підтримки прийняття рішень

ОК20. Об'єктно-орієнтоване програмування

Необхідні обов’язкові супутні дисципліни (кореквізити) – немає.

3. Мета та завдання навчальної дисципліни

Мета вивчення: надання студентам знань і здобуття навичок з принципів роботи та побудови сучасних систем захисту інформації та програмного забезпечення у інформаційних системах

Завдання: опанування студентами практичними навичками використання: методів криптографічного захисту інформації; сучасних криптографічних програмних бібліотек захисту інформації; методів цифрового підпису у системах електронного документообігу; методів захисту програмного забезпечення від несанкціонованого доступу; принципів захисту корпоративних мереж від несанкціонованого втручання.

Після опанування дисципліни здобувач набуде наступні компетентності:

Загальні компетентності:

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

Фахові компетентності:

ФК01. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

ФК05. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

ФК06. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

ФК11. Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.

ФК16. Здатність розробляти методичні, інформаційні, математичні, алгоритмічні та програмні засоби реалізації інформаційних технологій

ФК17. Здатність впроваджувати та адмініструвати роботу програмних систем та комп’ютерних мереж.

Програмні результати навчання:

ПРН10. Проводити передпроєктне обстеження предметної області, системний аналіз об'єкта проектування.

ПРН15. Мотивовано обирати мови програмування та технології розробки для розв’язання завдань створення і супроводження програмного забезпечення.

ПРН18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Задачі та призначення курсу.

Тема 1. Задачі та призначення курсу. Термінологія. Властивості та види інформації.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Шифри перестановок

- *Обсяг самостійної роботи здобувачів: 4 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 2. Види та форми подання інформації. Машинне подання інформації. Фізичне подання інформації та процеси її обробки

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Тема практичної роботи: Шифри заміни

- *Обсяг самостійної роботи здобувачів: 4 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 3. Класифікація об'єктів захисту інформації. Організація проектування АСОД.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 годин.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Криптоаналіз за допомогою частотних характеристик

Обсяг самостійної роботи здобувачів: 4 години.

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 4. Потенційні загрози безпеки інформації. Випадкові загрози. Навмисні загрози.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Шифрування гамуванням

- *Обсяг самостійної роботи здобувачів: 4 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 5. Огляд методів захисту інформації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Шифрування алгоритмом DES

- *Обсяг самостійної роботи здобувачів: 4 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 6. Обмеження доступу. Контроль доступу до апаратури. Розмежування та контроль доступу до інформації та методів захисту інформації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Шифрування методом Вернама

- *Обсяг самостійної роботи здобувачів: 4 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 7. Розподілення привілей на доступ. Ідентифікація та встановлення дійсності об'єкту (суб'єкт)

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Блочні шифри

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 8. Криптографічне перетворення інформації. Огляд та класифікація методів шифрування інформації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Шифрування IDEA

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Модульний контроль 1

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: за необхідністю*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.*
- *Обсяг самостійної роботи здобувачів – 5 години.*

Підготовка до модульного контролю.

Змістовний модуль 2. Криптографічне перетворення інформації

Тема 9. Вибір методу перетворення. Коди. Шифри. Шифр VERNAN.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Системи з відкритим ключем RSA

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 10. Криптографія за приватним ключем. Механізми шифрування по таємному ключу.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Шифрування Полига-Хеллмана

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 11. Криптографія по загальному ключу. Багатопользовательські криптографічні методи.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 годин.

Тема практичної роботи: Шифрування Єль-Гамаля

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): персональний комп'ютер або ноутбук.

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 12. Обмеження на криптографію. Криптографічні атаки..

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Перевірка відповідності ключа

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 13. Засоби формування цифрового підпису інформації, що передається.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Хешування

- *Обсяг самостійної роботи здобувачів: 2 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 14. Вибір засобів захисту інформації в трактах передачі даних Аналіз сучасних методів оцінки захищеності інформації. Принциповий підхід до оцінки рівня безпеки інформації від навмисного НСД

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 4 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи:

Електронний підпис та сигнатура

Обсяг самостійної роботи здобувачів: 2 години.

Опрацювання матеріалу лекцій. Формування питань до викладача.

Модульний контроль 2

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: за необхідністю*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.*
- *Обсяг самостійної роботи здобувачів – 5 години.*

Підготовка до модульного контролю.

Змістовний модуль 3. Сучасні методи захисту інформації

Тема 15. Методи програмної інженерії Сучасні методи захисту інформації WinCrypt API.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 8 годин.

Тема практичної роботи: Сучасні методи захисту інформації WinCrypt API.

Розрахункова робота: «Розробка системи захисту інформації за допомогою програмного криптографічного інтерфейсу WinCrypt API».

- *Обсяг самостійної роботи здобувачів: 16 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Оформлення лабораторної роботи та підготовка до її здачі, виконання розрахункової роботи, оформлення звіту та підготовка до захисту розрахункової роботи.

Модульний контроль 3

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
- *Обсяг аудиторного навантаження: за необхідністю*
- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.*
- *Обсяг самостійної роботи здобувачів – 5 годин.*

Підготовка до модульного контролю.

5. Індивідуальні завдання

Виконання розрахункової роботи за темою

"Розробка системи захисту інформації за допомогою програмного криптографічного інтерфейсу WinCrypt API".

6. Методи навчання

Словесні, наочні, практичні.

7. Методи контролю

Поточний контроль (теоретичне опитування й розв'язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	-	-	-
Виконання і захист практичних робіт	0...3	8	0...24
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Робота на лекціях	-	-	-
Виконання і захист практичних робіт	0...3	6	0...18
Модульний контроль	0…20	1	0…20
Змістовний модуль 3			
Робота на лекціях	-	-	-
Виконання і захист практичних робіт	0...3	1	0...3
Модульний контроль	0…10	1	0…10
Виконання і захист РГР (РР, РК)	0…15	1	0..15
Усього за семестр			**0…100**

Прийнята шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка для екзамену, *курсового проекту* (роботи), практики
90-100	відмінно
75-89	добре
60-74	задовільно
01-59	незадовільно з можливістю повторного складання

Семестровий контроль (іспит) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних питань (кожне питання 50 балів)

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Здати всі практичні роботи (достатньо виконання ручного розрахунку), захистити розрахункову роботу (достатньо виконання ручного розрахунку), мати необхідних мінімум знань за всіма темами та мінімум вмінь щодо застосування отриманих знань.

Добре (75-89). Здати всі практичні роботи (достатньо часткової програмної реалізації розрахунків), захистити розрахункову роботу (достатньо часткової програмної реалізації розрахунків), знати всі теми та уміти застосовувати їх.

Відмінно (90-100). Здати всі практичні роботи (тільки програмна реалізації розрахунків), захистити розрахункову роботу роботи (тільки програмна реалізації розрахунків), досконально знати всі теми та уміти застосовувати їх.

9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем.

Всі учасники освітнього процесу мають діяти згідно «Кодекс етичної поведінки у ХАІ» (http://surl.li/twxevg), «Положення про академічну доброчесність» (http://surl.li/temmvq), «Кодекс академічної доброчесності» (http://surl.li/uotynb).

10. Методичне забезпечення та інформаційні ресурси

Підручники, навчальні посібники, навчально-методичні посібники, конспекти лекцій, методичні рекомендації з проведення лабораторних робіт тощо, які видані в Університеті знаходяться за посиланням: https://library.khai.edu/catalog

1. Дистанційний курс дисципліни розроблено у системі дистанційного навчання Mentor, яку впроваджено в Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ», доступ до курсу за посиланням: https://mentor.khai.edu/course/view.php?id=215
2. Software Engineering Institute, https://www.sei.cmu.edu/
3. Спілка программістів. https://dou.ua/
4. Стандарти вищої освіти України бакалавра та магістра з інженерії програмного забезпечення, https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/121-inzheneriya-programnogo-zabezpechennya-bakalavr.pdf, https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/2020/11/17/121-inzheneriya-prohramnoho-zabezpechennya-mahistr.pdf

11. Рекомендована література

Базова

1. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с
2. Інформаційна безпека/ За ред. Ю. Я. Бобала та І. В. Горбатого, Львівська політехніка, 2019.-540 с.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
4. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв,О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
5. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науковопрактичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с
6. Кібербезпека: лабораторний практикум з основ крипографічного захисту/ Євсеєв С.П. , Король О.Г. Новий світ-2000, 2021.-241 с.

Допоміжна

1. КриптоаналіЗ. КриптографічніІ протоколи / О.М. Гапак // Навчальний посібник з курсу «Комп'ютерна криптографія» для студентів інженерно-технічного факультету спеціальності 123-«Комп’ютерна інженерія». Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. – 96с.
2. Чепурна М. М., Лук’яненко Ю. В. Захист інформації: навчальний посібник. Київ: Видавничий дім «КМ Академія», 2021..
3. Мельник Ю.М. Основи криптографії. – Київ: Наукова думка, 2021.
4. Ковальов О.В. Криптографічні методи захисту інформації: навчальний посібник. – Київ: Центр учбової літератури, 2017
5. Олексій Марков, "Криптографічні протоколи та алгоритми: від теорії до практики", видавництво "Ділові перспективи", 2019.

1. Інформаційні ресурси

1. http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi
2. https://esu.com.ua/article-1576
3. http://nbuv.gov.ua/node/208
4. http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1276-evolution-of-cryptographic-algorithms-for-encryption