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.Б. Туркін
(підпис) (ініціали та прізвище)

«_31_» ___08_____ 2021 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 01.09.2021 року

Харків – 2021 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 № 2 від « 31 » серпня 2021 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:
Тимчасовий студентський самоврядний від факультету №6 (підпис) Д.В. Кологрив
(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 кредита ЄКТС (120 годин), у тому числі аудиторних – 56 годин, самостійної роботи здобувачів **–** 64 години.

Форми здобуття освіти

Денна, дистанційна, дуальна.

Дисципліна – обов’язкова.

Види навчальної діяльності – лекції, практичні роботи, самостійна робота здобувача.

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

Мова викладання – українська.

Необхідні обов’язкові попередні дисципліни (пререквізити) – «Комп`ютерна дискретна математика», «Математичний аналіз», «Об’єктно-орієнтоване програмування», «Теорія ймовірностей та емпіричні методи програмної інженерії».

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.

Загальні компетентності:

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК05. Здатність вчитися і оволодівати сучасними знаннями.

ЗК06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності:

ФК03. Здатність розробляти архітектури, модулі та компоненти програмних систем.

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

ФК10. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.

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

ФК13. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

Програмні результати навчання:

ПРН01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПРН03. Знати основні процеси, фази та ітерації життєвого циклу програмного забезпечення.

ПРН05. Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об’єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.

ПРН06. Уміння вибирати та використовувати відповідну задачі методологію створення програмного забезпечення.

ПРН09. Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.

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.

ПРН25. Розуміти можливості веб-технології для використання в маркетингових та орієнтованих на користувачів цілях

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: 2 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, самостійна робота.

Обсяг аудиторного навантаження: 2 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: 2 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: 2 години.

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

Тема практичної роботи: Шифрування гамуванням

- *Обсяг самостійної роботи здобувачів: 3 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 5. Огляд методів захисту інформації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 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 інформаціїяд методів захисту інформації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

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

Тема практичної роботи:

Шифрування методом Вернама

- *Обсяг самостійної роботи здобувачів: 3 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: 2 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: 2 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: 2 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, самостійна робота.

Обсяг аудиторного навантаження: 2 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: 2 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: 2 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, самостійна робота.

Обсяг аудиторного навантаження: 2 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: 2 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: 4 годин.

Тема практичної роботи: Сучасні методи захисту інформації WinCrypt API

- *Обсяг самостійної роботи здобувачів: 11 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача. Оформлення лабораторної роботи та підготовка до її здачі

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

Не передбачено навчальним планом

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	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	2...5	4	8...20
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	2...3	6	12...18
Модульний контроль	10…20	1	10…20
Змістовний модуль 3			
Робота на лекціях	0…1	2	0…2
Виконання і захист лабораторних (практичних) робіт	3...6	1	3...6
Модульний контроль	10…20	1	10…20
Усього за семестр			**60…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). Показати мінімум знань та умінь.

Добре (75-89). Твердо знати мінімум, здати тестування та поза аудиторну самостійну роботу.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». 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. Питання, що стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

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:

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. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си (Брюс Шнайер). Издательство: Триумф, 2013 -815с.
2. Цифровая стеганография. Издательство: Солон-Пресс, 2016 – 272с.
3. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика. 1997 – 368с.
4. Либерти Джесс. С++. Энциклопедия пользователя: Пер. с англ./Джесс Либерти – К.: Издательство «ДиаСофт», 2000 –584с.
5. Труды института инженеров по электротехнике и радиоэлектронике (ТИИЭР). Малый тематический выпуск «Защита информации»: пер. с англ., Том 76, №5, Май 1998.
6. Домарев В.В. Защита информации и безопасность комптютерных систем. – К.: Издательство «ДиаСофт», 1999. – 480 с.

Допоміжна

1. Дж. Л. Месси. Введение в современную криптологию. // ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.24-42.
2. У. Диффи. Первые десять лет криптографии с открытым ключом. // ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.54-74.
3. А. В. Спесивцев и др. Защита информации в персональных компьютерах. – М., Радио и связь. 1992, с.140-149.
4. В. Жельников. Криптография от папируса до компьютера. – М., ABF, 1996.

1. Інформаційні ресурси

1. http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi
2. http://cryptography.ru/
3. http://algolist.manual.ru/defence/intro.php