Міністерство освіти і науки України
Український державний університет науки і технологій
Кафедра інформаційних технологій і систем

ЗАТВЕРДЖУЮ
Перший проректор УДУНТ

Проф. _____Анатолій РАДКЕВИЧ

"_____" _____2022 р.

Програма навчальної дисципліни

Технології захисту інформації

Шифр та назва спеціальності	121 Інженерія програмного забезпечення
Назва освітньої програми (програм)	Інженерія програмного забезпечення у промисловості і бізнесі
Рівень вищої освіти	1-й (бакалаврський)
Статус дисципліни	Дисципліна фундаментальної підготовки, обов'язкова навчальна дисципліна
Форма навчання	денна

Види навчальної роботи та її обсяг в акад. годинах (денна форма навчання)

	Усього
Усього годин за навчальним планом	**90**
у тому числі: **Аудиторні заняття**	**40**
з них: - лекції	16
- лабораторні роботи	24
- практичні заняття	-
- семінарські заняття	-
Самостійна робота	**50**
у тому числі при : - підготовці до аудиторних занять	20
- підготовці до заходів модульного контролю	9
- виконанні курсових проектів (робіт)	0
- опрацюванні розділів програми, які не викладаються на лекціях	21
Семестровий контроль	середнє арифметичне 3-х модульних оцінок або іспит

Характеристика дисципліни

Мета вивчення дисципліни - Вивчення і освоєння студентами інструментів забезпечення кібербезпеки, методів криптографії, алгоритмів побудови процесів захисту інформації від несанкціонованого втручання та застосування протоколів організації технології захисту комп'ютерних систем.

Компетентності, формування яких забезпечує навчальна дисципліна

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (у тому числі кібербезпеки).
СК10. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.
СК12. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.
СК13. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

В результаті вивчення дисципліни студент повинен
знати:
- основні напрямки в кіберпросторі;
- типи і властивості методів криптографічного захисту інформації;
- обмеження та можливості використання алгоритмів захисту інформації;
- вимоги протоколів до організації технології захисту комп'ютерних систем для забезпечення крипостійкості.

вміти:
- проводити базовий аналіз системи на наявність вразливостей;
- проводити порівняльний аналіз властивостей криптографічних методів, алгоритмів захисту інформації від несанкціонованого втручання;
- застосування протоколи організації технології захисту комп'ютерних систем

Дисципліна забезпечує досягнення таких програмних результатів навчання:
ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.
ПР21. 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.

Заходи та методи оцінювання

Отримання позитивної оцінки при виконанні 3-х модульних контрольних робіт за 12-бальною шкалою.
Підсумкова оцінка навчальної дисципліни визначається як середнє арифметичне 3-х модульних оцінок за 12-бальною шкалою або іспитом.

Передумови вивчення дисципліни

Вивченню дисципліни має передувати вивчення дисциплін:
- вища математика;
- основи теорії інформації;
- програмування.

Структура дисципліни

Модуль та назва	Тема заняття	Обсяг, годин
Модуль 1.	**Лекції**	**6**
Основні інструменти захисту та атаки в кіберпросторі	1. Основи кібербезпеки	2
	2. Інструменти в кібербезпеці	2
	3. Способи та методи збезпечення кібербезпеки	2
	Лабораторні роботи	**8**
	1. Встановлення та налаштування оточення. Аналіз та використання наявних інструментів	8
	Самостійна робота	**16**
	1. Підготовка віртуальних машин	6
	Підготовка до аудиторних занять	7
	Підготовка до модульного контролю	3
	Усього:	**30**
Модуль 2.	**Лекції**	**6**
Криптографічний захист	1. Криптографія	2
	2. Інструменти захисту інформації	2
	3. Інструменти злому зашифрованої інформації	2
	Лабораторні роботи	**8**
	1. Аналіз зашифрованих даних та методи злому	8
	Самостійна робота	**16**
	1. Методи шифрування в сучасному кіберпросторі	6
	Підготовка до аудиторних занять	7

	Підготовка до модульного контролю	3
	Усього:	**30**
Модуль 3.	**Лекції**	**4**
Моделювання атак	1. Інструменти аналізу захищеності інформаційних систем	2
	2. Сучасні моделі атаки на інформаційні системи	2
	Лабораторні роботи	**8**
	1. Підготовка репорту захищеності інформаційної системи	8
	Самостійна робота	**18**
	1. Інструменти моделювання атак на інформаційні системи	9
	Підготовка до аудиторних занять	6
	Підготовка до модульного контролю	3
	Усього:	**30**

Рекомендована література

Основна література:

1. Джон Еріксон Злом: Мистецтво експлуатації., 2008. -488 с.
2. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. «Корнійчук" Киев. 2000.
3. Петраков А.В. Основы практической защиты информации. М. «Радио и связь».2000.

Укладач:
Старший викладач кафедри ІТС _____Тетяна ФЕНЕНКО

Завідувач кафедри інформаційних
технологій і систем (ІТС):
д.т.н., доц. _____ Вікторія ГНАТУШЕНКО

Робоча програма погоджена групою забезпечення якості освітньої програми «Інженерія програмного забезпечення у промисловості і бізнесі», спеціальність 121 «Інженерія програмного забезпечення» (Протокол №4/21-22 від 15 червня 2022 р.).

Гарант освітньої програми,
к.т.н, доц. _____ Тетяна СЕЛІВЬОРСТОВА

Погоджено:
Керівник навчального відділу _____ Володимир ПУЛЬПІНСЬКИЙ