МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЗАТВЕРДЖУЮ

Декан математичного факультету

_____ С.І. Гоменюк
(підпис) (ініціали та прізвище)

«_____»_____2021 р.

БЕЗПЕКА ТА ЖИВУЧІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ
РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки бакалавра
очної (денної) та заочної (дистанційної) форм здобуття освіти
спеціальності 126 – Інформаційні системи та технології
освітньо-професійна програма «Інформаційні системи та технології»

Укладач: Горбенко В.І., кандидат фізико-математичних наук, доцент, доцент кафедри програмної інженерії

Обговорено та ухвалено
на засіданні кафедри програмної інженерії

Протокол № від “ ” _____ 2021 р.
Завідувач кафедри

_____ А.О. Лісняк
(підпис) (ініціали, прізвище)

Ухвалено науково-методичною радою
математичного факультету

Протокол № від “ ” _____ 2021 р.
Голова науково-методичної ради
математичного факультету

_____ О.С. Пшенична
(підпис) (ініціали, прізвище)

Погоджено
з навчально-методичним відділом

_____ _____
(підпис) (ініціали, прізвище)

2021 рік

1. Опис навчальної дисципліни

<table>
<tr><th>1</th><th>2</th><th colspan="2">3</th></tr>
<tr><td rowspan="2">Галузь знань, спеціальність, освітня програма
рівень вищої освіти</td><td rowspan="2">Нормативні показники для планування і розподілу дисципліни на змістові модулі</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>очна (денна) форма здобуття освіти</td><td>заочна (дистанційна) форма здобуття освіти</td></tr>
<tr><td rowspan="2">Галузь знань
12 Інформаційні технології</td><td rowspan="2">Кількість кредитів – 5</td><td colspan="2">Обов’язкова</td></tr>
<tr><td colspan="2">Цикл професійної підготовки спеціальності</td></tr>
<tr><td rowspan="2">Спеціальність
126 Інформаційні системи та технології</td><td rowspan="2">Загальна кількість годин – 150</td><td colspan="2">Семестр:</td></tr>
<tr><td>7-й</td><td>7-й</td></tr>
<tr><td rowspan="4">Освітньо-професійна програма
Програмна інженерія</td><td rowspan="4">Змістових модулів – 8</td><td colspan="2">Лекції</td></tr>
<tr><td>28 год.</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>28 год.</td><td>–</td></tr>
<tr><td rowspan="3">Рівень вищої освіти:
бакалаврський</td><td rowspan="3">Кількість поточних контрольних заходів – 16</td><td colspan="2">Самостійна робота</td></tr>
<tr><td>94 год.</td><td>–</td></tr>
<tr><td colspan="2">Вид підсумкового семестрового контролю:
екзамен</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Безпека та живучість інформаційних систем» є оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв, комп’ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту програм, даних та інформаційних систем у цілому.

Основними **завданнями** вивчення дисципліни «Безпека та живучість інформаційних систем» є:

- отримання теоретичних знань щодо принципів побудови захисту інформаційних систем;
- ознайомитися із стандартами захисту програмного забезпечення, даних та інформаційних систем;
- набути навички щодо визначення рівня забезпечення захисту та живучості інформаційної системи;
- набути навички щодо класифікації джерел виникнення проблем з безпекою інформаційної системи;
- набути навички із використання методів захисту комп’ютерних мереж, програм та даних;
- навчитися планувати та реалізовувати заходи підвищення безпеки та живучості інформаційної системи.

У результаті вивчення навчальної дисципліни студент повинен набути таких результатів навчання (знання, уміння тощо) та компетентностей:

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
1	**2**
Програмні компетентності: – ІК Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в області інформаційних систем та технологій, або в процесі навчання, що характеризуються комплексністю та невизначеністю умов, які потребують застосування теорій та методів інформаційних технологій. – КЗ 2 Здатність застосовувати знання у практичних ситуаціях. – КЗ 3 Здатність до розуміння предметної області та професійної діяльності. – КЗ 7 Здатність розробляти та управляти проєктами. – КС 1 Здатність аналізувати об’єкт проєктування або функціонування та його предметну область. – КС 6 Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків. – КС 7 Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення. – КС 8 Здатність управляти якістю продуктів і сервісів інформаційних систем та технологій протягом їх життєвого циклу. – КС 15 Здатність забезпечувати інформаційну безпеку в інформаційних системах з використанням сучасних методів аутентифікації, формування політик прав доступу та шифрування.	Методи: Наочні методи (схеми, моделі, алгоритми). Словесні методи (лекція, пояснення, робота з підручником). Практичні методи (творчі завдання, контрольні, складання схем). Логічні методи (створення проблемної ситуації). Метод формування пізнавального інтересу (навчальна дискусія, створення цікавих ситуацій).
Програмні результати навчання – ПР 3 Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп’ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проєктування і використання	Методи контролю і самоконтролю (усний, письмовий, програмований, лабораторно-практичний). Самостійно-пошукові методи (індивідуальна робота, лабораторна робота). Контрольні заходи: – теоретичне тестування за змістовим модулем; – захист лабораторних робіт; – індивідуальне практичне

інформаційних систем та технологій. – ПР 5 Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій. – ПР 13 Використовувати методи захисту інформації в інформаційних системах. – ПР 14 Розробляти та забезпечувати вимоги щодо якості, надійності та живучості інформаційних систем.	розрахункове завдання (ІПРЗ); – залік.

Міждисциплінарні зв'язки. Курс «Безпека та живучість інформаційних систем» є логічним продовженням курсів «Захист інформації» та «Технології розробки програмного забезпечення». Набуті при вивченні даного курсу знання необхідні для подальшого вивчення курсів «Аналіз даних і прогнозування в інформаційних системах», «Менеджмент проектів програмного забезпечення» та «Надійність, стандарти та якість програмного забезпечення», а також для проведення дослідницької діяльності за галуззю підготовки.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття безпеки та живучості інформаційних систем

Актуальність забезпечення захисту та живучості інформаційних систем. Основні поняття інформаційної безпеки та захисту інформації. Класифікація загроз інформаційної безпеки. Базова модель безпеки інформаційних систем. Міжнародні та національні стандарти безпеки та живучості інформаційних систем.

Змістовий модуль 2. Безпека та живучість операційних систем

Проблеми безпеки операційних систем як основи інформаційних систем. Загрози безпеки та живучості операційних систем. Поняття захищеності операційної системи. Архітектура підсистеми захисту операційної системи. Типи захисту файлової системи операційної системи. Проблеми інформаційної безпеки операційних систем у мережі.

Змістовий модуль 3. Політика інформаційної безпеки

Основні поняття політики безпеки. Структура політики корпоративної інформаційної безпеки. Базова політика безпеки. Спеціалізовані політики безпеки. Процедури безпеки. Політики безпеки та її розробка. Компоненти архітектури безпеки. Концепції безпеки у мережі.

Змістовий модуль 4. Технології криптографічного захисту

Технології криптографічного захисту. Основні поняття та стандарти криптографічного захисту. Симетричні та асиметричні криптосистеми шифрування. Електроний цифровий підпис. Методи та протоколи управління криптоключами.

Змістовий модуль 5. Ідентифікація, аутентифікація та управління доступом до інформаційної системи

Контроль та адміністрування дій користувача інформаційної системи. Методи аутентифікації. Застосування карт та токенів. Криптографічні протоколи аутентифікації. Біометрична аутентифікація користувача. Управління доступом до інформаційної системи. Система входу Single Sign-On. Система входу Web SSO. Продукти SSO корпоративного рівня. Захист електронного документообігу.

Змістовий модуль 6. Безпека та живучість корпоративних інформаційних систем

Структура корпоративної інформаційної системи та джерела проблем її безпеки. Архітектура та основні характеристики хмарних сервісів. Багаторівневий підхід забезпечення інформаційної безпеки КІС. Операційні системи для КІС. Концепції захисту мережі КІС. Технології визначення вторгнення та його попередження. Концепції захисту комп'ютерів робочих місць у КІС.

Змістовий модуль 7. Технології та протоколи захищених мереж

Технології віртуальних захищених мереж. Протоколи захищених каналів. Протоколи захищеного передавання даних. Протоколи SSL та TLS. Захист віддаленого доступу. Захист бездротових мереж.

Змістовий модуль 8. Управління інформаційною безпекою

Задачі управління інформаційною безпекою. Глобальна та локальна політика безпеки. Функціювання системи управління інформаційною безпекою. Планування та управління інформаційною безпекою. Аудит та моніторинг безпеки корпоративних інформаційних систем. Міжмережеве екранування. Сучасні системи управління безпекою та живучістю інформаційних систем.

4. Структура навчальної дисципліни

Змістовий модуль	Усього годин	Аудиторні (контактні) години					Самостійна робота, год		Система накопичення балів		
		Усього годин	Лекційні заняття, год		Лабораторні заняття, год				Теор. зав-ня, к-ть балів	Практ. зав-ня, к-ть балів	Усього балів
			о/д ф.	з/дист ф.	о/д ф.	з/дист ф.	о/д ф.	з/дист ф.			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	16	8	4		4		8		4	4	8
2	14	6	2		4		8		4	4	8
3	14	6	4		2		8		3	4	7
4	16	8	4		4		8		3	4	7
5	14	6	4		2		8		4	4	8
6	14	6	2		4		8		3	4	7
7	16	8	4		4		8		4	4	8
8	16	8	4		4		8		3	4	7
Усього за змістові модулі	120	56	28		28		64		28	32	60
Підсумковий семестровий контроль **екзамен**	30						30	30	20	20	40
Загалом	**150**								**100**		

5. Теми лекційних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	**2**	**3**	**4**
1	1. Актуальність забезпечення захисту інформаційних систем	2	
1	2. Базова модель безпеки інформаційних систем	2	
2	3. Проблеми операційних систем як основи інформаційних систем	2	
3	4. Проблеми інформаційної безпеки мереж	2	
3	5. Політики безпеки та її розробка.	2	
4	6. Технології криптографічного захисту.	2	
4	7. Методи та протоколи управління криптоключами.	2	
5	8. Управління доступом до інформаційної системи.	2	
5	9. Захист електронного документообігу.	2	
6	10. Комплексний захист у корпоративних інформаційних системах	2	
7	11. Протоколи захищених каналів	2	
7	12. Захист віддаленого доступу	2	
8	13. Міжмережеве екранування	2	
8	14. Управління інформаційною безпекою	2	
Разом		**28**	–

6. Теми лабораторних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	**2**	**3**	**4**
1	1. Кодування та коригування помилок передавання інформації	4	
2	2. Стійкість парольного захисту електронних документів та архівів	4	
3	3. Протокол ARP та контроль адресації канального рівня	2	
4	4. Симетричні криптосистеми	4	
5	5. Використання хмарних сервісів у документообігу	2	
6	6. Дослідження безпеки ресурсів мережі	4	
7	7. Протоколи захищеного передавання даних	4	
8	8. Міжмережеве екранування	4	
Разом		**28**	–

7. Види і зміст поточних контрольних заходів

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
1	Самостійна робота 1	Звіт з виконання завдань самостійної роботи модулю за темою “Класифікація загроз інформаційної безпеки”	Оцінюється повнота виконання завдань	4
	Лабораторна робота 1	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра	Лабораторна робота оцінюється в 4 бали	4

		математичного факультету.		
Усього за ЗМ 1 контр. заходів	**2**			**8**
2	Самостійна робота 2	Звіт з виконання завдань самостійної роботи модулю за темою “Типи захисту файлової системи ОС”	Оцінюється повнота виконання завдань	4
	Лабораторна робота 2	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 бали	4
Усього за ЗМ 2 контр. заходів	**2**			**8**
3	Тест 1	Тестування з теоретичних питань змістових модулів 1-2	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,3 бали.	3
	Лабораторна робота 3	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 3 контр. заходів	**2**			**7**
4	Тест 2	Тестування з теоретичних питань змістових модулів 3-4	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,3 бали.	3
	Лабораторна робота 4	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 4	**2**			**7**

контр. заходів				
5	Самостійна робота 4	Звіт з виконання завдань самостійної роботи модулю за темою “Біометрична аутентифікація користувача”	Оцінюється повнота виконання завдань	4
	Лабораторна робота 5	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 5 контр. заходів	**2**			**8**
6	Тест 3	Тестування з теоретичних питань змістових модулів 5-6	Тестові питання оцінюються з ура-хуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,3 бали.	3
	Лабораторна робота 6	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 6 контр. заходів	**2**			**7**
7	Самостійна робота 4	Звіт з виконання завдань самостійної роботи модулю за темою “Концепція побудови віртуальних захищених мереж”	Оцінюється повнота виконання завдань	4
	Лабораторна робота 7	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 7 контр. заходів	**2**			**8**
8	Тест 4	Тестування з теоретичних питань змістових модулів 7-8	Тестові питання оцінюються з ура-хуванням вагових коефіцієнтів. Кількість питань у тесті – 10.	3

			Правильна відповідь оцінюється у 0,3 бали.	
	Лабораторна робота 8	Звіт з лабораторної роботи оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету.	Лабораторна робота оцінюється в 4 балів	4
Усього за ЗМ 8 контр. заходів	**2**			**7**
Усього за змістові модулі контр. заходів	**16**			**60**

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
Підсумковий контроль	Екзамен	Питання для підготовки: Захист та живучість ІС. Основні поняття ІБ та ЗІ. Класифікація загроз ІБ. Базова модель безпеки ІС. Міжнародні та національні стандарти безпеки та живучості ІС. Проблеми безпеки ОС. Загрози безпеки та живучості ОС. Поняття захищеності ОС. Архітектура підсистеми захисту ОС. Типи захисту файлової системи ОС. Проблеми ІБ ОС у мережі. Основні поняття політики безпеки. Структура політики корпоративної ІБ. Базова політика безпеки. Спеціалізовані політики безпеки. Процедури безпеки. Політики безпеки та її розробка. Компоненти архітектури безпеки. Концепції безпеки у мережі. Технології криптозахисту. Основні поняття та стандарти криптозахисту. Симетричні та асиметричні криптосистеми шифрування. Електроний цифровий підпис. Протоколи управління криптоключами. Ідентифікація, аутентифікація та управління доступом до ІС. Контроль та адміністрування дій користувача ІС. Методи аутентифікації.	Екзамен проводиться в усній формі при очній формі навчання. Підсумковий контроль містить два теоретичних питання та одне практичне завдання. За відповіді на теоретичні питання підсумкового контролю студент може отримати до 10 балів (за розгорнуту і правильну відповідь на одне питання до 5 балів), за правильне розв’язання завдання – до 10 балів, всього за екзамен можна отримати до 20 балів. У разі дистанційної форми навчання екзамен проходить у тестовій формі через платформу Moodle. Підсумковий тест складається із 20 тестових питань. Правильна відповідь оцінюється у 1 бал або всього за підсумковий тест можна отримати до 20 балів.	20

Підсумковий контроль	Екзамен	Застосування карт та токенів. Криптографічні протоколи аутентифікації. Біометрична аутентифікація користувача. Управління доступом до ІС. Система входу Single Sign-On. Система входу Web SSO. SSO корпоративного рівня. Захист електронного документообігу. Структура корпоративної ІС та джерела проблем її безпеки. Архітектура та основні характеристики хмарних сервісів. Багаторівневий підхід забезпечення інформаційної безпеки КІС. Операційні системи для КІС. Концепції захисту мережі КІС. Технології віртуальних захищених мереж. Протоколи захищених каналів. Протоколи захищеного передавання даних. Технології визначення вторгнення та його попередження. Концепції захисту комп'ютерів робочих місць у КІС. Задачі управління ІБ. Глобальна та локальна політика безпеки. Функціювання системи управління ІБ. Планування та управління ІБ. Аудит та моніторинг безпеки КІС. Міжмережеве екранування. Захист віддаленого доступу. Сучасні системи управління безпекою та живучістю ІС. Усна частина підсумкового контролю передбачає розгорнуту та обґрунтовану відповідь на два теоретичних питання (з письмовою фіксацією всіх відповідей) і розгорнуте розв'язання одного практичного завдання. У разі дистанційної форми навчання екзамен проходить у тестовій формі через платформу Moodle.		
	Практичне завдання: індивідуальне практичне розрахункове завдання (ІПРЗ)	Підсумкове практичне завдання або індивідуальне практичне розрахункове завдання (ІПРЗ) складається з комплексного завдання. Звіт по виконаному ІПРЗ оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету. Звіт з ІПРЗ захищається на заліковому тижні.	ІПРЗ складається з 2 завдань, за кожне з яких студент може отримати до 10 балів, з урахуванням відповідей на запитання при захисті звіту.	20
Усього за підсумковий семестровий контроль	**2**			**40**

9. Рекомендована література

Основна:

1 Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

2 Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації : навч. посіб. Харків : Вид. ХНЕУ, 2013. 476 с.

3 Єсін В.І., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій: навч. посіб. – Харків : ХНУ імені В. Н. Каразіна, 2013. 632 с.

4 Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. 222 p.

5 Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.

Додаткова:

1 Додонов О.Г. Живучість складних систем: аналіз та моделювання: навч. посіб. у 2-х ч. / О.Г. Додонов, М.Г. Кузнєцова, О.С. Горбачик. — К.: НТУУ «КПІ», 2009. — 264 с.

2 Колпаков В. В., Данькевич А. О., Корж А. П., Борзенкова С. В. Промислові комп'ютерні мережі: конспект лекцій для студентів напряму підготовки «Автоматизоване управління технологічними процесами» Київ: НТУУ «КПІ», 2016. 71 с.

3 Clinton D. Linux Security Fundamentals. Indianapolis : Wiley & Sons Inc. 2021. 175 p.

4 Математика: методичні вказівки до написання курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра та магістра математичного факультету / Гоменюк С. І., Гребенюк С. М., Зіновєєв І. В., Манько Н. І.-В., Спиця О. Г., Ткаченко І. Г. Запоріжжя: ЗНУ, 2017. 52 с.

Інформаційні ресурси

1 Наукова бібліотека Запорізького національного університету. URL: http://library.znu.edu.ua/

2 RFC. URL: https://www.ietf.org/standards/rfcs/