ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ФІТ
Савенко О.С.
5 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека та якість інформаційних систем і технологій

Назва

Галузь знань 12 – Інформаційні технології
Спеціальність 126 – Інформаційні системи та технології очна денна форма здобуття освіти
Освітня програма Інформаційні системи та технології
Статус дисципліни: обов'язкова, дисципліна професійної підготовки
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	4	7	4	120	51	17	34			69				+

Робоча програма складена на основі стандарту вищої освіти зі спеціальності 126 Інформаційні системи та технології, освітньо-професійної програми та навчального плану

Програма складена _____ Засорнова І.О.
Підпис Ініціали, прізвище викладача(ів)

Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол № 1 від 30 08 2023 р.

Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Говорущенко Т.О.
Підпис Ініціали, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради _____ Савенко О.С.
Підпис Ініціали, прізвище

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету_____ФІТ_____
_____Савенко О.С.___
_____ _____ 2023_ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека та якість інформаційних систем і технологій

Назва

Галузь знань 12 – Інформаційні технології
Спеціальність 126 – Інформаційні системи та технології очна денна форма здобуття освіти
Освітня програма Інформаційні системи та технології
Статус дисципліни: обов'язкова, дисципліна професійної підготовки
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	4	7	4	120	51	17	34			69				+

Робоча програма складена на основі стандарту вищої освіти зі спеціальності 126 Інформаційні системи та технології, освітньо-професійної програми та навчального плану

Програма складена _____ _____Засорнова І.О._____
Підпис Ініціали, прізвище викладача(ів)

Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол № _1___ від _30_ __08____ 2023 р.

Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Говорущенко Т.О.
Підпис Ініціали, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради _____ _____Савенко О.С._____
Підпис Ініціали, прізвище

Хмельницький 2023

ВСТУП

Мета викладання дисципліни. Дисципліна «Безпека та якість інформаційних систем і технологій» є однією зі спеціальних профілюючих дисциплін і тому займає провідне місце у підготовці бакалаврів інформаційних систем та технологій.

Метою дисципліни «Безпека та якість інформаційних систем і технологій» є ознайомлення студентів із основними поняттями, технологіями та підходами щодо забезпечення якості та безпеки інформаційних систем, а також надання їм знань і умінь використання та впровадження отриманих знань на практиці.

Предмет дисципліни. Методи, засоби та технології забезпечення безпеки та якості інформаційних систем і технологій.

Завдання дисципліни. Надати студентам знання і практичні навички із забезпечення безпеки та якості інформаційних систем і технологій.

Після вивчення дисципліни «Безпека та якість інформаційних систем і технологій» студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

знати:

- об’єкт, предмет, задачі, проблематику дисципліни та її основні розділи;
- механізми проникнення зловмисного програмного забезпечення та протидію цим процесам, вразливості інформаційних систем та технологій;
- методи та засоби тестування програмної складової інформаційних систем для забезпечення якості;
- принципи побудови та використання програмних засобів та технологій для забезпечення безпеки та якості програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах.

уміти:

- застосовувати, впроваджувати та експлуатувати сучасні інформаційні технології та системи у різних галузях людської діяльності, національної економіки та виробництва, розробляти принципи політики безпеки в інформаційно-комунікаційних системах;
- проводити аналіз безпеки комп’ютерної системи або мережі;
- вибирати, проектувати, розгортати, інтегрувати, управляти, адмініструвати та супроводжувати застосування комунікаційних мереж, сервісів та інфраструктури організації; самостійно класифікувати загрози інформації та оцінювати її вразливість;
- застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення.

бути здатним:

- використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення і розгортання 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 оцінки якості та тестування програмного забезпечення інформаційних систем, а також для забезпечення безпеки ІСТ.
- проводити системний аналіз об’єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів циркулювання інформації в ІСТ з огляду на забезпечення інформаційної безпеки;
- демонструвати знання сучасного рівня та новітніх технологій в області безпеки ІСТ з метою їх запровадження у професійної діяльності;
- демонструвати знання і практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ для розв’язання задач проектування інформаційних систем та підвищення рівня безпеки зберігання інформації;
- обґрунтовувати вибір технічної структури з урахування політики безпеки та розробляти відповідне програмне забезпечення, що входить до складу ІСТ.

Компетентності, на формування яких спрямовано ОК:

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.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Здатність до розуміння предметної області та професійної діяльності.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК13. Здатність спілкуватися державною мовою з професійних питань як усно, так і письмово

ЗК14. Здатність розв’язувати поставлені задачі та приймати відповідні рішення; виявляти, ставити та вирішувати проблеми.

ФК6. 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.

ФК7. Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення.

ФК8. Здатність управляти якістю продуктів і сервісів інформаційних систем та технологій протягом їх життєвого циклу.

ФК20. Здатність організовувати збір та зберігання даних у базах та сховищах даних, захист інформації в інформаційних системах та технологія.

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН3. 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 інформаційних систем та технологій.

ПРН4. Проводити системний аналіз об’єктів проєктування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.

ПРН5. 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.

ПРН14. Адмініструвати, використовувати, адаптувати та експлуатувати наявні і новітні інформаційні системи та технології, а також комп’ютерні системи та мережі із забезпеченням захисту інформації з метою реалізації встановленої політики інформаційної безпеки

ПРН15. Оцінювати отримані результати та аргументовано захищати прийняті рішення; усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення; якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

БЕЗПЕКА ТА ЯКІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	7
Кількість встановлених кредитів ЄКТС	4
Форма здобуття освіти	Очна денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: 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 інформаційних систем та технологій; проводити системний аналіз об'єктів проєктування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях; 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; адмініструвати, використовувати, адаптувати та експлуатувати наявні і новітні інформаційні системи та технології, а також комп'ютерні системи та мережі із забезпеченням захисту інформації з метою реалізації встановленої політики інформаційної безпеки; оцінювати отримані результати та аргументовано захищати прийняті рішення; усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення; якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Зміст навчальної дисципліни. Поняття якості інформаційних систем. Дефекти. Методи та засоби тестування програмного забезпечення для забезпечення якості інформаційних систем. Системи відслідковування помилок та життєвий цикл дефекту. Поняття безпеки інформаційних систем. Тестування продуктивності інформаційної веб-системи. Загрози безпеці ІС. Модель порушника. Базові системи захисту, рівні інформаційно-комунікаційної системи. Типові вразливості систем та причини їх появи. Шкідливе програмне забезпечення як засоби несанкціонованого доступу. Основи безпеки інформації в комп'ютерних мережах. Засоби захисту в розподілених та веб-орієнтованих інформаційно-комунікаційних системах. Використання Honeypot-приманок для аналізу впливів спрямованих на порушення безпеки інформаційної системи в мережі. Вбудовані засоби забезпечення безпеки інформаційної системи, засоби міжмережевого екрану netfilter. Блокування атак відмова в обслуговуванні. Середовище контейнеризації Docker для сервера LEMP. Docker Compose. Сканування вразливостей хоста за допомогою Docker Bench.

Запланована навчальна діяльність: лекції – 17 год., лабораторні заняття – 34 год., самостійна робота – 69 год.; разом – 120 год.

Методи навчання: методи проблемного викладання, словесні, наочні (лекції); пояснювально-ілюстративні, дослідницькі, частково-пошукові, проблемного викладання (лабораторні заняття), проблемного викладання, практичні, дослідницькі, частково-пошукові (самостійна робота: індивідуальні завдання).

Форми оцінювання результатів навчання: захист лабораторних робіт, тестування, підсумковий контрольний захід.

Форма семестрового контролю: іспит

Навчальні ресурси:

1. Якість та тестування інформаційних систем. Навчальний посібник для самостійної роботи студентів вищих навчальних закладів. Київ: ННІІТ ДУТ, 2020. –128 с.
2. Проектування інформаційних систем: Загальні питання теорії проектування ІС (конспект лекцій) [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського; уклад.: О. С. Коваленко, Л. М. Добровська. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 192с.
3. Cybersecurity and Secure Information Systems. Challenges and Solutions in Smart Environments / A. E. Hassanien, M. Elhoseny, Springer Cham, 2019. – p. 314.
4. MOODLE Learning Platform. Web page: https://msn.khnu.km.ua.
5. University Electronic Library. Web page: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: кандидат технічних наук, доцент Нічепорук А.О.

1. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:		
	Денна форма		
	Лекції	Лабораторні роботи	СРС
Тема 1. Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем	8	16	36
Тема 2. Методи, засоби та технології забезпечення безпеки інформаційних систем	9	18	33
Разом за семестр:	**17***	**34**	**69**

Примітка. * по чисельнику – 18 годин, по знаменнику – 16 годин (розрахунок здійснюється відповідно до розкладу занять)

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем		
1	**Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем** Основні поняття та визначення комп'ютерних систем. Сучасний стан розвитку комп'ютерних систем. Якість інформаційних систем. Дефектологічні властивості ІСТ: дефектогенність, дефектабельність та дефектоскопічність. Модель класифікації критеріїв якості інформаційних систем. Тестування програмного забезпечення для інформаційних систем Основні терміни та поняття. Поняття бага, його атрибути. Тестування та мета тестування. Верифікація та валідація. Системи відслідковування помилок та життєвий цикл дефекту. Життєвий цикл дефекту. Літ.: [1, 2, 11]	2
2	**Види тестування програмного забезпечення для інформаційних систем** Види тестування програмного забезпечення для інформаційних систем: функціональне, навантажувальне, зручності використання, тестування білого та чорного ящика, регресійне тестування. Рівні тестування програмного забезпечення: модульне, інтеграційне та системне тестування. Літ.: [1, 2, 11]	2
3	**Тестування веб-орієнтованих інформаційних систем** Поняття про тестування веб-орієнтованих інформаційних систем та основні підходи до тестування веб-додатків. Етапи тестування. Чек-листи та правила їх складання. Літ.: [1, 2, 11]	2
4	**Забезпечення якості інформаційних систем. Стандарти та метрики якості інформаційних систем** Стандарти якості інформаційних систем, ISO9000, ISO 9126. Метрики якості інформаційних систем: метрики за тестовими випадками, метрики за багами/дефектами, метрики за задачами, юзабіліті метрики, метрики Kanban, метрики SCRUM. Валідація і верифікація [1, 11]	2
Тема 2. Методи, засоби та технології забезпечення безпеки інформаційних систем		
5	**Поняття безпеки інформаційних систем. Загрози безпеці ІС. Модель порушника** Поняття про інформаційну та інформаційно-телекомунікаційну системи. Політика безпеки. Цілісність, конфіденційність та доступність інформації. Резильєнтність та захищеність інформаційних систем. Завдання захисту та загрози безпеці інформації. Загроза, атака, вразливість, порушник, точка проникнення. Модель порушника. Класифікація загроз. Перелік типових загроз безпеці. Літ.: [2,4,10,12,13]	2
6	**Базові системи захисту** Рівні інформаційно-комунікаційної системи: рівені мережі, операційних систем, систем керування базами даних та прикладного програмного забезпечення. Структура інформаційно-комунікаційної системи. Несанкціонований доступ. Функціональні сервіси безпеки та їх механізми.	2

	Механізми захисту на різних рівнях ІКС. Основні підсистеми комплексу засобів захисту. Літ.: [2,4,10,12,13]	
7	**Проєктування ІС із врахуванням відмовостійкості. Типові вразливості систем та методи забезпечення відмовостійкості спеціалізованих інформаційних систем** Передумови виникнення вразливостей у комп'ютерних системах. Класифікація вад захисту. Помилки програмної реалізації системи. Люки. Переповнення буфера. Проєктування ІС із врахуванням впливу зловмисного програмного забезпечення та кібератак, методи забезпечення відмовостійкості спеціалізованих інформаційних, системи перехресне резервування, резерв часу та надлишковість продуктивності роботи, блокові мітки, структурне взаєморезервування клієнтської та серверної частин ІС. Літ.: [2,9,10,12,13]	2
8	**Методи забезпечення живучості та захисту інформації в спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення** Поняття живучості та резельєнтності ІС. Метод забезпечення живучості спеціалізованих ІТ в умовах впливів ЗПЗ та комп’ютерних атак з використанням параметричного контролю актуальності модулів ПЗ клієнтських АРМ та їх маскуванням. Забезпечення захисту інформації спеціалізованих інформаційних технологій в умовах впливів ЗПЗ Літ.: [2,9,10,12,13]	2
9	**Основи безпеки інформації в комп‘ютерних мережах** Модель взаємодії відкритих систем. Стеки протоколів. Загрози безпеці інформації у мережах. Безпека взаємодії відкритих систем. Автентифікація. Керування доступом. Конфіденційність даних. Співвідношення сервісів безпеки і рівнів моделі ISO. Цифровий підпис. Керування маршрутом Літ.: [2,4,10,12,13]	2
	Разом за семестр:	18/16*

Примітка. * по чисельнику – 18 годин, по знаменнику – 16 годин (розрахунок здійснюється відповідно до розкладу занять)

2.2 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кількість годин
1	Тестування веб-орієнтованих систем. Складання звітів про помилки. Літ.: [1, 9-11]	4
2	Тестування зручності використання та кросбраузерне тестування веб-орієнтованих інформаційних систем. Літ.: [1, 9-11]	4
3	Модульне тестування програмного забезпечення для забезпечення якості інформаційних систем. Літ.: [1, 9-11]	4
4	Модульне тестування програмного забезпечення інформаційних систем із використання Test doubles об’єктів. Літ.: [1, 9-11]	4
5	Оцінка якості інформаційних систем. Тестування продуктивності інформаційної веб-системи. Літ.: [1, 2, 8-12]	4
6	Дослідження та перевірка безпеки інформаційної системи у мережі. Створення Honeypot-приманок для аналізу впливів спрямованих на порушення безпеки інформаційної системи в мережі. Літ.: [2-7]	4
7	Забезпечення безпеки інформаційної системи засобами міжмережевого екрану netfilter через утиліту iptables. Блокування атак відмова в обслуговуванні Літ.: [2-7]	4
8	Проектування ІС із врахуванням відмово стійкості. Налаштування середовища контейнеризації Docker для сервера LEMP. Docker Compose. Сканування вразливостей хоста за допомогою Docker Bench. Літ.: [2,4,10,12,13]	4
9	Підсумкове заняття	2
	Разом за семестр	34

2.3 Зміст самостійної (індивідуальної) роботи

Самостійна робота студентів денної форми навчання полягає у систематичному опрацюванні програмного матеріалу, підготовці до виконання і захисту лабораторних робіт, тестування з теоретичного матеріалу, тощо.

Номер тижня	Вид самостійної роботи	К-ть годин
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	4
2	Підготовка до захисту лабораторної роботи №1	4
3	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2.	4
4	Підготовка до захисту лабораторної роботи №2	4
5	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3.	4
6	Підготовка до захисту лабораторної роботи №3	4
7	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4.	4
8	Підготовка до захисту лабораторної роботи №4.	4
9	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5.	4
10	Підготовка до захисту лабораторної роботи №5.	4
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6.	4
12	Підготовка до захисту лабораторної роботи №6.	4
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7.	4
14	Підготовка до захисту лабораторної роботи №7	4
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8.	4
16	Підготовка до захисту лабораторної роботи №8	4
17	Підготовка до підсумкового контрольного заходу	5
	Разом за семестр:	69

3. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами, наочними з використанням інформаційних технологій, а також з використанням методів проблемного навчання. Лабораторні заняття проводяться з використанням методів пояснювально-ілюстративних з використанням інформаційних технологій, проблемного викладання, дослідницьких, і мають за мету – набуття студентами практичних навичок. Самостійна робота передбачає виконання індивідуальних завдань, при розв'язанні яких застосовуються методи проблемного викладання, практичних та дослідницьких методів.

4. ФОРМИ І МЕТОДИ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Поточний контроль здійснюється під час лекційних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі *іспиту*. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

Кожний вид роботи з дисципліни оцінюється за *чотирибальною* шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав залік, вважається невстигаючим.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни і робочим навчальним планом.

Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. За несвоєчасний захист лабораторної роботи з неповажної причини студент за позитивну відповідь отримує оцінку «задовільно».

На тестування відводиться 20 хвилин. Тестування проводиться з використанням модульного середовища для навчання MOODLE. Правильні відповіді студент реєструє в он-лайн режимі в модульному середовищі MOODLE. Через 20 хвилин студенти завершують тестування та надсилають свої відповіді на сервер. Викладач оголошує результати тестування згідно журналу оцінок модульного середовища MOODLE.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку «відмінно», за шкалою ЄКТС – А, отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв'язувати теорію з практикою, вирішувати практичні та дослідницькі завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із застосовування, впровадження та експлуатування сучасних інформаційних технології та системи у різних галузях людської діяльності, національної економіки та виробництва, розробляти принципи політики безпеки в інформаційно-комунікаційних системах. Оцінка «відмінно», за шкалою ЄКТС – А, виставляється студенту, який глибоко засвоїв принципи побудови та використання програмних засобів та технологій для забезпечення безпеки та якості програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах

Оцінку «добре», за шкалою ЄКТС – В, отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку «добре», за шкалою ЄКТС – C, отримує студент за правильну відповідь з однією суттєвою помилкою.

Оцінки «задовільно», за шкалою ЄКТС – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок із застосування методів, засобів та технологій забезпечення безпеки та якості інформаційних систем. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки «задовільно», за шкалою ЄКТС – E, заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички із використання та розробки комп'ютерних та кіберфізичних систем.

Оцінка «незадовільно», за шкалою ЄКТС – FX, виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється студенту, який не може продовжити навчання без додаткових знань з курсу.

Оцінка «незадовільно», за шкалою ЄКТС – F, виставляється студенту за повне незнання і нерозуміння навчального матеріалу або відмову від відповіді і передбачає повторне навчання студента з дисципліни.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

<table>
<tr><td colspan="8">Аудиторна робота</td><td>Самостійна, індивідуальна робота</td><td>Форма семестрового контролю</td></tr>
<tr><td colspan="10">7 семестр</td></tr>
<tr><td colspan="8">Лабораторні роботи №:</td><td>Тестовий контроль:</td><td>Іспит</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>ТК</td><td></td></tr>
<tr><td colspan="8">ВК: 0,5</td><td>0,1</td><td>0,4</td></tr>
</table>

Примітка: ТК – тестовий контроль; ВК – ваговий коефіцієнт;

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені у наступній таблиці.

Перехід від інституційної шкали оцінювання до європейської (ЄКТС)

Оцінка ECTS	**Інституційна шкала балів**	**Інституційна оцінка**		**Критерії оцінювання**
A	4,75-5,00	5	Зараховано	**Відмінно** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків.
B	4,25-4,74	4		**Добре** – повне знання навчального матеріалу з кількома незначними помилками.
C	3,75-4,24	4		**Добре** – в загальному правильна відповідь з двома-трьома суттєвими помилками.
D	3,25-3,74	3		**Задовільно** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією.
E	3.00-3,24	3		**Задовільно** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00-2,99	2	Незараховано	**Незадовільно** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1,99	2		**Незадовільно** – необхідна серйозна подальша робота і повторне вивчення дисципліни.

5. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

1. Охарактеризуйте поняття якості інформаційної системи;
2. Відомі показники та метрики оцінки якості інформаційних систем;
3. Види тестування програмного забезпечення інформаційних систем;
4. Різновиди тестування продуктивності системи;
5. Поясніть різницю між термінами «автоматизована система», «інформаційно-комунікаційна система».
6. Основні особливості процесів ідентифікації та автентифікації.
7. На порушення яких властивостей інформації та системи спрямована загроза прослуховування трафіку?
8. Назвіть загрози, які розглядаються в моделі STRIDE.
9. Які з наявних способів реалізації загрози розглядаються в моделі загроз?
10. Модель порушника: особливості побудови.
11. Назвіть типові рівні інформаційно-комунікаційної системи.
12. Дайте визначення функціонального сервісу безпеки.
13. Які механізми захисту впроваджують на рівні захисту від НСД до ресурсів системи?
14. Які механізми захисту впроваджують на рівні захисту від несанкціонованого використання ресурсів системи?
15. Які механізми захисту впроваджують на рівні захисту від некоректного використання ресурсів системи?
16. Які механізми захисту впроваджують на рівні внесення інформаційної та функціональної надлишковості?
17. Який рівень захисту забезпечує захист конфіденційності інформації?
18. Яке завдання виконує підсистема ідентифікації та автентифікації?
19. Назвіть основні причини появи вразливостей у сучасних інформаційно- комунікаційних системах.
20. На яких етапах життєвого циклу ІКС можуть виникати вади захисту? Охарактеризуйте типові вади для кожного з етапів.
21. За якими головними ознаками доцільно класифікувати шкідливе програмне забезпечення?
22. Які класи шкідливого програмного забезпечення можна виділити за механізмами їх розповсюдження?
23. Що таке програмні закладки? Наведіть класифікацію програмних закладок.
24. Яким чином може здійснюватися керування ботнетом?
25. Які головні ознаки мають комп'ютерні віруси?
26. Наведіть класифікацію комп'ютерних вірусів.
27. У чому полягає особлива небезпека завантажувальних (бутових) вірусів?
28. Назвіть основні технології виявлення комп'ютерних вірусів. Які переваги й недоліки має кожна з цих технологій?
29. Які головні ознаки мережних хробаків, що вирізняють їх з-поміж інших шкідливих програм?
30. За якими ознаками класифікують мережних хробаків?
31. Назвіть стратегії проникнення на віддалені комп'ютери, які реалізовував хробак Морріса.
32. Які програмні засоби дістали назву «троянські коні»? Наведіть їх класифікацію.
33. Які програми можуть належати до спеціальних хакерських утиліт?
34. Що таке відкриті системи і які вони мають переваги?
35. Назвіть відомі Вам стеки мережних протоколів, і розкажіть про їх призначення.
36. Які проблеми безпеки можуть виникнути через протокол FTP?
37. Які засоби контролю і захисту сесії впроваджено у протоколі TCP?
38. Як реалізовано передбачення номерів TCP-послідовності, і для чого це використовують?
39. У чому полягає атака IP spoofing і як їй можна запобігти?
40. Які помилки оброблення фрагментованих пакетів можна було зустріти в мережних ОС і до

яких наслідків призводило використання цих помилок?
41. Сформулюйте вимоги до архітектури захищених мереж.
42. Які топології мереж сприяють побудові захищених мереж, а які - ні?
43. У який спосіб створюють віртуальні локальні мережі?
44. На яких рівнях мережної взаємодії можна реалізовувати міжмережні екрани?
45. Які переваги мають пакетні фільтри?
46. Наведіть приклад шлюзу мережного рівня.
47. Які переваги мають шлюзи прикладного рівня?
48. Назвіть основні способи обходу мережних екранів.
49. Мережні екрани якого рівня дають змогу застосовувати трансляцію мережних адрес?
50. Назвіть три складові технології виявлення атак.
51. Які основні методи аналізу даних для пошуку атак?
52. Що таке сканер безпеки? Які принципи його роботи?
53. Дайте визначення VPN. Які завдання захисту вирішує VPN?
54. Де можуть бути розміщені кінцеві точки захищених тунелів? Назвіть переваги й недоліки всіх варіантів.
55. На яких рівнях моделі OSI можна реалізувати VPN? Назвіть переваги й недоліки всіх варіантів.
56. У яких випадках найчастіше використовують протокол SSL/TLS?

6. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Якість та тестування інформаційних систем. Навчальний посібник для самостійної роботи студентів вищих навчальних закладів. Київ: ННІІТ ДУТ, 2020. –128 с.
2. Проектування інформаційних систем: Загальні питання теорії проектування ІС (конспект лекцій) [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського; уклад.: О. С. Коваленко, Л. М. Добровська. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 192с.
3. Cybersecurity and Secure Information Systems. Challenges and Solutions in Smart Environments / A. E. Hassanien, M. Elhoseny, Springer Cham, 2019. – p. 314.
4. Єсін В.І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х.: ХНУ імені В. Н. Каразіна, 2013. – 632 с. ISBN 978-966-623-927-6.
5. Chapple M. CISSP Certified Information Systems Security Professional / M. Chapple, D. Seidl, J. Michael Stewar, D. Gibson. – Sybex, 2018. – 1616 p.
6. Kim D. Fundamentals of Information Systems Security 3rd Edition / D. Kim, M.G. Solomon. – Jones & Bartlett Learning, 2016. – 571 p.
7. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. – Broadway Books, 2015. – 448 p.
8. Solomon M.G. Fundamentals of Communications and Networking / M.G. Solomon, D. Kim, J.L. Carrell. – Jones & Bartlett Learning, 2014. – 512 p.
9. Azad S. Practical Cryptography: Algorithms and Implementations Using C++ 1st Edition / S. Azad, A.K. Pathan. – Auerbach Publications, 2014. – 365 p.
10. Mayer-Schönberger V. Big Data: A Revolution That Will Transform How We Live, Work, and Thin / V. Mayer-Schönberger, K. Cukier. – Eamon Dolan.Mariner Books, 2014. – 272 p.
11. Antoniou J. Quality of Experience and Learning in Information Systems / J. Antoniou, Springer Cham, 2019. – 110 p.
12. Стецюк М.В. Архітектура спеціалізованих інформаційних систем з врахуванням вимог живучості та відмовостійкості в умовах впливів зловмисного програмного забезпечення / В.М. Стецюк, А.С. Каштальян, В.І. Грибинчук // Вимірювальна та обчислювальна техніка в технологічних процесах. - №2. - 2020 - С. 69-77.
13. Стецюк М.В. Метод забезпечення захисту інформації в спеціалізованих інформаційних технологіях при впливах зловмисного програмного забезпечення / В.М. Стецюк // Вимірювальна та обчислювальна техніка в технологічних процесах. - №2. – 2021. - С.57-68.

8. ІНФОРМАЦІЙНІ РЕСУРСИ

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань).
2. Електронна бібліотека університету