

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету ФІТ



Тетяна ГОВОРУЩЕНКО
Ім'я, ПРІЗВИЩЕ

2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека та якість інформаційних систем і технологій
Назва дисципліни

Галузь знань – 12 Інформаційні технології
Спеціальність – 126 Інформаційні системи та технології
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Інформаційні системи та технології
Обсяг дисципліни – 5 кредитів ЄКТС, **Шифр дисципліни** – ОПП.11
Мова навчання – українська
Статус дисципліни: обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

| Форма здобуття освіти | Курс | Семестр | Загальний обсяг | | Кількість годин | | | | | | Курсовий проект* | Курсова робота | Форма семестрового контролю | | |
|-----------------------|------|---------|-----------------|------------|-----------------|-------------------|--------------------|-------------------|---------------------|-------------------------------|------------------|----------------|-----------------------------|-------|----------|
| | | | Кредити ЄКТС | Години | Разом | Аудиторні заняття | | | | Самостійна робота, у т.ч. ІРС | | | Залік | Іспит | |
| | | | | | | Лекції | Лабораторні роботи | Практичні заняття | Семінарські заняття | | | | | | |
| Д | 4 | 7 | 5 | 150 | 98 | 16 | 32 | | | | 70 | | | | + |
| Разом ДФН | | | 5 | 150 | 98 | 16 | 32 | | | | 70 | | | | 2 |

Примітка. З навчальної дисципліни передбачений курсовий проект, зміст та вимоги до виконання якого регулюються відповідними методичними рекомендаціями.

Робоча програма складена на основі освітньо-професійної програми «Інформаційні системи та технології» за спеціальністю 126 «Інформаційні системи та технології»

Робоча програма складена  Віталій АЛЕКСЕЙКО
Підпис автора(ів) Науковий ступінь, вчене звання, ім'я, ПРІЗВИЩЕ автора(ів)

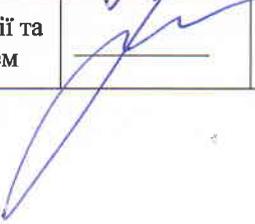
Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол від 18.08 2025 № 1 Зав. кафедри  Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету  Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

ЛИСТ ПОГОДЖЕННЯ

| Посада | Назва кафедри | Підпис | Ініціали, прізвище |
|----------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------|--------------------|
| Завідувач кафедри, д-р. філософії, доц. | Комп'ютерної інженерії та інформаційних систем |  | Ольга ПАВЛОВА |
| Гарант освітньо-професійної програми, д-р, техн.наук, професор | Комп'ютерної інженерії та інформаційних систем |  | Єлизавета ГНАТЧУК |

3. Пояснювальна записка

Дисципліна «Безпека та якість інформаційних систем і технологій» є однією з обов'язкових дисциплін фахової підготовки здобувачів першого (бакалаврського) рівня вищої освіти, які навчаються за освітньо-професійною програмою «Інформаційні системи та технології».

Пререквізити – Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека (ОЗП.05), Системне програмне забезпечення (ОФП.07), Комп'ютерна логіка (ОФП.17), Інформаційні технології (ОФП.19), Смарт-технології та Інтернет речей (ОФП.09), Смарт-технології та Інтернет речей (курсний проєкт) (ОФП.10), Системне програмне забезпечення (курсний проєкт) (ОФП.08).

Кореквізити – Переддипломна практика (ОФП.22), Кваліфікаційна робота (ОФП.23).

Відповідно до освітньої програми, дисципліна сприяє забезпеченню:

компетентностей: 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.

програмних результатів навчання: 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 проектування і використання інформаційних систем та технологій. ПРН4. Проводити системний аналіз об'єктів проектування 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.

Мета 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.

Результати навчання. Студент, 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 проектування і використання інформаційних систем та технологій; проводити системний аналіз об'єктів проектування 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 Nonepot-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

4. Структура залікових кредитів дисципліни

| Назва розділу (теми) | Кількість годин, відведених на: | | |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---------------------|-----------|
| | лекції | лабораторні заняття | СРС |
| Тема 1. Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем. | 8 | 16 | 35 |
| Тема 2. Методи, засоби та технології забезпечення безпеки інформаційних систем. | 8 | 16 | 35 |
| Разом за семестр: | 16 | 32 | 70 |

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

| Номер лекції | Перелік тем лекцій, їх анотації | Кількість годин |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <i>Тема 1. Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем</i> | | |
| 1 | Лекція №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, 4] | 2 |
| 2 | Лекція №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, 5] | 2 |
| 3 | Лекція №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, 5] | 2 |
| 4 | Лекція №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 Літ.: [1, 5, 6] | 2 |
| <i>Тема 2. Методи, засоби та технології забезпечення безпеки інформаційних систем</i> | | |
| 5 | Лекція №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. Класифікація загроз. Перелік типових загроз безпеці. Літ.: [1, 4, 5, 6] | 2 |
| 6 | Лекція №6. Базові системи захисту. Рівні інформаційно-комунікаційної системи: рівні мережі, операційних систем, систем керування базами даних та прикладного програмного забезпечення. Структура інформаційно-комунікаційної системи. Несанкціонований доступ. Функціональні сервіси безпеки та їх механізми. Механізми захисту на різних рівнях ІКС. Основні підсистеми комплексу засобів захисту. Літ.: [2, 3] | 2 |
| 7 | Лекція №7. Проектування 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. Проектування ІС із врахуванням впливу зловмисного програмного забезпечення та кібератак, методи забезпечення відмовостійкості спеціалізованих інформаційних систем, системи перехресне резервування, резерв часу та надлишковість продуктивності роботи, блокові мітки, структурне взаєморезервування клієнтської та серверної частин ІС. Літ.: [2, 4] | 2 |
| 8 | Лекція №8. 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.: [3, 5, 6] | 2 |

5.3 Зміст лабораторних занять

| № п/п | Тема лабораторного заняття | Кількість годин |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 1 | Ознайомлення з інтерфейсом середовищ Jira, ClickUp та їх базової структури. Навігація та організація інформації. Пошук та документування багів. Літ.: [1, 4, 6]. | 4 |
| 2 | Тестування веб-орієнтованих систем. Складання звітів про помилки. Літ.: [1, 5] | 4 |
| 3 | Тестування зручності використання та кросбраузерне тестування веборієнтованих інформаційних систем. Літ.: [4, 5] | 4 |
| 4 | Тестування мобільних застосунків. Літ.: [4, 5] | 4 |
| 5 | Тест-дизайн та тест-кейси. Літ.: [1, 6]. | 4 |
| 6 | Тест-плани. Літ.: [1, 3, 6]. | 4 |
| 7 | Тестування комп'ютерних ігор. Літ.: [2, 6]. | 4 |
| 8 | Ролі у процесі розробки та тестування ПЗ. комунікації у сфері тестування Літ.: [1, 2, 5]. | 4 |
| Разом: | | 32 |

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до лабораторних занять. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

| № п/п | Теми самостійної роботи | Кількість годин |
|-----------------|-------------------------------------------------------------------------|-----------------|
| 1 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1. | 10 |
| 2 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2. | 8 |
| 3 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3. | 8 |
| 4 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4. | 8 |
| 5 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5. | 8 |
| 6 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6. | 8 |
| 7 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7. | 8 |
| 8 | Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8. | 12 |
| Загалом: | | 70 |

6. Технології та 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.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- Підсумкова контрольна робота.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, **не допускається** до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який **має** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до практичних занять (вивчення теоретичного матеріалу з теми), активно працювати на занятті, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами завдань тощо; до лабораторного заняття (вивчення теоретичного матеріалу з теми роботи, активно працювати на занятті, якісно підготувати звіт, захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті). Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час лабораторних занять та підсумкової контрольної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності **не допускаються**.

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

| Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей | Узагальнений зміст критерія оцінювання |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Відмінно (високий) | Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві <i>помилки</i> . |
| Добре (середній) | Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три <i>несуттєві помилки</i> . |
| Задовільно (достатній) | Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і <i>суттєві помилки</i> у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді. |
| Незадовільно (недостатній) | Здобувач вищої освіти виявив 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 здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни. |

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі

| Аудиторна робота | | | | | | | | Семестровий контроль | |
|-------------------------------------------------------------|-----|-----|-----|-----|-----|-----|-----|----------------------|---------------|
| Лабораторні роботи №: | | | | | | | | Іспит | Разом балів |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | |
| Кількість балів за вид навчальної роботи (мінімум-максимум) | | | | | | | | | |
| 4-7 | 4-7 | 4-7 | 4-7 | 4-7 | 4-7 | 4-7 | 4-7 | 28-44 | 60-100 |
| 32-56 | | | | | | | | 28-44 | 60-100 |

Примітки: *За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; повнота відповіді та знання; дотримання вимог при оформленні результатів.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому *не зараховується* і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

| Види завдань | Для кожного окремого виду завдань | | |
|-------------------------------------------------------------------|------------------------------------------|---------------------------------------------------|---------------------------------------|
| | Мінімальний (достатній) бал (задовільно) | Потенційні позитивні бали* (середній бал) (добре) | Максимальний (високий) бал (відмінно) |
| Теоретичне питання №1 (складається з 2-х частин по 7 балів кожна) | 10 | 12 | 14 |
| Практичне завдання (2 завдання по 15 балів) | 18 | 24 | 30 |
| Разом: | 28 | 36 | 44 |

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

| Оцінка ЄКТС | Рейтингова шкала балів | Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни) | |
|-------------|------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Залік | Іспит/диференційований залік |
| A | 90-100 | Зарахован | <i>Відмінно/Excellent</i> – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом |
| B | 83-89 | | <i>Добре/Good</i> – середній (максимально достатній) рівень досягнення |

| | | | |
|----|-------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | 73-82 | | запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом |
| D | 66-72 | | <i>Задовільно/Satisfactory</i> – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни |
| E | 60-65 | | |
| FX | 40-59 | Незараховано | <i>Незадовільно/Fail</i> – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом |
| F | 0-39 | | <i>Незадовільно/Fail</i> – Результати навчання відсутні |

10. Питання для самоконтролю результатів навчання

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

11. Навчально-методичне забезпечення

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

12. Матеріально-технічне та програмне забезпечення дисципліни

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

При вивченні навчальної дисципліни використовується спеціальне програмне прикладне забезпечення ClickUp або його аналоги, яке є безкоштовним та відкритим.

13. Рекомендована література:

1. Якість та тестування інформаційних систем. Навчальний посібник для самостійної роботи студентів вищих навчальних закладів. Київ: ННІТ 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. 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.
6. 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.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : <https://msn.khmnu.edu.ua/course/view.php?id=7763>.
- Електронна бібліотека університету. URL: <http://library.khmnu.edu.ua/>
3. Репозитарій ХНУ. URL : <https://elar.khmnu.edu.ua/home>

БЕЗПЕКА ТА ЯКІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

| | |
|---------------------------------------------------------|------------------------|
| Тип дисципліни | Обов'язкова |
| Рівень вищої освіти | Перший (бакалаврський) |
| Мова викладання | Українська |
| Семестр | сьомий |
| Кількість призначених кредитів ЄКТС | 5,0 |
| Форми здобуття освіти, для яких викладається дисципліна | Очна (денна) |

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: 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, вимог якості; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій; застосовувати правила оформлення проєктних матеріалів інформаційних систем та технологій, знати склад та послідовність виконання проєктних робіт з урахуванням вимог відповідних нормативно-правових документів для запровадження у професійній діяльності; розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.; демонструвати вміння розробляти техніко-економічне обґрунтування розроблення інформаційних систем та технологій та вміти оцінювати економічну ефективність їх впровадження; 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. Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем. Методи, засоби та технології забезпечення безпеки інформаційних систем
Пререквізити: Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека (ОЗП.05), Системне програмне забезпечення (ОФП.07), Комп'ютерна логіка (ОФП.17), Інформаційні технології (ОФП.19), Смарт-технології та Інтернет речей (ОФП.09), Смарт-технології та Інтернет речей (курсний проєкт) (ОФП.10), Системне програмне забезпечення (курсний проєкт) (ОФП.08).

Кореквізити – Переддипломна практика (ОФП.22), Кваліфікаційна робота (ОФП.23).

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для *першого* (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); лабораторні заняття: з використанням методів проєктної діяльності, тренінгових вправ, аналіз проблемних ситуацій, пояснення, дискусія тощо; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання лабораторних робіт, поточного та підсумкового контролю), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання лабораторних робіт; підсумкова контрольна робота.

Вид семестрового контролю: іспит

Навчальні ресурси:

1. Якість та тестування інформаційних систем. Навчальний посібник для самостійної роботи студентів вищих навчальних закладів. Київ: ННІТ ДУТ, 2020. –128 с.
2. Проєктування інформаційних систем: Загальні питання теорії проєктування 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. 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.
6. 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.
7. Модульне середовище для навчання. Доступ до ресурсу: <https://msn.khmnu.edu.ua/course/view.php?id=7763>.
8. Електронна бібліотека університету. Доступ до ресурсу: <http://library.khmnu.edu.ua/>

Викладачі: Алексейко В. О.