ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

ЗАТВЕРДЖУЮ
Декан ФІТ [illegible] Т.О.
вересня 2024 р.

СИЛАБУС

Навчальна дисципліна **Безпека та якість інформаційних систем і технологій**

Освітньо-професійна програма **Інформаційні системи та технології**

Рівень вищої освіти **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	**Засорнова Ірина Олександрівна**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/zasornova-iryna/
E-mail викладача(ів)	zasornovair@khmnu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=7763
Навчальний рік	2024-2025
Консультації	**Очні**: п'ятниця, 2-а пара, 1-116; **онлайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		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				+

Анотація 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. Дисципліна викладається для здобувачів першого (бакалаврського) рівня вищої освіти денної форми навчання спеціальності «Інформаційні системи та технології». При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема, методи проблемного навчання.

Пререквізити: Комп'ютерна логіка; Інформаційні технології; Системне програмне забезпечення; Проектно-технологічна практика;

Кореквізити: Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека; кваліфікаційна робота

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп‘ютерної інженерії та інформаційних систем

ЗАТВЕРДЖУЮ
Декан ФІТ_____ Говорущенко Т.О.
_____5 _вересня_____ 2024__р.

СИЛАБУС

Навчальна дисципліна **Безпека та якість інформаційних систем і технологій**

Освітньо-професійна програма **Інформаційні системи та технології**

Рівень вищої освіти **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	**Засорнова Ірина Олександрівна**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/zasornova-iryna/
E-mail викладача(ів)	zasornovair@khmnu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=7763
Навчальний рік	2024-2025
Консультації	**Очні**: п’ятниця, 2-а пара, 1-116**;** **онлайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

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

Анотація 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. Дисципліна викладається для здобувачів першого (бакалаврського) рівня вищої освіти денної форми навчання спеціальності «Інформаційні системи та технології». При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема, методи проблемного навчання.

Пререквізити: Комп’ютерна логіка; Інформаційні технології; Системне програмне забезпечення; Проєктно-технологічна практика;

Кореквізити: Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека; кваліфікаційна робота

Мета і завдання дисципліни

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.

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

Очікувані 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.

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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема практичного заняття*	Тема лабораторної роботи*	Самостійна робота студентів		
				Зміст	Год.	Література
1	Якість інформаційних систем. Тестування програмного забезпечення для забезпечення якості інформаційних систем			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	4	[1, 9-11]
2			Тестування веб-орієнтованих систем. Складання звітів про помилки	Підготовка до захисту лабораторної роботи №1	4	[1, 9-11]
3	Види тестування програмного забезпечення для інформаційних систем			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2.	4	[1, 9-11]
4			Тестування зручності використання та кросбраузерне тестування веб-орієнтованих інформаційних систем	Підготовка до захисту лабораторної роботи №2	4	[1, 9-11]
5	Тестування веб-орієнтованих інформаційних систем			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3.	4	[1, 9-11]
6			Модульне тестування програмного забезпечення для забезпечення якості інформаційних систем	Підготовка до захисту лабораторної роботи №3	4	[1, 9-11]
7	Забезпечення якості інформаційних систем. Стандарти та метрики якості інформаційних систем			Опрацювання лекційного матеріалу.	4	[1, 9-11]
8	Поняття безпеки інформаційних систем. Загрози безпеці ІС. Модель порушника			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4.	4	[2-8,12,13]
9			Модульне тестування програмного	Підготовка до захисту лабораторної	4	[2-8,12,13]

			забезпечення інформаційних систем із використання Test doubles об’єктів	роботи №4.		
10	Базові системи захисту			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5.	4	[2-8,12,13]
11			Оцінка якості інформаційних систем. Тестування продуктивності інформаційної веб-системи	Підготовка до захисту лабораторної роботи №5.	4	[2-8,12,13]
12	Проєктування ІС із врахуванням відмовостійкості. Типові вразливості систем та методи забезпечення відмовостійкості спеціалізованих інформаційних систем			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6.	4	[2-8,12,13]
13			Дослідження та перевірка безпеки інформаційної системи у мережі. Створення Honeypot-приманок для аналізу впливів спрямованих на порушення безпеки інформаційної системи в мережі	Підготовка до захисту лабораторної роботи №6.	4	[2-8,12,13]
14	Методи забезпечення живучості та захисту інформації в спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення			Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7.	4	[2-8,12,13]
15			Забезпечення безпеки інформаційної системи засобами міжмережевого екрану netfilter через утиліту iptables. Блокування атак відмова в обслуговуванні	Підготовка до захисту лабораторної роботи №7	4	[2-8,12,13]
16	Основи безпеки інформації в комп‘ютерних мережах			Опрацювання лекційного матеріалу. Підготовка до	4	[2-8,12,13]

				лабораторної роботи №8.		
17			Проектування ІС із врахуванням відмово стійкості. Налаштування середовища контейнеризації Docker для сервера LEMP. Docker Compose. Сканування вразливостей хоста за допомогою Docker Bench.	Підготовка до захисту лабораторної роботи №8. Підготовка до підсумкового контрольного заходу	5	[2-8,12,13]

Примітка: * Послідовність проведення занять визначається розкладом (може не відповідати нумерованим тижням)

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, лабораторні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. Пропущене лабораторне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних занять студент має підготуватися за відповідною темою і проявляти активність. Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ.

Критерії оцінювання результатів навчання.

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

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

Аудиторна робота								Самостійна, індивідуальна робота	Форма семестрового контролю
7 семестр									
Лабораторні роботи №:								Контроль:	Іспит
1	2	3	4	5	6	7	8	ТК	
ВК:	0,5							0,1	0,4

Умовні позначення: ТК – тестовий контроль; Т – тема дисципліни; ВК – ваговий коефіцієнт.

Співвідношення інституційної шкали оцінювання і шкали оцінювання 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.

Питання для підсумкового контролю з дисципліни

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?

9. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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

Розробник: к.т.н., доц. Засорнова І.О.

Погоджено:

Зав. каф. КІС: к.т.н., доц. Засорнова І.О.

Гарант ОПП «ІСТ»: д.т.н., проф. Гнатчук Є.Г.