ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Говорущенко Т.О.
«05» вересня 2024 р.

СИЛАБУС

Вибіркова дисципліна **Стандарти та засоби інформаційної безпеки**

Загальна інформація

Позиція	Зміст інформації
Викладач	**Капустян Марія Вікторівна**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/kapustyan-mariya-viktorivna/
E-mail викладача	kapustianm@khmnu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/enrol/index.php?id=7741
Навчальний рік	2024/2025
Консультації	Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	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
Д	1	непарний	8	240	102	34	34	34		138			+	
Разом			**8**	**240**	**102**	**34**	**34**	**34**		**138**			**1**	

Анотація дисципліни

Дисципліна "Стандарти та засоби інформаційної безпеки" є однією із вибіркових дисциплін загальної підготовки бакалаврів галузі інформаційних технологій.

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

Розробник: к.т.н., доц., Капустян М.В.

Погоджено:

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

Гарант ОПП «КІП»: д.т.н., проф. Лисенко С.М.

Мета і завдання дисципліни

Метою дисципліни "Стандарти та засоби інформаційної безпеки" є: 1) формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації; 2) формування компетентностей та практичних навичок щодо забезпечення захисту програмної продукції; 3) розвиток у студентів фахового стилю мислення; 4) формування у майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, організації та держави, необхідних для подальшої роботи; 5) вивчення застосування методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Завдання дисципліни. Надати студентам знання і практичні навички із забезпечення інформаційної безпеки в комп'ютерних системах та мережах.

Очікувані результати навчання.

Студент, який успішно завершив вивчення дисципліни, повинен: вміло *використовувати* набуті знання зі стандартів інформаційної безпеки, основних методів та засобів захисту; *виконувати* основні задачі із забезпечення захисту інформації; *демонструвати* практичні навички із застосування криптографічних засобів захисту; *аналізувати* стан інформаційної безпеки та *визначати* причини появи каналів витоку інформації.

Компетентності, на формування яких спрямовано ОК:

Інтегральна – Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов

ЗК2 – Здатність вчитися і оволодівати сучасними знаннями

ЗК3 – Здатність застосовувати знання у практичних ситуаціях

ЗК4 – Здатність спілкуватися державною мовою як усно, так і письмово

ЗК7 – Вміння виявляти, ставити та вирішувати проблеми

ЗК11 – Здатність до розуміння предметної галузі та професійної діяльності.

ЗК12 – Здатність використовувати інформаційні та комунікаційні технології

ЗК13 – Здатність розв'язувати поставлені задачі та приймати відповідні рішення

ФК1 – Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії

ФК7 – Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності

ФК9 – Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи

ФК13 – Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій

ФК16 – Здатність до аналізу, синтезу і оптимізації комп'ютерних та інформаційних технологій з використанням математичних моделей і методів

ФК20 – Здатність використовувати та керувати сучасними інформаційними технологіями, технологіями комп'ютерної інженерії, методиками й техніками кібербезпеки під час виконання функціональних завдань та обов'язків

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН3 – Знати новітні технології в галузі комп’ютерної інженерії

ПРН6 – Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей

ПРН11 – Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії

ПРН15 – Вміти виконувати експериментальні дослідження за професійною тематикою

ПРН17 – Спілкуватись усно та письмово з професійних питань українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською)

ПРН18 – Використовувати інформаційні технології для ефективного спілкування на професійному та соціальному рівнях

ПРН19 – Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення

ПРН20 – Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення

ПРН21 – Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики

ПРН23 – 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 програмно-технічних засобів комп’ютерних систем та мереж

ПРН25 – Адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та технології комп’ютерної інженерії із забезпеченням захисту інформації в комп’ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки

Тематичний і календарний план вивчення дисципліни

Номер лекції	Перелік тем лекцій, їхні анотації	Кількість годин
	Непарний семестр	
1	**Вступ до інформаційної безпеки** Поняття інформації та даних. Загальні поняття захисту інформації. Канал передачі інформації. Канали витоку інформації. Закони України про захист інформації. Аналіз даних захисту.	2
2	**Політика інформаційної безпеки.** Управління безпекою. Розробка правил безпеки.	2
3	**Міжнародні стандарти у галузі інформаційної безпеки.** Правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем. Метод шифрування. Ключ шифрування.	4
4	**Методи шифрування.** Симетричні методи шифрування. Несиметричні методи шифрування. Проблеми та перспективи криптографічних систем. Симетричне шифрування. Асиметричне шифрування та його використання. Управління ключами шифрування.	2
5	**Електронний цифровий підпис (ЕЦП).** Призначення ЕЦП. Необхідність сертифікації засобів ЕЦП і відкритих ключів. Особливості рукописного підпису. Особливості ЕЦП.	4
6	**Еліптичне шифрування інформації.** Поняття токенів. Еліптичне шифрування інформації.	2
7	**Системи захисту в інформаційних мережах.** Загальна характеристика. Фізична безпека. Аутентифікація та безпека мережі. Паролі. Захист інформації в бездротових локальних мережах..	2
8	**Криптостійкість засобів ЕЦП.** Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні.	4
9	**Телекомунікації та віддалений доступ. Резервне копіювання**. Адміністрування інформаційних систем. Безпека протоколів TCP/IP. Програмні засоби захисту інформації.	2
10	**Інформаційні технології та право.** Комп'ютерні злочини. Правила роботи з WWW. Обов'язки користувача.	2
11	**Правила використання електронної пошти.** Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією.	2
12	**Комп'ютерні віруси.** Класифікація і властивості вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.	4
Разом за сьомий семестр:		**34**

Примітка: *Лекції проводяться кожного тижня по дві години; 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 та 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 їх початку; 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

<table>
<tr><td colspan="8">Аудиторна робота</td><td>Семестр. контроль (залік)</td></tr>
<tr><td colspan="9">І семестр</td></tr>
<tr><td colspan="8">Лабораторні роботи №:</td><td rowspan="3">Залік за рейтингом</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></tr>
<tr><td>ВК:</td><td colspan="7">1</td></tr>
</table>

Умовні позначення: 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. Загальні поняття захисту інформації.
2. Закони України про захист інформації.
3. Аналіз даних захисту.
4. Право інтелектуальної власності та політика інформаційної безпеки.
5. Управління безпекою.
6. Розробка правил безпеки.
7. Міжнародні правила застосування шифру.
8. Управління криптографією.
9. Вимоги до криптографічних систем.
10. Метод шифрування.
11. Ключ шифрування.
12. Симетричні методи шифрування.
13. Несиметричні методи шифрування.
14. Проблеми та перспективи криптографічних систем.
15. Симетричне шифрування.
16. Асиметричне шифрування та його використання.
17. Управління ключами шифрування.
18. Правовий статус електронного цифрового підпису
19. Призначення електронного підпису.
20. Необхідність сертифікації засобів ЕЦП і відкритих ключів.
21. Особливості рукописного підпису.
22. Особливості ЕЦП.
23. Поняття токенів.
24. Еліптичне шифрування інформації.
25. Загальна характеристика систем захисту в інформаційних мережах.
26. Фізична безпека.
27. Аутентифікація та безпека мережі.
28. Паролі.
29. Захист інформації в бездротових локальних мережах.
30. Криптостійкість засобів ЕЦП.
31. Поняття електронного сертифікату.
32. Моделі систем сертифікації.

33. Проблеми та перспективи впровадження ЕЦП в Україні.
34. Користувацький інтерфейс.
35. Телекомунікації та віддалений доступ.
36. Резервне копіювання.
37. Адміністрування інформаційних систем.
38. Безпека протоколів TCP/IP.
39. Програмні засоби захисту інформації.
40. Інформаційні технології та право.
41. Комп'ютерні злочини.
42. Правила роботи з WWW.
43. Обов'язки користувача.
44. Правила використання електронної пошти.
45. Адміністрування електронної пошти.
46. Використання електронної пошти для конфіденційного обміну інформацією.
47. Комп'ютерні віруси та їх властивості.
48. Класифікація вірусів.
49. Основні види комп'ютерних вірусів та схеми їх функціонування.
50. Структура комп'ютерних вірусів.
51. Програми виявлення вірусів та заходи по захисту та профілактиці.
52. Антивірусні пакети.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

Розробник: к.т.н., доц., Капустян М.В.

Погоджено:

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