ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ

Спеціальність: 122 Комп'ютерні науки
Обов'язкова дисципліна: професійної підготовки.
Циклова комісія, з комп'ютерних технологій.
Викладач(і): викладач вищої категорії, Шибаєв Денис Сергійович

Вивчається у 7 семестрі (4 курс, 1 семестр)
Обсяг 120 годин.
З них аудиторні 68 год у вигляді з них лекційних - 32, практичних – 36, **7 семестр – 4 год/тиждень.**
Підсумкова форма контролю: залік
Самостійна робота: - 52 годин. Самостійна робота здобувача відбувається впродовж семестру та складається з підготовки до аудиторних занять, контрольних заходів, індивідуальних завдань.
Вид індивідуальної роботи: не передбачено.
Консультації: здійснюються викладачем впродовж семестру згідно розкладу.

Мета дисципліни:

полягає в наданні студентам основних знань, навичок і практичного досвіду, необхідних для розробки та організації процесів захисту інформації, методів комплексного забезпечення криптографічної цілісності програмних систем. Дисципліна включає в себе вивчення основ кібербезпеки, криптографії, вірусології та програмної розробки спеціалізованих систем шифрування.

Завдання дисципліни:

– Вивчення основних принципів і методів захисту інформації. Ознайомлення студентів з базовими концепціями інформаційної безпеки, такими як конфіденційність, цілісність, доступність, а також методами забезпечення цих принципів.

– Аналіз загроз і вразливостей. Вивчення різних видів загроз і вразливостей, які можуть виникати в інформаційних системах, та методів їх виявлення і аналізу.

– Проектування і впровадження систем захисту. Навчання проектуванню систем захисту інформації, вибору та налаштуванню відповідних засобів і механізмів захисту, таких як шифрування, антивірусне програмне забезпечення, міжмережеві екрани, системи виявлення вторгнень тощо.

– Моніторинг і управління інформаційною безпекою. Ознайомлення з методами моніторингу інформаційних систем для виявлення потенційних загроз, управління інцидентами інформаційної безпеки та проведення аудитів безпеки.

– Розробка політик і процедур безпеки. Створення та впровадження політик і процедур, спрямованих на забезпечення інформаційної безпеки, включаючи політики доступу, зберігання та обробки даних, а також навчання персоналу.

– Забезпечення відповідності законодавству і стандартам. Вивчення вимог законодавства та стандартів у сфері інформаційної безпеки та їх впровадження в організації.

– Розвиток навичок аналізу та вирішення проблем. Формування навичок аналізу та критичного мислення для вирішення проблем, пов'язаних з інформаційною безпекою, та прийняття обґрунтованих рішень.

Основні результати навчання

РН05. Розуміти основні методи і технології об'єктно-орієнтованого та компонентного програмування.
РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем.
РН10. Знати методології, методи, моделі, процеси і технології життєвого циклу розробки та тестування програмного забезпечення.

Тематика та види навчальних занять

Усі заняття проводяться як комплексні, а саме - як поєднання лекційного матеріалу та практичного опрацювання. Орієнтовна кількість лекційного матеріалу – 32 год, а практичної роботи 36 год

Навчання складається з 2 тем, кожна з яких закінчується підсумковою практичною роботою та контрольною роботою:

1. **Тема 1. Стародавні системи шифрування**
2. **Тема 2. Сучасна криптографія**
3. **Тема 3. Електронно-цифровий підпис**

4. **Тема 4. Комп'ютерна вірусологія**
5. **Тема 5. Кіберзлочинність та захист у законодавстві**
6. **Тема 6. Симетричні криптографічні системи**
7. **Тема 7. Асиметричні криптографічні системи**

Оцінювання результатів навчання

В організації навчального процесу під час вивчення дисципліни застосовують підсумкову форму контролю як розрахунок середньої з усіх підсумкових контрольних робіт для семестрового заліку. Контроль кожної контрольної роботи виконується за критеріями у табл. 1, 2.

Практичні роботи для отримання підсумкового заліку повинні бути виконані усі в обов'язковому порядку. За кожну практичну роботу проставляється позначка її виконання «заліковано».

На заліковому занятті виконуються підсумкові практичні або контрольні роботи, які не були зараховані у поточному семестрі.

Якщо виконані усі практичні та контрольні роботи – підсумкова оцінка заліку виставляється автоматично

Оцінки за шкалою ECTS відповідають наступним балам для розрахунку середнього:

A – 5 бал, **B** – 4,5 бал, **C** – 4 бал, **D**- 3,5 бал, **E** – 3 бал, **FX,F** – 0 бал

Таблиця 1 – Критерії оцінювання поточних та підсумкових робіт з теоретичних питань

Оцінка за нац. шк.	**ECTS**	**Критерії оцінювання виконання КР.**
Відмінно	A	Повністю розкрита суть питання, послідовно і логічно викладена, наведені приклади, проілюстровано відповідь усім необхідним. Здобувач показав високі знання понятійного апарату і літературних джерел, вміння аргументувати думки, проводити грунтовний аналіз та порівняння.
Добре	B	Майже повністю розкрита суть питання, послідовно і логічно викладена, але наведені приклади і ілюстрації відповіді проведені не повністю. Здобувач продемонстрував добре вміння аналізувати отриману інформацію, але не до кінця розкрив деякі питання.
Добре	C	Основна частина питань розкрита повністю, викладена послідовно і логічно. Але деякі питання не розкриті, але частково викладені, наведені приклади і ілюстрації відповіді проведені не достатньо. Здобувач продемонстрував вміння аналізувати отриману інформацію, але деякі питання не проаналізував.
Задовільно	D	Більше половини питань розкриті та викладені майже повністю. Але половина питань або не розкрита, або розкрита частково, при цьому здобувач продемонстрував тільки часткове вміння аналізу отриманої інформації по деяким питанням.
Задовільно	E	Тільки половина питань розкриті та викладені повністю або частково. А друга половина питань або не розкриті, або викладена невелика частина, при цьому здобувач продемонстрував невелику долю вміння аналізу отриманої інформації.
Незадовільно	FX	Суть питання більшою мірою не розкрита. Є прогалини у розумінні предмету питання. При цьому здобувач продемонстрував незадовільне вміння проводити аналіз отриманої інформації.
	F	Відповідь відсутня.

Таблиця 2 – Критерії оцінювання поточних та підсумкових практичних робіт

Оцінка за нац. шк.	**ECTS**	**Критерії оцінювання виконання КР.**
Відмінно	A	Наведено розв'язання задачі, усі дії виконані вірно, без помилок. При цьому здобувач продемонстрував відмінне знання основ операційних систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів.
Добре	B	Наведено розв'язання усіх задач, але були допущені неточності та незначні помилки. Здобувач продемонстрував дуже добре знання основ операційних

		систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів.
Добре	C	Наведено розв'язання майже усіх задач, але була допущена невелика кількість помилок. Здобувач продемонстрував добре знання основ операційних систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів.
Задовільно	D	Більше половини задач розв'язані. Але частина завдань розв'язана тільки частково, при цьому здобувач продемонстрував задовільне знання основ операційних систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів..
Задовільно	E	Половина задач розв'язані. Але частина завдань не розв'язана або розв'язана тільки частково, при цьому здобувач продемонстрував достатнє знання основ операційних систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів.
Незадовільно	FX	Основна частина задач не розв'язані. Невелика частина завдань розв'язана тільки частково, при цьому здобувач продемонстрував недостатнє знання основ операційних систем, вміння використовувати засоби управління та захисту операційних систем та їх компонентів..
	F	Відповідь відсутня.

Посилання на рекомендовані джерела

1. Щур Н.О., Покотило О.А. Основи криптології: навч. Посібник / Н.О. Щур, О.А. Покотило. – Житомир: Державний університет «Житомирська політехніка», 2021 - 120 с.
2. Гапак О.М. Захист інформації в комп'ютерних системах / О.М. Гапак, С.І.Балога. – Ужгород, 2021. – 184 с.
3. Семенов С.Г. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.–251 с.
4. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. / В.М. Вишняков. – Київ: КНУБА, 2022. – 120 с.
5. Карачка А.Ф. Технології захисту інформації / А.Ф. Карачка. – Тернопіль, ТНЕУ, 2017. - 86 с.
6. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
7. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

Політика освітнього процесу та підсумкового контролю

Активна участь в практичних заняттях, дотримання графіків здачі контрольних та індивідуальних завдань, самостійна робота здобувача при підготовці до всіх видів аудиторних занять, присутність на консультаціях може бути відзначена на підсумковій роботі додаванням від 0,5 до 1 балу. Здобувачі зобов'язані дотримуватись принципів академічної доброчесності при виконанні підсумкових контрольних робіт.

Відсутність здобувача на контрольній роботі відповідає оцінці «0 бал».

Під час всіх видів аудиторних занять здійснювати телефонні дзвінки забороняється.

Дозволяється використання будь-яких підручників, посібників, конспектів лекцій, інтернет-ресурсів під час проходження підсумкових практичних робіт

Заборонено використання будь-яких підручників, посібників, конспектів лекцій, шпаргалок під час проходження підсумкових контрольних робіт.

Перескладання заліку відбувається за встановленим розкладом, або після термінів перескладання індивідуально за направленням навчальної частини.