СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

Галузь знань	12–Інформаційні технолошії
Шифр та назва спеціальності	125 – Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-12 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Голев Денис Володимирович
d.v_holev@suitt.edu.ua

Старший викладач кафедри Кібербезпеки та технічного захисту інформації

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна "Комп'ютерні технології" призначений для ознайомлення учасників із основними аспектами та принципами роботи комп'ютерів та супутніх технологій. Програма включає в себе вивчення архітектури комп'ютерів, операційних систем, мережевих технологій та інших ключових понять. Курс надає студентам навички, необхідні для

	розуміння та використання сучасних комп'ютерних технологій в різних сферах.
Мета дисципліни	1.1 Метою вивчення дисципліни є забезпечення студентів необхідними знаннями та практичними навичками для роботи з комп'ютерними технологіями в різних сферах життя та діяльності, таких як бізнес, освіта, наука, медицина та інші. 1.2 Основними завданнями вивчення дисципліни "Комп'ютерні технології" є наступні: – навчання студентів засобам та технологіям обробки, зберігання, передачі та аналізу даних, що допоможе їм розуміти, як працюють сучасні комп'ютерні системи; – отримання навичок роботи з різноманітним програмним забезпеченням, включаючи операційні системи; – ознайомлення з технологіями мереж та комунікацій, включаючи бездротові мережі, мережі на основі інтернет-технологій та протоколи комунікації; – вивчення принципів кібербезпеки та захисту інформації, що допоможе студентам зрозуміти, як захищати комп'ютерні системи від зловмисників та кібератак.
Компетентності, формуванню яких сприяє дисципліна	КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ5. Здатність до пошуку, оброблення та аналізу інформації. КФ1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ2. Здатність до використання інформаційно–комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Результати навчання	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язуванні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 15. Використовувати сучасне програмно–апаратне забезпечення інформаційно–комунікаційних технологій. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

Обсяг дисципліни	Загальний обсяг дисципліни: 10 кредитів ЄКТС 300 годин. Для денної форми навчання: лекції – 34 години, практичні заняття –34 години, лабораторні заняття – 34 години, самостійна робота – 198 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 1-му та 2-му семестрі

Програма дисципліни

	Змістовий модуль 1. Архітектура комп'ютера.
Тема 1.	Процесор: вивчення принципів роботи процесора, його основних компонентів, архітектури та механізмів виконання команд.
Тема 2.	Пам'ять: вивчення різних видів пам'яті, їх призначення, організації та роботи з ними.
Тема 3.	Ввід-вивід: вивчення принципів роботи з пристроями введення-виведення, організації та забезпечення їх взаємодії з процесором та пам'яттю.
Тема 4.	Шина: вивчення принципів роботи шини даних та шини адрес, їх організації та взаємодії з іншими компонентами системи.
Тема 5.	Архітектура комп'ютерної системи: вивчення загальної структури та організації комп'ютерної системи, її компонентів та взаємодії між ними.
Тема 6.	Інструкції процесора: вивчення основних видів команд процесора, їх формату та призначення, робота зі стеком та реєстрами.
Тема 7.	Мікроархітектура: вивчення структури та принципів роботи мікроархітектури, її елементів та механізмів, оптимізація та підвищення продуктивності.
	Змістовий модуль 2. Операційні системи сімейства Linux.
Тема 1.	Ядро Linux: вивчення структури та основних компонентів ядра Linux, його основних функцій та механізмів роботи.
Тема 2.	Файлова система: вивчення принципів організації та роботи з файловою системою, її особливостей та налаштування.
Тема 3.	Процеси та потоки: вивчення принципів роботи з процесами та потоками в операційній системі Linux, їх створення, керування та моніторинг.
Тема 4.	Мережеві протоколи та сервіси: вивчення принципів роботи мережевих протоколів та сервісів в операційній системі Linux, їх налаштування та управління.
Тема 5.	Системні драйвери: вивчення принципів роботи з системними драйверами, їх розробка, налагодження та взаємодія з ядром Linux.

Тема 6.	Обробка сигналів та винятків: вивчення принципів обробки сигналів та винятків в операційній системі Linux, їх використання та керування.
Тема 7.	Система безпеки: вивчення принципів роботи системи безпеки операційної системи Linux, захисту від зловмисних атак та інших загроз безпеці.
Тема 8.	Командний рядок: вивчення принципів роботи з командним рядком операційної системи Linux, його основних команд та інструментів.
	Змістовий модуль 3. Операційні системи сімейства Windows.
Тема 1.	Ядро ОС: вивчення структури та основних компонентів ядра ОС Windows, його функцій та механізмів роботи.
Тема 2.	Файлова система: вивчення принципів організації та роботи з файловою системою ОС Windows, її особливостей та налаштування.
Тема 3.	Процеси та потоки: вивчення принципів роботи з процесами та потоками в ОС Windows, їх створення, керування та моніторинг.
Тема 4.	Мережеві протоколи та сервіси: вивчення принципів роботи мережевих протоколів та сервісів в ОС Windows, їх налаштування та управління.
Тема 5.	Драйвери: вивчення принципів роботи з драйверами пристроїв в ОС Windows, їх розробка, налагодження та взаємодія з ядром ОС.
Тема 6.	Система безпеки: вивчення принципів роботи системи безпеки ОС Windows, захисту від зловмисних атак та інших загроз безпеці.
Тема 7.	Робота з користувачем: вивчення принципів роботи з користувачем ОС Windows, налаштування та управління правами користувачів, контроль доступу та інші функції.
	Змістовий модуль 4. Безпека операційних систем.
Тема 1.	Аутентифікація та авторизація - механізми, що дозволяють перевірити ідентифікацію користувачів та контролювати їх доступ до ресурсів системи.
Тема 2.	Захист мережі - забезпечення захисту мережі від несанкціонованого доступу та атак ззовні.
Тема 3.	Захист даних - механізми, що забезпечують конфіденційність, цілісність та доступність даних на пристроях зберігання.
Тема 4.	Захист від шкідливих програм - механізми, що забезпечують захист від шкідливих програм та вразливостей системи.
Тема 5.	Аудит безпеки - забезпечення можливості аналізувати журнали подій системи для виявлення можливих вторгнень та порушень безпеки.
Тема 6.	Захист фізичного рівня - забезпечення безпеки обладнання та інфраструктури, на якій працює операційна система.
Тема 7.	Управління правами доступу - механізми, що дозволяють керувати правами доступу користувачів до ресурсів системи.

Список рекомендованих джерел

1. Шон Харрис. CISSP Руководство для подготовки к екзамену / Шон Харрис // Пятая редакции, 2019. - 875 с.

2. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загальногокористування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.

3. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина 1: лаб. практ. – Одеса: ОНАЗ ім. О.С. Попова, 2011.

4. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев // За ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. – С.176

5. Таненбаум Э., Бос Х. Т18 Современные операционные системы. 4-е изд. — СПб.: Питер, 2015. — 1120 с.: ил. — (Серия «Классика computer science»)

6. Таненбаум Э. Архитектура компьютера / Э. Таненбаум, Т. Остин. – Спб: Питер, 2013. – 816 с. – (6).

7. Чарльз Р. Северанс Как работают компьютерные сети и интернет / пер. с англ. П. М. Бомбаковой – М.: ДМК Пресс, 2022. – 116 с.: ил.

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 13^{00} до 14^{30} год., ауд. 250 або zoom

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				

35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.