



# СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

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

### Викладачі

Голев Денис Володимирович  
[d.v\\_holev@suitt.edu.ua](mailto: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.
<b>Мета дисципліни</b>	<p>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.</p> <p>1.2 Основними завданнями вивчення дисципліни "Комп'ютерні технології" є наступні:</p> <ul style="list-style-type: none"> <li>– навчання студентів засобам та технологіям обробки, зберігання, передачі та аналізу даних, що допоможе їм розуміти, як працюють сучасні комп'ютерні системи;</li> <li>– отримання навичок роботи з різноманітним програмним забезпеченням, включаючи операційні системи;</li> <li>– ознайомлення з технологіями мереж та комунікацій, включаючи бездротові мережі, мережі на основі інтернет-технологій та протоколи комунікації;</li> <li>– вивчення принципів кібербезпеки та захисту інформації, що допоможе студентам зрозуміти, як захищати комп'ютерні системи від зловмисників та кібератак.</li> </ul>
<b>Компетентності, формуванню яких сприяє дисципліна</b>	<p>КЗ2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>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.</p> <p>КФ2. Здатність до використання інформаційно–комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.</p>
<b>Результати навчання</b>	<p>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.</p> <p>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.</p> <p>ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.</p> <p>ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.</p> <p>ПРН 15. Використовувати сучасне програмно–апаратне забезпечення інформаційно–комунікаційних технологій.</p> <p>ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</p>

<b>Обсяг дисципліни</b>	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.
<b>Форма підсумкового контролю</b>	Екзамен
<b>Терміни викладання дисципліни</b>	Дисципліна викладається у 1-му та 2-му семестрі

### Програма дисципліни

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

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

### Список рекомендованих джерел

1. Fernando Maymí, Shon Harris. CISSP All-In-One Exam Guide / Ninth Edition / McGraw Hill / 2022. – 1361
2. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. 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. практик. – 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. Andrew S. Tanenbaum, Herbert Bos Modern Operating Systems, 5th Edition – 2023 xxviii, 1156\1185

### Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 13<sup>00</sup> до 14<sup>30</sup> 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: <i>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.</i>
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано		
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, за посиланням [.....](#)