



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

АРХІТЕКТУРА ТА МОДЕЛІ БЕЗПЕКИ

Галузь знань	12 Інформаційні технології
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-18 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Кіреєв Ігор Анатолійович
kireev.igor@ukr.net



Доцент кафедри Кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни

Дисципліна «Архітектура та моделі безпеки» базується на професійно-орієнтованих дисциплінах. Предметом вивчення навчальної дисципліни є архітектура, принципи побудови та моделі безпеки комп'ютерних систем, які включають аналіз стану безпеки та ефективності функціонування систем захисту інформації комп'ютерних систем, концепції, принципи, структури і стандарти, використовувані для побудови, моніторингу та підтримки безпеки

	комп'ютерних систем на різних рівнях доступності, цілісності та конфіденційності інформації.
Мета дисципліни	– є вивчення класичних основ побудови комп'ютерних систем, їх архітектури, алгоритмів та методів, застосованих при їх розробці, моделі забезпечення безпеки комп'ютерних систем, на базі яких виробляються архітектурні, схемотехнічні, програмно-алгоритмічні розв'язки при створенні захищених комп'ютерних систем, вивчення основних формальних моделей політик безпеки, моделей дискреційного, мандатного та рольового керування доступом.
Компетентності, формуванню яких сприяє дисципліна	<p>КЗ1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</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>КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>
Результати навчання	<p>ПРН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p> <p>ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.</p> <p>ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передач даних.</p> <p>ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних, інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.</p> <p>ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.</p> <p>ПРН36. Виявляти небезпечні сигнали технічних засобів.</p> <p>ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.</p> <p>ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</p>

Обсяг дисципліни	Загальний обсяг дисципліни: 5 кредитів ЄКТС 160 годин. Для денної форми навчання: лекції – 28 годин, практичні заняття –14 годин, лабораторні заняття –26 години, самостійна робота – 96 години.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі

Програма дисципліни

Тема 1.	<i>Цілі та задачі курсу архітектура та моделі безпеки КС, основні поняття .</i> Архітектура, принципи побудови та моделі безпеки комп'ютерних систем, аналіз стану безпеки та ефективності функціонування систем захисту інформації комп'ютерних систем, концепції, принципи, структури і стандарти ІБ.
Тема 2.	<i>Функціонування комп'ютерної системи. Принципи побудови ПК .</i> Принципи побудови ПК згідно фон Неймана. Магістрально-модульна структура побудови комп'ютерної системи (центральний процесор, пам'ять, зовнішні пристрої вводу-виводу, контролери і магістраль - системна шина (system bus). Шина адреса, шина даних і шина керування.
Тема 3.	<i>Многопроцесорна обробка. Архітектура операційної системи .</i> Симетричний і асиметричний режими. Архітектура операційної системи - кооперативна багатозадачність, архітектура і управління вводом-виводом, управління процесами, управління потоками. Робота процесів по перериваннях: масковані і немасковані. Діспетчірізація і синхронізація процесів.
Тема 4.	<i>Управління пам'яттю, структура , ієрархія пам'яті..</i> Управління пам'яттю, адресний простір комп'ютерної системи, ієрархія пам'яті. Типи пам'яті: пам'ять з довільним доступом, прямий доступ до пам'яті. Пам'ять тільки для читання, пам'ять для читання і запису, Кеш-пам'ять (кеш команд, кеш даних, кеш жорсткого диска). Відображення пам'яті. Основна (оперативна) і зовнішня (вторинна) пам'ять Витоку пам'яті. Апаратний захист пам'яті і процесора.
Тема 5.	<i>Сінхронний і асинхронний ввід-вивід інформації в КС .</i> Методи, які використовуються при ізоляції процесів: інкапсуляція об'єктів, тимчасове мультиплексування, поділ імен, віртуальне отображення. Порти вводу- виводу комп'ютерної системи. Драйвера, стики, інтерфейси і протоколи обміну. Мережеві протоколи. Периферійні пристрої комп'ютерних систем.
Тема 6.	<i>Віртуальна пам'ять і віртуальні машини .</i> Вторинні сховища (secondary storage) є енергонезалежні носії -віртуальне пам'ять. Підкачка (paging) віртуальної пам'яті. Режими процесора і кільця захисту. Класифікація: внутрішні і зовнішні. Архітектура кілець захисту: ядро операційної системи, операційна система, драйвери і утиліти вводу - виводу, додатки користувачів.

Тема 7.	<p><i>Архітектура операційної системи. Монолітна та багаторівнева архітектура ОС .</i></p> <p>Архітектура операційної системи. Монолітна архітектура ОС (monolithic operating system architecture), багаторівнева архітектура ОС (layered operating system architecture). Домени - це набір об'єктів, домен виконання (execution domain). Поділ на рівні (layering) і приховування даних (data hiding). Еволюція термінології. Віртуальні машини (virtual machine) і середовища - Java Virtual Machine (JVM).</p>
Тема 8.	<p><i>Додаткові пристрої зберігання. Класифікація.</i></p> <p>Блокові і символьні пристрої вводу - виводу. Управління пристроями вводу - виводу. Контролери переривань. Апаратні та програмні переривання. Процедури вводу - виводу операційною системою: програмований , керований перериваннями , з використанням DMA , з частковим і повним відображенням.</p>
Тема 9.	<p><i>Архітектура системи. Підмножини суб'єктів і об'єктів.</i></p> <p>Довірена комп'ютерна база, довірений канал, довірена оболонка . Критерій оцінки - «Помаранчева книга». Периметр безпеки (security perimeter). Монітор звернень) - абстрактна машина і ядро безпеки . Політика безпеки. Багаторівневі політики безпеки. Принцип найменших привілеїв.</p>
Тема 10.	<p><i>Методи розмежування і управління доступом: дискреційна, мандатна і рольова моделі. Матриця контролю доступу</i></p> <p>Моделі безпеки комп'ютерних систем. Модель кінцевих автоматів (state machine model), переходи стану (state transition). модель безпеки Bell-LaPadula - захист конфіденційності. Модель Biba - захист цілісності. Модель Clark-Wilson - політики безпеки і цілісності. Взаємини між політикою безпеки та моделлю безпеки.</p>
Тема 11.	<p><i>Матриця контролю доступу. Цілі моделей цілісності.</i></p> <p>Модель інформаційних потоків. Рівні безпеки. Приховані канали (covert channel). Типи прихованих каналів: по пам'яті і по часу. багаторівнева безпека - модель невляння. Сітчаста модель , межі доступу в сітчастій моделі. Модель Brewer and Nash - модель «Китайської стіни». Моделі безпеки КС-кінцевих автоматів , переходи стану. Рівні безпеки. Приховані канали - по пам'яті і по часу .</p>
Тема 12	<p><i>Динамічне управління доступом. Модель Graham-Denning та Harrison-Ruzzo-Ulman.</i></p> <p>Режими безпеки функціонування. Типи користувачів, типи даних (рівні класифікації, рівні допуску, категорії). Спеціальний режим безпеки (dedicated security mode). Режим підвищеної безпеки системи (system high-security mode). Роздільний режим безпеки (compartment security mode). Робочі станції роздільного режиму. Багаторівневий режим безпеки (multilevel security mode).</p>
Тема 13.	<p><i>Програмні та апаратні охоронці. Довіра і гарантії.</i></p> <p>Методи оцінки систем. Помаранчева Книга. Система класифікації TCSEC. Рівні гарантій: А - перевірений захист , В - мандатний захист , С - дискреційний захист , D - мінімальна безпека . Помаранчева книга і райдужна серія. Червона книга. ITSEC. Загальні критерії.</p>
Тема 14.	<p><i>Сертифікація і акредитація (поняття, визначення). Нормативні документи та вимоги до них .</i></p> <p>Види та мета сертифікації продукції в державній системі сертифікації. Обов'язкова та добровільна сертифікація. Сертифікати відповідності та свідоцтва. Акредитація. План акредитації. Узгодження плану, вимоги для акредитації. Оцінка документів для акредитації.</p>

Список рекомендованих джерел

1. Shon Harris, Fernando Mayumi. Praise for CISSP® All-in-One Exam Guide Copyright © 2019 by McGraw-Hill Education. - 16921. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків:НТМТ, 2014. –298с.
2. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб./ Д.В. Євграфов. –К.:НТУУ"КПІ", 2014. –176с.
3. Методики оцінки інформаційної захищеності : навч. посібник / Н.В. Кондратьєва, В.Г. Кононович, О.В. Кочетков За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – С. 234.
4. Shon Harris, Fernando Mayumi. Praise for CISSP® All-in-One Exam Guide Copyright © 2019 by McGraw-Hill Education. - 1692
- 6 Лахно В.А., Васіліу Є.В. та ін. Методи та засоби захисту інформації [Навчальний посібник] – К.: ЦП «Компринт» О.В., 2021. 444 с.1. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків:НТМТ, 2014. –298с.
7. Information Technology – Practice for Information Security Management. International Standard ISO/IEC 17799:2000(E).

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 13⁰⁰ до 14³⁰ год., ауд. 250 або zoom – доц. І.А.Кіреєв

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, лабораторних 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 <https://e-learning.suitt.edu.ua/course/view.php?id=928>