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

Кірєєв 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	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КФ3.Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ5.Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ7.Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ10.Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
Результати навчання	ПРН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передач даних. 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. ПРН34.Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН36. Виявляти небезпечні сигнали технічних засобів. ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредити ЄКТС 120 годин
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 4-му семестрі

Програма дисципліни

Тема 1.	***Цілі та задачі курсу архітектура та моделі безпеки КС, основні поняття .*** 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.	***Функціонування комп'ютерної системи. Принципи побудови ПК .*** 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.	***Многопроцесорна обробка. Архітектура операційної системи .*** 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.	***Управління пам'яттю, структура , ієрархія пам'яті..*** Управління пам'ятою, 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.	***Сінхронний і асінхронний ввод-вивод інформації в КС .*** Методи, які використовуються при ізоляції процесів: інкапсуляція об'єктів, тимчасове мультиплексування, поділ імен, віртуальне отображеніе. Порти вводу- виводу комп'ютерної системи. Драйвера, стикі, інтерфейси і протоколи обміну. Мережеві протоколи. Периферійні пристрої комп'ютерних систем.
Тема 6.	***Віртуальна пам'ять і віртуальні машини .*** 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.	***Архітектура операційної системи. Монолітна та багаторівнева архітектура ОС .*** 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).
Тема 8.	***Додаткові пристрої зберігання. Класифікація.*** 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.
Тема 9.	***Архітектура системи. Підмножини суб'єктів і об'єктів.*** 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 привілегій.
Тема 10.	***Методи розмежування і управління доступом: діскреційна, мандатна і рольова моделі. Матриця контролю доступу*** 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.
Тема 11.	***Матриця контролю доступу. Цілі моделей цілістності.*** Модель інформаційних потоків. Рівні безпеки. Приховані канали (covert channel). Типи прихованих каналів: по пам'яті і по часу. багаторівнева безпека - модель невліяння. Сітчаста модель , межі доступу в сітчастої 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 .
Тема 12	***Динамічне управління доступом. Модель Graham-Denning та Harrison-Ruzzo-Ulman.*** 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).
Тема 13.	***Програмні та апаратні охоронці. Довіра і гарантії.*** Методи оцінки систем. Помаранчева Книга. Система класифікації TCSEC. Рівні гарантій: A - перевірений захист , B - мандатний захист , C - діскреційний захист , D - мінімальна безпека . Помаранчева книга і райдужна серія. Червона книга. ITSEC. Загальні критерії.
Тема 14.	***Сертифікація і акредитація (поняття, визначення). Нормативні документи та вимоги до них .*** Види та мета сертифікації продукції в державній системе сертифікації. Обов'язкова та добровільна сертифікація. Сертифікати відповідності та свідоцтва. Аккредітація. План акредитації. Узгодження плану, вимоги для акредитації. Оцінка документів для акредитації.

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., Василіу 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 2024 року з 13^{00} до 14^{30} год., ауд. 250 або zoom – доц. І.А. Кірєєв

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, 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