КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
_____ Наталія ТМЄНОВА
(підпис)
«____» _____ 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для здобувачів освіти

галузь знань	**12 «Інформаційні технології»**
спеціальність	**126 «Інформаційні системи та технології»**
освітній рівень	**бакалавр**
освітня програма	**«Програмні технології інтернет речей»**
вид дисципліни	**обов'язкова**
Форма навчання	**денна**
Навчальний рік	**2024/2025**
Семестр	**3**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладачі: доцент кафедри, к.т.н. Олена СІПКО

Пролонговано: на 2024/2025 н.р. _____ (О. ДРУЖИНІНА) «25» 06 2025 р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»____ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»____ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2024

Розробник: Олена СІПКО., к.т.н., доцент кафедри інформаційних систем та технологій

ЗАТВЕРДЖЕНО
В.о. завідувача кафедри
інформаційних систем та технологій
_____ Володимир ДРУЖИНІН
протокол № 10.23/24 від «27» червня 2024 р.

Схвалено науково-методичною комісією факультету інформаційних технологій

Протокол № ___ від «27» червня 2024 р.

Голова науково-методичної комісії _____ (Галина КРАСОВСЬКА)

«___» _____ 2024 року.

Програму перевірено

1. Мета та завдання дисципліни

Мета дисципліни — формування у студентів теоретичних знань та практичних навичок, необхідних для створення умов, що запобігають розголошенню, витоку і неправомірному оволодінню конфіденційною інформацією, а також запобігають протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

- Володіти навичками: застосування сучасних інформаційних технологій.

3. Анотація навчальної дисципліни:
Навчальна дисципліна «Основи інформаційної безпеки» забезпечує дослідження способів, методів, засобів і каналів реалізації загроз безпеки на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації. Під час вивчення дисципліни розглядається історія, стан та основні тенденції інформаційної безпеки в світі. Аналізуються особистий, корпоративний, відомчий, державний, міжнародний рівні інформаційної безпеки в розрізі трьох аспектів: цілісність, конфіденційність, доступність. Приділяється увага менеджменту інформаційної безпеки, побудові структури підрозділів, визначенню вимог до посадових осіб та вимогам міжнародних та вітчизняних стандартів інформаційної безпеки. Розглядаються основні загрози інформації. Вивчаються законодавчий, адміністративний, процедурний ти програмно-технічний рівні інформаційної безпеки. Курс інтегрований до курсу академії Cisco – Cybersecurity Essentials. Всі здобувачі отримують безкоштовний доступ до курсу, а за результатами успішного проходження курсу – отримують сертифікат.

4. Завдання (навчальні цілі): Основне завдання вивчення дисципліни полягає в опануванні студентами необхідних знань і практичних навичок використання існуючих засобів для забезпечення захисту інформації в IT системах, в тому числі і для IoT речей. Основними завданнями вивчення дисципліни є аналізування інформаційних потоків на підприємстві та визначення загроз; використання сучасних інформаційних систем та технологій, методик й технік кібербезпеки під час виконання функціональних завдань та обов’язків; аналіз інформаційних ризиків та розроблення політики безпеки; визначення та формулювання задач захисту інформації; користування нормативною базою для вирішення задач забезпечення інформаційної безпеки; обґрунтовування застосування методів та засобів забезпечення інформаційної безпеки; користування науковою та довідковою літературою за напрямком дисципліни.

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. Вміти; 3. Комунікація; 4. Автономність та відповідальність)		*Форми (та / або методи і технології) викладання і навчання*	*Методи оцінювання та пороговий критерій оцінювання*	*Відсоток у підсумковій оцінці з дисципліни*
Код	Результат навчання			
1.1	Знати проблеми інформаційної безпеки та технології безпеки даних..	*Лекція, лабораторна робота, самостійна робота, дискус, аналітична доповідь, проходження курсу академії Cisco Cybersecurity Essentials*	*Завдання на виконання лабораторних робіт, тестування, іспит*	*10%*
1.2	Знати базові технології мережевої безпеки.			*10%*
1.3	Знати принципи багаторівневого захисту корпоративних інформаційних систем, технології виявлення та запобігання вторгнень, управління інформаційною безпекою			*10%*
1.4	Знати складові кібербезпеки: конфіденційність, цілісність, доступність			*10%*
2.1	Вміти програмно реалізовувати алгоритми захисту інформації.			*15%*
2.2	Вміти вибирати методи захисту інформації і застосовувати їх на практиці для захисту інформації від несанкціонованого доступу.			*15%*
2.3	Вміти налагоджувати систему для безпечної роботи			*10%*
3.1	Вміти презентувати, обговорювати та захищати власні погляди в усній і письмовій формах та за допомогою інформаційно-комунікаційних технологій.			*20%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни (код) **Програмні результати навчання (назва)**	**1.1**	**1.2**	**1.3**	**1.4**	**2.1**	**2.2**	**2.3**	**3.1**
ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня для розв'язання задач проектування і використання інформаційних систем та технологій.	+	+	+	+	+	+	+	+
ПР 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.		+	+		+			+
ПР 8. Застосовувати правила оформлення проектних матеріалів інформаційних систем та технологій, знати склад та послідовність виконання проектних робіт з урахуванням вимог відповідних нормативно-правових документів для запровадження у професійній діяльності.	+		+					+
ПР 9. Здійснювати системний аналіз архітектури підприємства та його ІТ- інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.					+	+	+	
ПР 19. Використовувати можливості апаратного забезпечення, використовувати можливості операційних систем, використовувати можливості мережевих програмних систем, забезпечувати захищеність програм і даних від несанкціонованих дій.			+		+			

7. Схема формування оцінки:

7.1. Форми оцінювання: рівень досягнення всіх запланованих результатів навчання визначається за результатами виконання та захистів індивідуальних лабораторних робіт, виконанні самостійної роботи, участі в дискусах, підготовці та виступах з аналітичними доповідями, тестування, проходження курсу академії Cisco Cybersecurity Essentials з отриманням сертифікату та підсумкового оцінювання.

Питома вага результатів навчання у підсумковій оцінці за умови її опанування на належному рівні наступні:

- результати навчання – 1 (знання) РН 1.1. - РН 1.4. – до 40%;
- результати навчання – 2 (вміння) РН 2.1. - РН 2.3. – до 40%;
- результати навчання – 3 (комунікація) РН 3.1. – до 20%.

7.2. Організація оцінювання:

Семестрове оцінювання: ***60 балів (60%)***

Оцінка за семестр формується шляхом успішного виконання та захисту лабораторних робіт, проходження тестування по кожній темі.

Поточне оцінювання проводиться у формі опитування студентів за темами попередніх лекцій, темами лабораторних робіт чи темами домашнього завдання, проміжного тестування. Здобувач виконує та захищає 12 лабораторних робіт, що оцінюються від 2 до 4 балів за 1 роботу.

Якщо здобувач не вчасно виконує практичну роботу, то оцінка знижується на 0,5 бали за кожен тиждень протермінування. Робота вважається зданою вчасно, коли захист відбувається на наступній парі після видачі завдання, якщо викладачем не повідомлено інші терміни. Терміни здачі викладач оголошує та викладає окремим повідомленням в класі системи Microsoft Teams (чи інших затверджених кафедрою системах навчання).

Протягом семестру проводиться проміжний контроль у формі тестування за тематикою лекційних занять. Оцінюється від 7 до 12 балів.

Здобувач допускається до семестрового контролю при наявності конспекту лекцій, всіх зданих і захищених лабораторних робіт, успішно складених тестів по всім розділах. Обов'язковим для проміжного контролю є виконання лабораторних робіт, передбачених робочою програмою навчальної дисципліни у визначені терміни.

У випадку відсутності здобувача з поважних причин відпрацювання та перездачі модульних контрольних робіт здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року.

Підсумкове оцінювання *у* формі іспиту: складає *40 модульних балів* *(40% від загального рейтингу).* Екзаменаційне оцінювання проводиться в письмово-усній формі. Екзаменаційні питання охоплюють всі теми семестрового курсу дисципліни.

Здобувач не допускається до екзамену, якщо під час семестру набрав менше 36 балів. Для здобувачів, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум (36 балів), для допуску до екзамену обов'язковими є перездача тестів, виконання та захист запланованих лабораторних робіт на позитивну оцінку.

Оцінка за екзамен не може бути меншою **24 балів** для отримання позитивної оцінки за дисципліну.

Підсумкова оцінка визначається шляхом підсумовування балів семестрової роботи та екзамену. Якщо у підсумку студент набрав менше 60 балів, йому ставиться оцінка «незадовільно».

При простому розрахунку отримаємо:

	Лабораторні роботи	Аналітична доповідь, дискусія, тести по лекціях, проходження курсу академії Cisco Cybersecurity Essentials.	Екзамен	Підсумкова оцінка
Мінімум	29	7	24	60
Максимум	48	12	40	100

7.3 Таблиця відповідності оцінок

За національною шкалою	За 100-бальною шкалою
Відмінно / Excellent	90-100
Добре / Good	85-89
	75-84
Задовільно / Satisfactory	65-74
	60-64
Незадовільно / Fail	35-59
	0-34

8. Структура навчальної дисципліни.

№ п/п	Назва лекції	Кількість годин		
		Лекції	**Лабораторні**	**СР**
1	Аналіз загроз інформаційної безпеки.	1	2	4
2	Політика інформаційної безпеки.	1	2	4
3	Стандарти інформаційної безпеки.	1	2	4
4	Криптографічний захист інформації.	1	2	6
5	Технологія автентифікації. Протоколи захисту.	2	2	4
6	Технології захищених мереж.	1	2	6
7	Шифрування, приховування, маскування інформації	2	4	6
8	Симетричне та асиметричне шифрування. Відкриті та закриті ключі.	2	3	6
9	Безпека операційних систем.	2	3	6
10	Виявлення та запобігання вторгнень.	1	3	4
11	Технології захисту від шкідливих програм та спаму.	2	3	6
12	Управління засобами забезпечення інформаційної безпеки.	1	4	6
13	Забезпечення безпеки хмарних технологій.	1	2	4
	ВСЬОГО ЗА СЕМЕСТР	**18**	**34**	**66**

Загальний обсяг 120 *год.,* в тому числі:
Лекцій – 18 *год.*
Лабораторні заняття - 34 *год.*
Консультації - 2 *год.*
Самостійна робота - 66 *год.*

9. Рекомендовані джерела:

Основна: *(Базова)*

1 Савченко Ю.Г., Хлобистова О.А., Гладка М.В. Технології захисту інформації: навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» заочної та скороченої форми навчання. – К.: НУХТ, 2013. – 84 с.

2 Є.Яковенко, І. Журавель, І. Горбатий, А. Бондарєв. Інформаційна безпека. Львівська політехніка. Львів, 2019. – 580 с.

3 Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.

4 Остроухов В.В., Присяжнюк М.М., Фармагей О.І., Чеховська М.М. Інформаційна безпека. Підручник. Ліра-К. – К.-2021. – 412с.

5 Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Магнолія 2006., К.2021.–450с.

6 Roman V. Yampolskiy. Artificial Intelligence Safety and Security. CRC Press, 2018. – 444 p.

7 Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД "Гельветика", 2017. – 168 с

8 Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. –КІІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с

9 Комплексна безпека інформаційних мережевих систем: навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 256 с.

10 В.П. Бабак, О.Г. Корченко. Інформаційна безпека та сучасні мережеві технології. – К. : НАУ, 2003. – 670 с.

Додаткова:

1 Закон України «Про захист інформації в автоматизованих системах»

2 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації від несанкціонованого доступу

3 НД ТЗІ Класифікація автоматизованих систем і стандартні профілі захищеності опрацьованої інформації від несанкціонованого доступу.

4 Широчин В. П., Широчин С. В., Мухін В. Є. Основи безпеки комп`ютерних систем. К.: «Корнійчук». 2009 р. - 285 с.

5 Орлов П.І.. Інформація та інформатизація. – Харків: НУВС. - 2003.- 723с.

6 Задирака В.К., Олексюк О.С. Методи захисту фінансової інформації: Навчальний посібник. - Тернопіль: "Збруч", 2000. - 460с.

7 Інформаційна безпека. Практикум /В. М. Ахрамович., В. В. Козлов; Націон. акад. статистики, обліку та аудиту. – К. : ДП «Інформ. – аналіт. агентство», 2015. – 340 с. іл. – Бібліограф.: 337 с.

8 Ахрамович В.М., Чегренец В.М. Інформаційна безпека. Практикум / В.М.Ахрамович., В.М. Чегренец; Державного університету телекомунікацій. – К.:ДУТ, 2017. – 396 с. іл. – Бібліограф.:393 с.

9 ДСТУ ISO/IEC TR 13335-1-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT).

10 ДСТУ ISO/IEC TR 13335-2-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (ISO/IEC TR 13335-2:1997, IDT).

11 ДСТУ ISO/IEC TR 13335-3-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT (ISO/IEC TR 13335-3:1998, IDT).

10. Додаткові ресурси:

Курси академії Cisco: Introduction to Cybersecurity, Cybersecurity Essentials.