

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет радіофізики, електроніки та комп'ютерних систем

Кафедра комп'ютерної інженерії

«ЗАТВЕРДЖУЮ»

Заступник декана з навчальної роботи

_____ Світлана ЄФІМЕНКО

« ____ » _____ 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Безпека комп'ютерних мереж та систем
для студентів**

галузь знань
спеціальність
рівень вищої освіти
освітньо-наукова програма
вид дисципліни

F Інформаційні технології
F7 Комп'ютерна інженерія
другий (магістерський)
Комп'ютерні системи та мережі
вибіркова

Форма навчання	Денна
Навчальний рік	2025/2026
Семестр	4
Кількість кредитів ECTS	5
Мова викладання	українська
Форма заключного контролю	залік

Викладач:

Віталій МАР'ЯНОВСЬКИЙ, кандидат тех. наук, асистент кафедри комп'ютерної інженерії

Пролонговано: на 20__/20__ н. р. _____ (_____) « ____ » _____ 20__ р.

на 20__/20__ н. р. _____ (_____) « ____ » _____ 20__ р.

Розробник:

Віталій МАР'ЯНОВСЬКИЙ, кандидат тех. наук, асистент кафедри комп'ютерної інженерії

«ЗАТВЕРДЖЕНО»

Завідувач кафедри комп'ютерної інженерії

_____ **Юрій БОЙКО**

Протокол № ____ від « ____ » _____ 2025 р.

Схвалено науково-методичною комісією факультету радіофізики, електроніки та комп'ютерних систем

Протокол № ____ від « ____ » _____ 2025 р.

Голова науково-методичної комісії

Сергій РАДЧЕНКО

« ____ » _____ 2025 року.

ВСТУП

1. Мета дисципліни – є вивчення принципів захисту кінцевих пристроїв та мережевого обладнання від втручань та спроб вивести з ладу можливостями мережевого обладнання.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

Навчальна дисципліна «Безпека комп'ютерних мереж та систем» використовує знання циклу дисциплін «Комутація та маршрутизація в комп'ютерних мережах», «Англійська мова в галузі інформаційних технологій».

3. Анотація навчальної дисципліни:

У програмі дисципліни розглядається шляхи підвищення безпеки в мережах використовуючи можливості мережевого обладнання. По відношенню до місцезнаходженні зловмисника атаки можна розділити на атаки в середині мереж та ззовні.

Інструментами боротьби з зовнішніми атаками мають біти периферійні пристрої, які здатні виконують відповідну фільтрацію та контроль даних що передаються. Методи захисту ґрунтуються на особливостях кінцевого обладнання, захист якого необхідно забезпечити. Існує велика кількість різноманітних інструментів та механізмів захисту від зовнішніх втручань. Успішність захисту та контролю залежить від їх правильного використання.

Захист від внутрішніх атак ускладнених тим, що немає єдиної точки мережі до якої можна застосувати фільтрацію та контроль. В таких випадках безпека ґрупується на можливостях все існуючої мережевої інфраструктури, а саме комутаційного обладнання.

4. Завдання навчальної дисципліни (навчальні цілі):

1. Надати основні відомості курсу «Безпека комп'ютерних мереж та систем», які складають важливу частину підготовки студентів за спеціальністю «Комп'ютерна інженерія».
2. Навчити застосовувати основні відомості курсу у професійній діяльності, розвивати у студентів аналітичне мислення та науковий підхід.
3. Навчити застосовувати отримані знання та вміння в побудові захищених мереж та підтримці роботи систем виявлення вторгнень.
4. Дисципліна спрямована на формування програмних компетентностей:
 - ЗК3. Здатність проводити дослідження на відповідному рівні.
 - ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
 - СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.
 - СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.
 - СК11. Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

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 (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	Результат навчання			
1	знати:	лекційні заняття	письмові модульні контрольні роботи та залік	до 50
1.1	Принципи налаштування міжмережевих екранів	лекція	Залік, контрольні роботи, завдання для самостійної роботи	10
1.2	Принципи роботи систем виявлення та уникнення вторгнень	лекція	Залік, контрольні роботи, завдання для самостійної роботи	5
1.3	Класифікацію та відмінності різних типів міжмережевих екранів	лекція	Залік, контрольні роботи, завдання для самостійної роботи	10
1.4	Протоколи та механізми захисту при побудові віртуальних приватних мереж	лекція	Залік, контрольні роботи, завдання для самостійної роботи	5
1.5	Механізми захисту локальних мереж на основі можливостей керованих комутаторів	лекція	Залік, контрольні роботи, завдання для самостійної роботи	10
1.6	Принципи автентифікації, авторизації та обліку для задачі дистанційного доступу та керування мережим обладнанням	лекція	Залік, контрольні роботи, завдання для самостійної роботи	10
2	вміти:	Лабораторні роботи	письмові модульні контрольні роботи	до 40
2.1	Впроваджувати механізми захисту комутаторів та маршрутизатор	Лабораторна робота	МКР	10
2.2	Будувати віртуальні приватні мережі	Лабораторна робота	МКР	10
2.3	Виявляти загрози на основі систем уникнення вторгнень	Лабораторна робота	МКР	5
2.4	Забезпечити ізоляцію та захист кінцевих пристроїв від інших учасників локальної мережі	Лабораторна робота	МКР	10
2.5	Впроваджувати розроблені політики безпеки з системи захисту мережі	Лабораторна робота	МКР	5
3	комунікація:	Лекційні заняття та лабораторні роботи	письмові модульні контрольні роботи та залік	до 5
3.1	Готовність до конструктивної наукової дискусії і обговоренню технічних питань, необхідних для вирішення комплексної задачі	Лабораторна робота	МКР	2
3.2	Здатність адекватно доводити і обґрунтовувати свою точку зору з дотриманням загальноприйнятих норм етики	Лабораторна робота	МКР	3
4	автономність та відповідальність:	лекційні заняття	письмові модульні контрольні роботи	до 5
4.1	Здатність до самостійного забезпечення повного життєвого циклу систем та мереж	лекція	МКР	5

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни	Код													
	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	2.4	2.5	3.1	3.2	4.1
Програмні результати навчання (назва)														
ПРН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	+		+	+	+	+	+	+	+	+				
ПРН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.		+									+	+	+	
ПРН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.														+

7. Схема формування оцінки

7.1. Форми оцінювання

Рівень досягнення всіх запланованих результатів навчання визначається за результатами виконання лабораторних робіт, написання письмових контрольних робіт та залікової роботи. Внесок результатів навчання у підсумкову оцінку, за умови їх опанування на належному рівні:

- результати навчання 1.1 – 1.6 [знання] – до 50 %;
- результат навчання 2.1 – 2.5 [вміння] – до 40%;
- результат навчання 3.1-3.2 [комунікація] – до 5%;
- результат навчання 4.1 [автономність та відповідальність] – до 5%;

Форми оцінювання:

- **семестрове оцінювання:** Навчальний семестр має два змістовні модулі. Після завершення кожного теми проводяться письмові модульні контрольні роботи. Перший змістовий модуль є результатом проведення оцінювання знань за перші чотири теми. Другий змістовий модуль є результатом оцінювання наступних чотирьох тем. Обов'язковим для допуску до заліку є: виконання лабораторних робіт з оцінкою не менше 24 та написання модульних контрольних робіт з сумарною кількістю балів не менше 12.
- **підсумкове оцінювання (у формі заліку):** форма заліку – письмова. Письмова робота складається з тесту, питання оцінюються відповідно до коефіцієнтів в залежності від їх складності. Всього за залік можна отримати від 0 до 40 балів. Умовою досягнення позитивної оцінки за дисципліну є отримання не менш ніж 60 балів, оцінка за залік не може бути меншою **24 балів**.
- **умови допуску до підсумкового оцінювання:** умовою допуску до заліку є отримання студентом сумарно не менше, ніж *критично-розрахунковий мінімум* за семестр, 36 балів. студенти, які протягом семестру сумарно набрали меншу кількість балів, ніж критично-розрахунковий мінімум у **36 балів**, для одержання допуску до заліку обов'язково повинні виконати додаткове завдання за тематикою лабораторних робіт.

У випадку відсутності студента з поважних причин відпрацювання та перездачі модульних контрольних робіт допуск до заліку здійснюється у відповідності до “Положення про організацію освітнього процесу у Київському національному університеті”

7.2. Організація оцінювання;

Оцінювання за формами контролю:

Семестрова робота	Кількість балів	
	Min. – 36	Max. – 60
Модульна контрольна робота 1	6	10
Модульна контрольна робота 2	6	10
Лабораторні роботи	24	40

Орієнтований графік оцінювання:

Форма оцінювання	Орієнтовний період для здійснення відповідної форми оцінювання
Модульна контрольна робота 1	березень
Модульна контрольна робота 2	квітень
Робота на лабораторних	з лютого по квітень
Залік	травень

Розрахунок балів, які отримують при успішній здачі заліку:

Значення	Протягом семестру	Залік	Підсумкова оцінка
Мінімум	36	24	60
Максимум	60	40	100

7.3. Шкала відповідності оцінок

Оцінка (за національною шкалою) / National grade	Рівень досягнень, % / Marks, %
Зараховано / Passed	60 – 100%
Не зараховано / Fail	0 – 59%

8. Структура навчальної дисципліни. Тематичний план лекційних занять

№ з/п	Назва теми	Кількість годин		
		Лекції	Лабораторні роботи	Самостійна робота
1	Сучасні загрози в мережах	2	2	10
2	Захист мережевого обладнання	2	2	10
3	Автентифікація, авторизація, облік	4	2	20
4	Впровадження міжмережевих екранів	4	2	10
5	Захист в локальних мережах	4	2	10
6	Віртуальні приватні мережі	4	4	10
7	Системи виявлення та уникнення вторгнень	4	2	10
8	Порівняння методів та засобів захисту різних виробників мережевого обладнання на прикладі Cisco, Fortinet, Huawei	2	2	10
9	Принципи керування безпекою мережі	4	2	10
Всього		30	20	100

Загальний обсяг **150** год., в тому числі:

Лекції **30** год.

Лабораторні роботи **20** год.

Самостійна робота **100** год.

9. Рекомендована література:

Основні джерела:

- [1] Network Security [Електронний ресурс] – Режим доступу до ресурсу: <https://www.netacad.com/courses/cybersecurity/network-security> (для авторизованих користувачів).

- [2] Thomas M. Thomas, Donald Stoddard. Network Security First-Step, 2nd Edition. Cisco Press. 2011. – 448 с.
 - [3] Микитишин А.Г. Комп'ютерні мережі [навчальний посібник] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006». – 256 с.
 - [4] Wendell Odom. CCNA Routing and Switching 200-125 Official Cert Guide Library. Published Jul 26, 2016 by Cisco Press
 - [5] Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с
 - [6] Семенов С.Г. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко – Х.: НТУ «ХПІ», 2014. – 251 с.
 - [7] Кавун С.В. Основи інформаційної безпеки / С.В. Кавун, О.А. Смірнов, В.Ф. Столбов Кіровоград : Вид. КНТУ, 2012. - 414 с.
 - [8] Смірнов О.А. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. - Кіровоград, 2010.- 322 с.
- Додаткові джерела:**
- [9] Kevin Wallace. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Published Dec 9, 2014 by Cisco Press
 - [10] Jeff Doyle, Jennifer DeHaven Carroll. Routing TCP/IP, Volume 1, 2nd Edition. Published Oct 19, 2005 by Cisco Press
 - [11] Буров Є.В. Комп'ютерні мережі. Підручник (затв. МОН України), 2015, 262 ст.
 - [12] Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
 - [13] Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
 - [14] Бабенко Т.В. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. Д.: Національний гірничий університет, 2013. 318 с.
 - [15] Yusuf Bhajji. Network Security Technologies and Solutions (CCIE Professional Development Series). 2016 by Cisco Press. Part of the CCIE Professional Development series., 2016. – 840 с.