КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет радіофізики, електроніки та комп'ютерних систем
Кафедра комп'ютерної інженерії

«ЗАТВЕРДЖУЮ»

Заступник декана з навчальної роботи

_____ Наталія ГОРБОВЦОВА

« ____ » _____ 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації у комп'ютерних системах

галузь знань	12 Інформаційні технології
спеціальність	123 Комп'ютерна інженерія "
рівень вищої освіти	перший освітньо-науковий
освітньо-наукова програма	"Інженерія комп'ютерних систем і мереж"
вид дисципліни	Вибіркові компоненти вибору студентів ОП

Форма навчання	денна
Навчальний рік	2023/2024
Семестр	7
Кількість кредитів ECTS	4
Мова викладання	українська
Форма заключного контролю	залік

Викладач:
Олександр БОРЕЦЬКИЙ, кандидат технічних наук, асистент кафедри комп'ютерної інженерії

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

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

КИЇВ – 2023

Розробник:
Олександр БОРЕЦЬКИЙ, кандидат технічних наук, асистент кафедри комп'ютерної інженерії

«ЗАТВЕРДЖЕНО»

Завідувач кафедри комп'ютерної інженерії

_____ Юрій БОЙКО

Протокол № __ від « ___ » _____ 2023 р.

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

Протокол № ___ від « ___ » _____ 2023 р.

Голова науково-методичної комісії Сергій РАДЧЕНКО

« ___ » _____ 2023 р.

ВСТУП

1. Мета дисципліни «Захист інформації у комп'ютерних системах» є отримання знань та практичних навичок в області захисту інформації та кібербезпеки.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

Навчальна дисципліна «Захист інформації у комп'ютерних системах» базується на циклі дисциплін професійної та практичної підготовки. До вивчення дисципліни «Захист інформації у комп'ютерних системах» необхідно пройти підготовку і скласти іспити/заліки з таких дисциплін:
«Апаратне та програмне забезпечення комп’ютерних систем», «Програмування», «Комп’ютерні мережі», «Системне програмне забезпечення» «Вища математика».

Попередні вимоги:

студент повинен знати: вищу математику, програмно-апаратний склад персонального комп’ютера, операційні системи, комп’ютерні мережі, програмування.

студент повинен вміти: користуватися персональним комп’ютером, використовувати гіпервізор для налаштування віртуальних машин та мережі між ними, встановлювати ОС та системне програмне забезпечення у віртуальних машинах, налаштування системного програмного забезпечення.

3. Анотація навчальної дисципліни: Навчальна дисципліна «Захист інформації у комп'ютерних системах» входить у блок дисциплін за вибором з переліку спеціальності «комп’ютерна інженерія» (студент обирає 2 або більше дисципліни з кожного переліку). Матеріал дисципліни «Захист інформації у комп'ютерних системах» є базовим для подальшого вивчення та вдосконалення в магістратурі зі спеціальності «123 Комп’ютерна інженерія».

Курс охоплює теоретичні відомості, організаційні підходи та практичні засоби захисту інформації в сучасних комп’ютерних системах і різних елементів криптографічного захисту інформації у комп’ютерних систем. Під час виконання лабораторних робіт студенти отримують практичні навички використання програмних інструментів аудиту безпеки комп’ютерних систем та роботи з алгоритмами шифрування і аутентифікації.

В курсі робиться акцент на комплексний підхід до організації всіх аспектів захисту інформації у комп’ютерних системах.

4. Завдання навчальної дисципліни (навчальні цілі):

1. Надати основні відомості курсу «Захист інформації в комп’ютерних системах», які складають професійну частину інженерної підготовки студента-бакалавра за спеціальністю «Комп’ютерна інженерія».
2. Узагальнювати й систематизувати знання щодо вразливостей та підходів до захисту сучасних обчислювальних систем, навчити основам аудиту комп’ютерної безпеки, простежити взаємозв’язок усіх елементів побудови

комплексних засобів захисту комп’ютерних систем; продемонструвати застосування теоретичних відомостей до розв’язання практичних задач.

3. Навчити застосовувати знання, уміння, навички і комунікації у професійній діяльності, розвивати логічне мислення та аналітичний підхід студентів.

4. Навчити застосовувати отримані знання та уміння в побудові та експлуатації захищених комп’ютерних систем.

Дисципліна спрямована на формування програмних компетентностей:

– ЗК2. Здатність вчитися і оволодівати сучасними знаннями.
– ЗК3. Здатність застосовувати знання у практичних ситуаціях.

– ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти 3 метою здійснення професійної діяльності в галузі комп’ютерної інженерії.
– ФК4. Здатність забезпечувати захист інформації, що обробляється в комп’ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.
– ФК8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об’єктах різного призначення.
– ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.
– ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.
– ФК13. Здатність вирішувати проблеми у галузі комп’ютерних та інформаційних технологій, визначати обмеження цих технологій.

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	до 45
1.1	Принципи захисту інформації в комп'ютерних системах	*лекція*	МКР	6
1.2	Основні методи та засоби для аудиту безпеки комп'ютерних систем	*лекція*	МКР	6
1.3	Принципи роботи механізмів захисту на рівні операційних систем	*лекція*	МКР	6
1.4	Основні методи криптографічного захисту інформації	*лекція*	*МКР*	*6*
1.5	Структуру типових криптографічних шифрів	*лекція*	МКР	6
1.6	Принцип роботи інфраструктури відкритих ключів	*лекція*	МКР	6
1.7	Теорію криптографічних протоколів	*лекція*	МКР	9
2	**вміти**:	*лекційні заняття, лабораторні роботи*	письмові модульні контрольні роботи	до 45
2.1	Використовувати програмне забезпечення для аудиту комп'ютерних систем	*лекція/лабораторні роботи*	МКР	11
2.2	Працювати з базами даних вразливостей програмного забезпечення	*лекція/лабораторні роботи*	МКР	11
2.3	Налаштовувати засоби захисту інформації на рівні операційної системи	*лекція/лабораторні роботи*	МКР	11
2.4	Працювати з криптографічними бібліотеками для створення надійного каналу зв'язку	*лекція/лабораторні роботи*	МКР	12
3	**комунікація:**	лекційні заняття	письмові модульні контрольні роботи	до 5
3.1	Здатність грамотно будувати професійну комунікацію як в усній, так і письмовій формах українською мовою, розуміти технічну термінологію англійською мовою.	*лекція*	МКР	2
3.2	Використовувати сучасні засоби комунікацій для ефективного спілкування на професійному та соціальному рівнях.	*лекція*	МКР	3
4	**автономія та відповідальність:**	лекційні заняття	письмові модульні контрольні роботи	до 5
4.1	Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати рішення у межах компетенції.	*лекція/лабораторні роботи*	МКР	2
4.2	Здатність використання в процесі навчання наукової літератури та інформації з відкритих джерел.	*лекція, самостійна робота*	МКР	3

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни / **Програмні результати навчання (назва)**	Код														
	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	3.1	3.2	4.1	4.2
ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.	+		+	+			+							+	+
ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.	+			+	+	+					+				
ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.	+	+								+					
ПРН14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів		+							+	+					
ПРН18. Використовувати інформаційні технології та для ефективного спілкування на професійному та соціальному рівнях.												+		+	+
ПРН21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.		+						+	+					+	+

7. Схема формування оцінки

7.1. Форми оцінювання

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

- результати навчання 1.1 – 1.7 [**знання**] – до 45 %;
- результат навчання 2.1 – 2.4 [**вміння**] – до 45%;
- результат навчання 3.1 – 3.2 [**комунікація**] – до 5%;
- результат навчання 4.1 – 4.2 [**автономність та відповідальність**] – до 5%;

Форми оцінювання:

- **семестрове оцінювання**: Навчальний семестр має два змістові модулі: у змістовий модуль 1 (ЗМ1) входять теми 1-5, у змістовий модуль 2 (ЗМ2) входять теми 6-13. Проміжний модульний контроль оцінюється в 20 балів.
- **підсумкове оцінювання (у формі заліку):** Заліковий білет складається із 4 відкритих питань. Кожне питання оцінюється від 0 до 10 балів. Всього за залікову роботу можна отримати від 0 до 40 балів. Умовою досягнення позитивної оцінки за дисципліну є отримання не менш ніж 60 балів, оцінка за іспит не може бути меншою 13 балів.
- **умови допуску до підсумкового заліку:** умовою допуску до заліку є отримання студентом сумарно не менше, ніж *критично-розрахунковий мінімум* за семестр. Студенти, які протягом семестру сумарно набрали меншу кількість балів, ніж критично-розрахунковий мінімум **20 балів**, для одержання допуску до заліку обов'язково повинні написати додаткову контрольну роботу.

У випадку відсутності студента з поважних причин відпрацювання та перездачі модульних контрольних робіт здійснюються 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.	Max.
Модульна контрольна робота 1	7	20
Модульна контрольна робота 2	7	20
Лабораторні роботи	6	20

Орієнтований графік оцінювання:

Форма оцінювання	Орієнтовний період для здійснення відповідної форми оцінювання
Модульна контрольна робота 1	жовтень
Модульна контрольна робота 2	листопад
Підсумкове оцінювання лабораторних робіт	грудень
Добір балів/додаткова контрольна робота	грудень
Іспит	грудень

Розрахунок балів, які отримують при успішній здачі іспиту:

Значення	Змістовні модулі	Лабораторні роботи	Іспит	Підсумкова оцінка
Мінімум	14	6	13	60
Максимум	40	20	40	100

7.3. Шкала відповідності оцінок

Оцінка (за національною шкалою) / National grade	Рівень досягнень, % / Marks, %
Відмінно / Excellent	60-100%
Незадовільно / Fail	0-59%

8. Структура навчальної дисципліни. Тематичний план лекційних занять

№ п/п	Назва теми	Кількість годин		
		Лекції	Лабораторні заняття	Самостійна робота
Змістовий модуль 1. «Захист інформації в сучасних комп'ютерних системах»				
1	Поняття безпеки в комп'ютерних системах	2	-	3
2	Найбільш поширені техніки атак на комп'ютерні системи	2	3	4
3	Вразливості програмного забезпечення	4	3	8
4	Безпека та засоби захисту на рівні операційної системи	4	4	4
5	Захист від атак на комп'ютерні системи в корпоративній мережі	2	-	8
	Всього	**14**	**14**	**35**
Змістовий модуль 2. «Криптографічний захист інформації»				
6	Вступ до криптографії	1	-	3
7	Математичні основи криптографії	2	-	2
8	Частотний аналіз текстів	1	6	4
9	Блочні шифри	2	6	4
10	Аутентифікація повідомлень	2		4
11	Протокол обміну ключами Діффі-Хеллмана	2	-	4
12	Rivest-Shamir-Adleman (RSA)	2	-	4
13	Керування ключами та криптографічні протоколи	2	2	2
	Всього	**14**	**14**	**27**

Загальний обсяг **120** год., в тому числі:
Лекції **28** год.
Лабораторні роботи **28** год.
Самостійна робота **64** год.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основні джерела:

[1] Hertzog, Raphaël, and Jim O'Gorman. *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. offsec Press, 2017.

[2] Kocher, Paul, et al. "Spectre attacks: Exploiting speculative execution." *arXiv preprint arXiv:1801.01203* (2018).

[3] Savard, John JG. "A cryptographic compendium." *John Savard's Home Page* 30 (1999).
[4] Гапак О.М. Методичні вказівки і завдання до лабораторних робіт з курсу «Захист інформації в комп'ютерних системах» для студентів 3-4-го курсу інженерно-технічного факультету спеціальності «комп'ютерна інженерія». – Ужгород: «АУТДОР-ШАРК», 2019. – 52 с.
[5] Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: BHV, 2009. – 608 с.

Додаткові джерела

[6] Остапов С.Е., Валь Л.О. Основи криптографії: навчальний посібник. Чернівці: Книги–XXI, 2008. – 188с.
[7] Schneier B. Applied cryptography, 1996 //Cover and title pages. – 1997. – Т. 125147.