НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»
Декан факультету інформаційних технологій

_____О. Г. Глазунова

«_____»_____20___р.

«СХВАЛЕНО»

на засіданні кафедри комп'ютерних наук

Протокол №_____від «_»_____20___р.
Завідувач кафедри
_____Б. Л. Голуб

"**РОЗГЛЯНУТО** "

Гарант ОП «Інформаційні управляючі системи та технології»

_____ проф., д.т.н., Бондаренко В. Є.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА І НАДІЙНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ

спеціальність 122 «Комп'ютерні науки**»**
освітня програма «Інформаційні управляючі системи та технології»

факультет інформаційних технологій

Розробник: к.т.н., доцент, доцент кафедри комп'ютерних наук , Пархоменко І. І.

Київ 2021

Опис навчальної дисципліни

Безпека і надійність комп’ютерних систем

Галузь знань, спеціальність, освітній ступінь	
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп’ютерні науки
Освітня програма	«Інформаційні управляючі системи та технології»
Освітній ступінь	Магістр
Характеристика навчальної дисципліни	
Вид	Обов’язкова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	2
Форма контролю	Іспит
Показники навчальної дисципліни для денної та заочної форм навчання	
	денна форма навчання
Рік підготовки	1
Семестр	2
Лекційні заняття	15 год.
Лабораторні заняття	30 год.
Самостійна робота	75 год.
Кількість тижневих годин для денної форми навчання: аудиторних самостійної роботи студента −	3 год.

1. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є оволодіти сучасними методами захисту інформації в комп'ютерних системах та мережах, особливостями їх апаратної та програмної реалізацій, отримання студентами знань з області теорії надійності, методів забезпечення надійності функціонування комп'ютерних систем

Завдання вивчення навчальної дисципліни

Завданнями вивчення навчальної дисципліни є:

- реалізувати захист конфіденційності інформації;
- здійснити захист цілісності інформації;
- організувати доступності інформації
- реалізовувати основні розрахункові моделі оцінки показників надійності апаратних і програмних засобів комп'ютерних систем

Місце навчальної дисципліни в системі професійної підготовки фахівця

На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних методах захисту інформації в комп'ютерних системах та мережах.

Інтегровані вимоги до знань і умінь з навчальної дисципліни

У результаті вивчення навчальної дисципліни студент повинен:

Знати:

- види загроз інформації в комп'ютерних мережах;
- основні протоколи безпеки;
- основні програмні засоби захисту інформації в комп'ютерних мережах;
- основні апаратні засоби захисту інформації в комп'ютерних мережах;
- засоби організації розмежування доступу комп'ютерних мережах;
- основні поняття теорії надійності;
- елементи та функції комп'ютерних систем;
- класифікацію відмов інформаційних систем;
- методи забезпечення надійності КС.

Вміти:

- підібрати тип та структуру локальної комп'ютерної мережі;
- підібрати комплекс необхідних апаратно-програмних засобів для комп'ютерної мережі;
- підібрати комплекс необхідних організаційних заходів, що попереджують можливий вплив дестабілізуючих факторів на інформацію, що захищається;
- досліджувати характеристики при миттєвих і поступових відмовах;
- визначати комплексні показники надійності КС;

- проводити діагностику і контроль на надійність обробки, передачі і зберігання інформації;
- реалізовувати методи забезпечення надійності функціонування КС

Перелік дисциплін, які необхідні для вивчення курсу.

- Проектування інформаційно-управляючих та інтелектуальних систем
- Стандартизація та сертифікація інформаційних технологій
- Технології розподілених систем та обчислень
- Архітектура комп'ютерів
- Методи та засоби комп'ютерних інформаційних технологій
- Технолгії захисту інформації
- Комп'ютерні мережі (локальні, корпоративні, глобальні)

Вивчення дисципліни «Безпека і надійність комп’ютерних систем» сприяє формуванню у студентів наступних компетентностей.

Загальні компетентності:

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК2. Здатність до пошуку, оброблення інформації з різних джерел.

ЗК3. Здатність вчитися, оволодівати сучасними знаннями та застосовувати їх у практичних ситуаціях.

ЗК4. Здатність до адаптації та дії в новій ситуації, виявляти, ставити та вирішувати проблеми.

ЗК5. Здатність проводити дослідження, оцінювати і забезпечувати якість виконуваних робіт, приймати обґрунтовані рішення та генерувати нові ідеї.

Фахові компетентності:

ФК9. Здатність до самостійної роботи. Здатність використовувати на практиці навички і вміння в організації науково-дослідних та виробничих робіт.

ФК15. Здатність до захисту об’єктів інтелектуальної власності в Україні та Світі.

ФК16. Здатність організовувати роботу відповідно до вимог безпеки життєдіяльності й охорони праці.

Це забезпечує досягнення програмних результатів навчання ПР1, ПР2, ПР15, ПР16.

2. Програма навчальної дисципліни

Модуль №1
Сервіси безпеки в інформаційно-комунікаційних системах

Тема №1.

Проблеми безпеки корпоративних інформаційних систем. Основні програмно-технічні заходи безпеки.

Основні поняття інформаційної безпеки. основні поняття програмно-технічного рівня інформаційної безпеки. Сервіси безпеки. Архітектурна безпека корпоративних мереж. Модель комп`ютерної мережі. Модель загроз безпеки. Модель протидії загрозам безпеки.

Тема №2

Ідентифікація та автентифікація. управління доступом в корпоративних мережах.

Функції ідентифікації та аутентифікації. Типи парольної аутентифікації. Надійність парольного захисту. Одноразові паролі. Сервер аутентифікації Kerberos. Ідентифікація/автентифікація за допомогою біометричних даних. Управління доступом. Дискреційне управління доступом. Мандатне управління доступом. Рольове управління доступом.

Тема №3

Екранування, аналіз захищеності. протоколювання і аудит.

Протидія несанкціонованому міжмережевому доступу. Фільтрація трафіку. Виконання функцій посередництва. Особливості міжмережевого екранування на різних рівнях моделі OSI. Шлюз сеансового рівня. Прикладний шлюз. Розробка політики міжмережевої взаємодії. Визначення схеми підключення міжмережевого екрану. Настройка параметрів функціонування брандмауера. Критерії оцінки міжмережевих екранів. Сучасні системи FireWall. Сервіс аналізу захищеності. Мережеві сканери. Антивірусний захист. Функції аудиту. Активний аудит.

Тема №4

Шифрування. Цифрові сертифікати. Контроль цілісності. Забезпечення доступності.

Криптографічні сервіси безпеки. Симетричне і асиметричне шифрування. Використання цифрових сертифікатів. Акредитований центр сертифікації ключів. Відкриті і закриті ключі. Алгоритми шифрування. Способи контролю цілісності. Основи заходів забезпечення високої доступності.

Тема №5

Тунелювання і керування.

Причини використання тунелювання. Віртуальні приватні мережі (VPN). Особливості використання тунелювання при застосуванні протоколів IPv4 та IPv6. Протокол IPSec. Управління компонентами і засобами безпеки. Моніторинг,

контроль та координація компонентів. Управління конфігурацією. Управління відмовами. Проактивне управління.

Модуль№2

Способи та методи забезпечення надійності функціонування КС

Тема №6.

Елементи теорії надійності

Значення та місце дисципліни в системі підготовки спеціалістів комп'ютерних наук. Загальні відомості про дисципліну, її зв'язок з іншими дисциплінами. Поняття надійності і безпеки. Основні визначення надійності та їх зміст.

Тема №7.

Методи забезпечення надійності.

Ймовірність безвідмовної роботи. Ймовірність відмови. Відновлювальні і не відновлювальні об'єкти. Методи структурної надлишковості. Часова налишковість.

Тема №8.

Надійність та контроль пристроїв комп'ютерних систем.

Класифікація методів контролю комп'ютерних систем. Резервування. Класичний метод резервування – мажоритарний. Коригувальні коди. Самодіагностика і автоматизоване технічне обслуговування на виходах цифрового пристрою.

Тема №9.

Інформаційна надлишковість як універсальний засіб контролю.

Традиційно поняття інформаційної надлишковості (ІН). Кодові методи функціонального контролю. Здатність виявлення або виправлення помилок. Апаратні витрати для виявлення і корекції помилок. Забезпечення селективність по відношенню до помилок, які корегуються.

Тема №10.

Забезпечення надійності обчислювальних процесів

Забезпечення відмовостійкості систем. Реалізації багатопроцесорної обробки. Моделі розподіленої пам'яті. Принцип «швидкого прояву несправності» (fail fast design). Міжмодульна синхронізація, синхронізація рівня ліній зв'язку, обробку помилок. Кластерні системи.

4. Структура навчальної дисципліни

№ п/п	*НАЗВА ТЕМИ*	Обсяг навчальних занять (Год.)				
		Всього	**Лекції**	**Лабор.**	**СРС**	**ІР**
1	***2***	***3***	***4***	***5***	***6***	***7***
1	Проблеми безпеки корпоративних інформаційних систем. Основні програмно-технічні заходи безпеки.	11	2	2	7	
2	Ідентифікація та автентифікація. управління доступом в корпоративних мережах.	13	2	4	7	
3	Екранування, аналіз захищеності. Протоколювання і аудит.	13	2	4	7	
4	Шифрування. Цифрові сертифікати. Контроль цілісності. Забезпечення доступності.	13	1	4	8	
5	Тунелювання і керування.	11	1	2	8	
	Модульна контрольна робота №1					
Всього за модулем №1		**61**	**8**	**16**	**37**	
6	Елементи теорії надійності. Основні визначення надійності та їх зміст.	11	2	2	7	
7	Методи забезпечення надійності	13	2	4	7	
8	Надійність та контроль пристроїв комп'ютерних систем.	13	1	4	8	
9	Інформаційна надлишковість як універсальний засіб контролю	11	1	2	8	
10	Забезпечення надійності обчислювальних процесів	11	1	2	8	
	Модульна контрольна робота №2					
Всього за модулем №2		**59**	**7**	**14**	**38**	
Усього за навчальною дисципліною		**120**	**15**	**30**	**75**	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Типи сценаріїв входу до мережі. Створення об’єкту користувача. Профілі користувачів.	2
2	Типи парольної аутентифікації. Сервер аутентифікації Kerberos. Управління доступом.	4
3	Визначення схеми підключення міжмережевого екрану. Встановлення і налаштування систем FireWall. Настройка параметрів функціонування брандмауера.	4
4	Встановлення та конфігурування центру сертифікації.	4
5	Реалізація протоколу IPSec в операційній системі.	2

	Налаштування VPN-каналу	
6	Розгляд функції надійності та функції розподілу. Способи визначення інтенсивності відмов.	2
7	Показники надійності відновлювальних та не відновлювальних об’єктів комп’ютерних систем. Коефіцієнт готовності. Реалізація структурної надлишковості на прикладі RAID-систем.	4
8	Визначення причин відмов і збоїв комп’ютерних систем. Способи реалізації методів контролю.	4
9	Розгляд способів визначення інформаційної надлишковості. Кодові методи функціонального контролю	2
10	Способи реалізації кластерних систем. Надійність програмного забезпечення.	2

6. Індивідуальні завдання

1. Проблеми безпеки корпоративних інформаційних систем.

2. Загрози безпеки інформаційних систем та мереж

3. Встановлення і конфігурування систем FireWall

4. Створення захищеного VPN з'єднання

5. Розподілу криптографічних ключів та засобів побудови захищених віртуальних мереж

6. Категорії надійності. Поняття надійності і безпеки.

7. Показники надійності відновлювальних об’єктів. Коефіцієнт готовності. Основні моделі теорії надійності.

8. Схема розрахунку надійності комп’ютерних систем. Оцінка надійності методом перетворення мереж.

9. Надійність відновлювальних нерезервованих систем при наявності однієї підсистеми та n підсистем.

10. Статистичне моделювання надійності програм.

7. Методи навчання

При викладанні дисципліни використовуються наступні методи навчання:

М1. Лекція (проблемна, інтерактивна)

М2. Лабораторна робота – для використання набутих знань до розв’язування практичних завдань;

М3. Проблемне навчання – створення проблемної ситуації для зацікавленого і активного сприйняття матеріалу.

М4. Проектне навчання (індивідуальне, малі групи, групове)

М5. Он-лайн навчання

8. Форми контролю

При викладанні дисципліни передбачені такі форми контролю:

МК1. Тестування

МК2. Контрольне завдання

МК4. Методи усного контролю

МК5. Екзамен

МК7. Звіт

Для студентів денної форми навчання: усне опитування (МК4) та експрес контроль (МК1) на лабораторних заняттях, захист індивідуальних лабораторних завдань (МК7), аудиторні модульні контрольні роботи (МК2).

9. Розподіл балів, які отримують студенти

Поточний контроль				Рейтинг з навчальної роботи $R_{НР}$	Рейтинг з додаткової роботи $R_{ДР}$	Рейтинг штрафний $R_{ШТР}$	Підсумкова атестація (екзамен чи залік)	Загальна кількість балів
Змістовий модуль 1	Змістовий модуль 2	Змістовий модуль 3	Змістовий модуль 4					
0-100	0-100	0-100	0-100	0-70	0-20	0-5	0-30	0-100

Примітки. 1. Відповідно до «Положення про кредитно-модульну систему навчання в НУБіП України», затвердженого ректором університету 03.04.2009 р., рейтинг студента з навчальної роботи $\mathbf{R_{НР}}$ стосовно вивчення певної дисципліни визначається за формулою

$$R_{НР} = \frac{0{,}7 \cdot (R^{(1)}_{ЗМ} \cdot К^{(1)}_{ЗМ} + \ ... + R^{(n)}_{ЗМ} \cdot К^{(n)}_{ЗМ})}{К_{ДИС}} + R_{ДР} - R_{ШТР},$$

де $\mathbf{R^{(1)}_{ЗМ}, \ldots R^{(n)}_{ЗМ}}$ − рейтингові оцінки змістових модулів за 100-бальною шкалою;

$\mathbf{n}$ − кількість змістових модулів;

$\mathbf{К^{(1)}_{ЗМ}, \ldots К^{(n)}_{ЗМ}}$ − кількість кредитів ECTS, передбачених робочим навчальним планом для відповідного змістового модуля;

$\mathbf{К_{ДИС} = К^{(1)}_{ЗМ} + \ldots + К^{(n)}_{ЗМ}}$ − кількість кредитів ECTS, передбачених робочим навчальним планом для дисципліни у поточному семестрі;

$\mathbf{R_{ДР}}$ − рейтинг з додаткової роботи;

$\mathbf{R_{ШТР}}$ − рейтинг штрафний.

Наведену формулу можна спростити, якщо прийняти $\mathbf{К^{(1)}_{ЗМ} = \ldots = К^{(n)}_{ЗМ}}$. Тоді вона буде мати вигляд

$$R_{НР} = \frac{0{,}7 \cdot (R^{(1)}_{ЗМ} + \ ... + R^{(n)}_{ЗМ})}{n} + R_{ДР} - R_{ШТР}.$$

Рейтинг з додаткової роботи $\mathbf{R_{ДР}}$ додається до $\mathbf{R_{НР}}$ і не може перевищувати 20 балів. Він визначається лектором і надається студентам рішенням кафедри за виконання робіт, які не передбачені навчальним планом, але сприяють підвищенню рівня знань студентів з дисципліни.

Рейтинг штрафний $\mathbf{R_{ШТР}}$ не перевищує 5 балів і віднімається від $\mathbf{R_{НР}}$. Він

визначається лектором і вводиться рішенням кафедри для студентів, які матеріал змістового модуля засвоїли невчасно, не дотримувалися графіка роботи, пропускали заняття тощо.

2. Згідно із зазначеним Положенням ***підготовка і захист курсового проекту (роботи)*** оцінюється за 100 бальною шкалою і далі переводиться в оцінки за національною шкалою та шкалою ECTS.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	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

10. Рекомендована література

1. Э. Мейфолд «Безопасность сетей» // Пер. с англ. // К.: «Диалектика», 2006. – 528 с.
2. Галатенко В.А Основы информационной безопасности - М.: Мир, 2008. -208 с.
3. Галатенко В.А Стандарти информационной безопасности - М.: ИУИТ, 2004. -328 с.
4. Стенг Д., Мун С. Секреты безопасности сетей. – К.: «Диалектика», 1995. – 544 с.
5. Жельников В. Криптография от папируса до компьютера. -М., 1996. -336 с.
6. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. / Пер. с анг. /М.: Мир,1982. – 204 с.
7. Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с анлг. – М.: Мир, 1993. – 216 с.
8. Берлоу Р, Прошан Ф., Математическая теория надежности – М. сов. радио, 1969
9. Голинкевич Т.А. Прикладная теория надежности. Учебник для вузов. – М. Высш.шк. 1985.
10. Половко А.М., Гуров С.В. Основы теории надежности – Спб, 2006.

11. Черкесов Г.Н. Надежность аппаратно-программных комплексов. Учебник для вузов. – Спб, 2005.
12. Липаев В.В. Надежность программных средств – М. СИНТЕГ, 1998.
13. Тарасенко В.П., Мламан А.Ю., Черніченко Ю.П., Конійчук В.І. Надійність комп'ютерних систем – К.: «Корнійчук», 2007. -256с.