КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою
(пост. пс 10 від «30» 01 2021 р.)
Ректор

_____ А.А. Мазаракі

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ/ SECURITY OF INFORMATION SYSTEMS AND NETWORKS

РОБОЧА ПРОГРАМА / COURSE OUTLINE

освітній ступінь	**бакалавр**	/ Bachelor
галузь знань	**12 Інформаційні технології**	/ Information Technology
спеціальності	**122 Комп'ютерні науки**	/ Computer Science

Київ 2020

Автори: В.І. ПАШОРІН, кандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Робочу програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «12» січня 2021 р., протокол № 16.

Рецензенти: С.Л. РЗАЄВА, кандидат технічних наук, доцент
П.Г. ДЕМІДОВ, кандидат технічних наук, доцент

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І МЕРЕЖ /
SECURITY OF INFORMATION SYSTEMS AND CHAINS

РОБОЧА ПРОГРАМА /
COURSE OUTLINE

освітній ступінь	**бакалавр**	/	bachelor
галузь знань	**12 Інформаційні технології**	/	Information Technologies
спеціальність	**122 Комп'ютерні науки**	/	Computer Sciences

1. СТРУКТУРА ДИСЦИПЛІНИ ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ (ТЕМАТИЧНИЙ ПЛАН)

Назва теми	Кількість годин				Форми контролю
	Усього год/кредитів	Лекції	Практичні заняття / МК	Самостійна робота студ.	
Тема 1.Основні положення теорії інформаційної безпеки	12	2	-	10	УО, ЛР, ПСР
Тема 2. Правове забезпечення інформаційної безпеки	12	2	-	10	УО Пр
Тема 3. Адміністративне та організаційне забезпечення інформаційної безпеки	30	6	6	18	УО, ЛР, ПСР
Тема 4. Програмно–технічне забезпечення інформаційної безпеки	36	6	10	20	УО, ЛР, ПСР, Т
Тема 5. Основи криптографічного захисту інформації	30	6	6	18	УО, ЛР, ПСР
Тема 6. Захист від руйнуючих програмних дій	24	6	-	18	УО, ЛР, ПСР
Тема 7. Безпечна робота в комп’ютерних мережах	36	6	12	18	УО, ЛР, ПСР, Т, ПК
Разом	180/6	34	34	112	
Підсумковий контроль - екзамен					

Примітка: УО – опитування з використанням комп’ютерних навчальних тренажерів; Т – тестування; ЛР – захист лабораторних робіт; ПСР – перевірка самостійної роботи; ПК - підсумковий контроль.

2. ТЕМАТИКА ТА ЗМІСТ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ ТА САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
ТЕМА 1. ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
Знати: основні концептуальні положення системи захисту інформаційних систем і мереж; класифікацію загроз інформації та міри протидії ***Вміти:*** визначати порушення в роботі інформаційних систем; вибирати засоби безпеки інформаційних систем	**Лекція №1. Безпека інформаційних систем в умовах функціонування глобальних мереж**. План лекції: 1. Актуальність, цілі і завдання інформаційної безпеки. 2. Принципи, головні задачі та функції безпеки інформаційних систем. 3. Види можливих порушень в роботі інформаційної системи. 4. Основні поняття і класифікація загроз. Основні загрози доступності, цілісності та конфіденційності інформації. 5. Модель інформаційної безпеки організації: структура і компоненти. Засоби безпеки інформаційних систем і мереж. **Список рекомендованих джерел:** *Основний*: 2, 3, 4. *Додатковий*: 10, 11. *Інтернет-джерела*: 15.	12 2
	Самостійна робота студентів. Вивчення матеріалу лекції з питань: 1. Розголошування та витік інформації. 2.Несанкціонований доступ до системи або мережі 3. Порушники інформаційної безпеки. 4. Класифікація порушників. 5.Методика вторгнення до інформаційної системи **Список рекомендованих джерел:** *Основний*: 2, 3, 4.	10

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Додатковий: 10, 11. *Інтернет-джерела*: 15.	
ТЕМА 2. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
Знати: особливості законодавчого рівня забезпечення інформаційної безпеки. ***Вміти:*** застосовувати положення правових актів для забезпечення інформаційної безпеки обчислення даних.	**Лекція №2. Законодавство по захисту інформації в інформаційних системах** План лекції: 1 Правові норми забезпечення безпеки і захисту інформації. 2. Українське законодавство в галузі інформаційної безпеки. 3. Зарубіжне законодавство в галузі інформаційної безпеки. **Список рекомендованих джерел:** *Основний: 1, 2*. *Додатковий: 6, 7.* *Інтернет-джерела: 15-16.*	12 2
	Самостійна робота студентів. Вивчення матеріалу лекції з питань: 1. Правові норми забезпечення безпеки і захисту інформації. 2. Міжнародні стандарти інформаційної безпеки. **Список рекомендованих джерел:** *Основний: 1, 2.* *Додатковий: 6, 7.* *Інтернет-джерела: 14, 16, 19.*	10
ТЕМА 3. АДМІНІСТРАТИВНЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
Знати: - особливості	**Лекція №3. Організаційний захист інформації в інформаційних системах** План лекції:	30 6

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
адміністративних методів захисту інформаційних систем і мереж; - особливості організаційних заходів щодо захисту інформації в інформаційних системах. ***Вміти*:** розробляти основні положення політики безпеки і програму її реалізації.	1. Поняття та принципи політики інформаційної безпеки. 2. Впровадження програми безпеки на об'єктах інформаційної діяльності. 3. Організаційна структура системи забезпечення безпеки інформації. 4. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9.* *Інтернет-джерела: 15, 19, 20.*	
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка питань: 1.Критерії оцінювання захищеності інформаційної системи. "Критерії оцінки довірених комп'ютерних систем" ("Помаранчева книга"). 2. Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. 3. Базова і спеціалізовані політики безпеки. **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9.* *Інтернет-джерела: 15, 17. 18.*	18
	Практичне заняття №1. Створення політики інформаційної безпеки для організації **Мета:** вміти побудувати план захисту інформації в інформаційній системі **Завдання:** 1. Проаналізувати та систематизувати існуючи методики розробки політик безпеки на підприємстві (за варіантом). 2. Створити документ с викладенням політики інформаційної безпеки (за	6

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	варіантом). 3. Підготувати звіт-презентацію по розробці, розгортанню та ефективному використанню політики інформаційної безпеки. 4. Скласти план захисту інформації в інформаційній системі	
ТЕМА 4. ПРОГРАМНО–ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
Знати: канали витоку інформації в інформаційних системах; методи і засоби блокування каналів витоку інформації; особливості інженерно-технічного рівня захисту інформаційних систем і мереж; ***Вміти:*** реєструвати	**Лекція №4. Канали витоку інформації.** План лекції: 1. Класифікація та характеристики технічних каналів витоку інформації. 2. Радіоканали витоку інформації та їх класифікація. 3. Класифікація та характеристики візуально-оптичних каналів витоку інформації. 4. Електричні канали витоку інформації. **Список рекомендованих джерел:** *Основний: 2, 3, 4.* *Додатковий: 9, 12.* *Інтернет-джерела: 15-16.*	36 2
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка питань: 1**.** Класифікація та характеристики матеріально-речових каналів витоку інформації. 2. Радіозакладні пристрої та їх класифікація 3. Технічні засоби перехоплення інформації. 4. Методи та види несанкціонованого доступу до інформаційних систем. **Список рекомендованих джерел**	5

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
порушення режиму безпеки і складати звіти;	*Основний: 2, 3, 4.* *Додатковий: 9, 12.* *Інтернет-джерела: 15.*	
створювати захист інформації за допомогою технічних засобів; захищати інформаційні системи за допомогою програмних засобів; створювати захист інформації за допомогою програмних засобів; використовувати системні ресурси для захисту інформації; захищати інформаційні системи за допомогою програмних засобів; використовувати системні ресурси для захисту інформації;	**Практичне заняття №2. Засоби несанкціонованого доступу до інформації** **Мета:** знати засоби несанкціонованого доступу до інформації. **Завдання:** 1. Проаналізувати та систематизувати існуючи засоби несанкціонованого доступу до інформації (за варіантом): - по акустичних каналах ; - через лінії електроживлення та заземлення; - через лінії зв'язку; - через візуально-оптичні канали; - через побічні електромагнітні випромінювання та наводки. 2. Підготувати звіт-презентацію по розглянутих засобах несанкціонованого доступу до інформації.	2
	Лекція №5. Технічний захист інформації і об'єкти захисту План лекції: 1. Властивості об'єктів захисту в інформаційній системі 2. Активні та пасивні методи забезпечення технічного захисту в інформаційних системах 3. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. 4. Програмні засоби захисту інформації в інформаційних системах. **Список рекомендованих джерел:**	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Основний: 1, 2. *Додатковий: 1.* *Інтернет-джерела: 15.*	
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка питань: 1. Системи технічної та фізичної охорони об'єктів інформаційної діяльності. 2. Основні етапи створення комплексу технічного захисту на об'єкті інформаційної діяльності 3. Технічні засоби пасивного виявлення радіозакладних пристроїв: - індикатори електромагнітних випромінювань, інтерцептори, радіочастотоміри та скануючи приймачі. 4. Класифікація, характеристики та методика пошуку акустичних закладних пристроїв. 5. Перспективні системи технічного захисту інформації **Список рекомендованих джерел:** *Інтернет-джерела: 16, 19, 20.*	5
	Практичне заняття №3. Методи і засоби технічного захисту інформації **Мета:** зрозуміти методів і засобів технічного захисту інформації. **Завдання:** 1. Проаналізувати та систематизувати існуючи засоби захисту інформації від витоку (за варіантом): - по акустичних каналах ; - через лінії електроживлення та заземлення; - через лінії зв'язку;	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	через візуально-оптичні канали; - через побічні електромагнітні випромінювання та наводки. - засоби телевізійної охорони. 2. Підготувати звіт-презентацію по розглянутих технічних засобах захисту інформації.	
	Лекція №6. Технічний захист інформації і об'єкти захисту План лекції: 1. Ідентифікація, автентифікація та авторизація суб'єктів інформаційної системи. 2. Сутність методів ідентифікації та автентифікації. 3. Біометрична автентифікація **Список рекомендованих джерел:** *Основний: 1, 2.* *Додатковий: 1.* *Інтернет-джерела: 15.*	2
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка питань: 1. Функціональне призначення та реалізація парольного захисту. 2. Паролі в ОС Windows 3. Поняття розмежування доступу до інформації і об'єктів інформаційної системи. 4. Дискреційне і мандатне управління доступом к об'єктам комп'ютерних систем 5. Рольове керування доступом	10

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	6. Реєстрація подій і аудит безпеки. **Список рекомендованих джерел:** *Інтернет-джерела: 18-20.*	
	Практичні заняття №4,5 Парольний захист. Безпека зберігання даних в ОС Microsoft Windows **Мета:** Вияснення паролю користувача з використанням утіліти для зламу пароля. Знати і розуміти концепцію безпека зберігання даних в ОС Microsoft Windows. **Завдання:** 1. Проаналізувати та систематизувати існуючи засоби парольного захисту архівних файлів із паролями різної довжини й структури. 2. Проаналізувати захищеність даних паролями різної складності за допомогою програми Advanced ZIP Password Recovery. 3. Підготувати звіт за результатами виконання лабораторної роботи. 4. Створити тіньові копії спільних каталогів. 5. Виконати повну й додаткову архівацію за допомогою програми Backup. 6. Виконати відновлення даних за допомогою програми Backup. 7. Створити дзеркальні тома в ОС Windows Server 8. Підготувати звіт про виконання лабораторної роботи	4
	Практичне заняття №6 Дослідження та захист реєстру операційної системи Windows **Мета:** концепція дослідження та захист реєстру операційної системи Windows. **Завдання:** 1. Підготувати віртуальну машину з ОС Windows для виконання	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	лабораторної роботи. 2. Підготувати текстовий файл, у який внести задані за варіантом настроювання реєстру. 3. Запустити файл настроювання реєстру й перевірити роботу внесених змін. 4. Підготувати звіт про виконання лабораторної роботи	
ТЕМА 5. ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ		
Знати: основні поняття криптографічного і стеганографічного захисту інформації пояснювати заходи керування загрозами користувача; основні поняття криптографічного і стеганографічного захисту інформації ***Вміти:*** опрацювати додаткові ресурси та завдання даної теми;	**Лекція №7 Принципи криптографії. Криптографічні системи.** План лекції: 1. Основні терміни та поняття криптографії. 2. Історія та законодавча база криптографії. 3. Перші методи шифрування перестановки та заміни застосунка. Керування загрозами для застосунків. 4. Симетричні криптосистеми. Стандарт шифрування даних DES. 5. Асиметричні криптосистеми. Стандарт шифрування даних RSA. 6. Основні типи алгоритмів шифрування**.** **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 8, 9, 12, 13.* *Інтернет-джерела: 15, 17, 18, 19.*	30 4
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка питань: 1. Одноалфавітні системи шифрування 2. Багатоалфавітні системи шифрування 3. Захист документів Microsoft Office від несанкціонованого доступу	10

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
застосовувати засоби кібербезпеки.	4. Шифруюча файлова система **Список рекомендованих джерел:** *Інтернет-джерела: 18-20.*	
	Практичне заняття №7 Створення алгоритму криптографічного захисту **Мета.** Ознайомлення з порядком побудови алгоритму криптографічного захисту **Завдання:** Ознайомитися з методом шифрування за варіантом. 2. Розробити блок-схему алгоритму шифрування та розшифровування. 3. Реалізувати формальні моделі у вигляді двох підсистем модуля з мінімальним інтерфейсом. 4. Описати особливості реалізації завдання та варіанти застосування розробленого модуля.	6
	Лекція №8 Електронний цифровий підпис План лекції: 1. Підпис і його властивості 2. Особливості шифрування ЕЦП 3. Склад цифрового підпису 4. Технологія застосування ЕЦП 5. Організаційне забезпечення електронного цифрового підпису. 6. Управління ключами та сертифікація ключів. **Список рекомендованих джерел:** Основний: 2,3,4. Додатковий: 9, 12, 13. Інтернет-джерела: 16-19.	2

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка до лабораторного заняття з питань: 1.Стеганографічні методи захисту інформації **Список рекомендованих джерел** *Інтернет-джерела: 15-20.*	8
ТЕМА 6. ЗАХИСТ ВІД РУЙНУЮЧИХ ПРОГРАМНИХ ДІЙ		
Знати: - класифікацію та особливості комп'ютерних вірусів; - правила захисту відшкідливого програмного забезпечення ***Вміти:*** захищати комп'ютер від шкідливого програмного забезпечення	**Лекція № 9 Шкідливе програмне забезпечення** План лекції: 1**.** Поняття і класифікація комп'ютерних вірусів. 2. Програми – закладки і методи захисту від них. 3. Троянські програми. 4. Черв'яки і інші шкідливі програми. 5. Антивірусні програми і комплекси. **Список рекомендованих джерел:** *Основний: 2,3,4.* *Додатковий: 9, 12, 13.* *Інтернет-джерела: 15-20.*	24 6
	Самостійна робота студентів. Вивчення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Правила використання стороннього програмного забезпечення. 2. Спам і засоби боротьби з ним. **Список рекомендованих джерел** *Інтернет-джерела: 15-20.*	18

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
ТЕМА 7. БЕЗПЕЧНА РОБОТА В КОМП'ЮТЕРНИХ МЕРЕЖАХ		
Вміти: - організовувати безпечну роботу в комп'ютерних мережах; - використовувати електронну пошту для захищеного обміну інформацією ***Знати:*** - організацію безпечної роботи в бездротових мережах; - правила безпеки при роботі в бездротових мережах	**Лекція № 10 Шкідливе програмне забезпечення. Віртуальні захищені мережі VPN** План лекції: 1. Аналіз загроз мережевої безпеки. 2. Види, функції та особливості роботи міжмережевих екранів. 3. Конфігурування міжмережевих екранів. 4. Класифікація та варіанти архітектури мереж VPN 5. Засоби захисту мереж VPN. **Список рекомендованих джерел:** *Основний: 2,3,4,5.* *Додатковий: 9, 12, 14.* *Інтернет-джерела: 15, 16, 19, 20.*	30 4
	Самостійна робота студентів Вивчення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Правила безпечної роботи в мережах. 2. Захист на мережевому рівні. 3. Схеми мережевого захисту на базі міжмережевих екранів. 4. Правила користування електронною поштою. 5. Адміністрування електронної пошти. 6. Використання електронної пошти для конфіденційного обміну інформацією	18
	Практичне заняття № 8 Дослідження системи захищеного електронного листування PGP **Мета:** дослідити систему захищеного електронного листування PGP.	12

Результати навчання	Навчальна діяльність*	Робочий час студента, год
1	2	3
	Завдання: 1. Створити ключі в програмі PGP. 2. Зашифрувати та надати електронний цифровий підпис електронному повідомленню 3. Налаштувати систему захищеного електронного листування. 4. Підготувати звіт про виконання лабораторної роботи	
	Лекція № 11 Захист Wi-Fi мереж. **План лекції:** 1. Безпека безпроводових мереж. 2. Погрози і ризики безпеки безпроводових мереж. 3. Протоколи безпеки безпроводових мереж. **Список рекомендованих джерел:** *Основний: 2,3,4,5.* *Додатковий: 9, 12, 14.* *Інтернет-джерела: 15, 17-20.*	2
	Всього	**180**

3. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації – Чернівці.- Видавничий дом «Родовід», 2018. – 471с.
3. Кавун С.В. Інформаційна безпека. Харків : ХНЕУ, 2016. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2016. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2017. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. 5. Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах/Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №3.160 С.
10. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
11. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
12. A.Menezes, P. van Oorshot, S.Vanstone. Handbook of Applied Cryptography. CRC Press Inc, 2015, 780 p.
13. Г.В.Кузнецов, В.В.Фомичов, С.О.Сушко. Математичні основи криптографії: Ч.1. Дніпропетровськ: Національний гірничий університет, 2014,391с.
14. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К. КНТ. 2012, 160с.

Інтернет-джерела

15. Защита информации – режим доступу: http://www.bseu.by/it/tohod/lekcii9_2.htm
16. Захист інформації – режим доступу: http://www.warning.dp.ua/tel28.htm
17. Безпека на прикладному рівні – режим доступу: http://www.dut.edu.ua

18. IEEE computer society. SWEBOK – режим доступу: *http://www.computer.org/portal/web/swebok/htmlformat*
19. Process Models in Software Engineering – режим доступу: *http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE-Encyc.pdf*
20. Technical writing for software engineers – режим доступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

** Курсивом виділені назви видань, які знаходяться в бібліотеці КНТЕУ.*