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
(прот. № від 2021 р.)
Ректор
А. А. Мазаракі

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ / SECURITY OF INFORMATION SYSTEMS

РОБОЧА ПРОГРАМА/ COURSE OUTLINE

освітній ступінь	**Магістр** / Master
галузь знань	**12 Інформаційні технології** / Information Technologies
спеціальність	**124 Системний аналіз** / System Analysis
спеціалізація	**Інформаційні технології та бізнес-аналітика (Data Science)** / Information Technologies and Business Analytics (Data Science)

Київ 2021

Автори: В.А. ЛАХНО, доктор технічних наук, професор
кафедри інженерії програмного забезпечення та кібербезпеки
М.В. САШНЬОВА, кандидат технічних наук, доцент
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 «25» травня 2021 р., протокол №9.

Рецензенти: С.Л. РЗАЄВА, кандидат технічних наук, доцент
О.О. РУДЕНКО, Front-end Team Lead at Astound Commerce
О.А. ХАРЧЕНКО, декан факультету інформаційних технологій, кандидат технічних наук, доцент
С.М. МИРОНЕЦЬ, завідувач кафедри психології, доктор психологічних наук, доцент
В.А. ОСИКА, декан факультету торгівлі та маркетингу, доктор технічних наук, професор

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ / SECURITY OF INFORMATION SYSTEMS

РОБОЧА ПРОГРАМА
COURSE OUTLINE

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології** / Information Technology
спеціальність	**124 Системний аналіз** / System Analysis
спеціалізація	Інформаційні технології та бізнес-аналітика (Data Science) / Information Technologies and Business Analytics (Data Science)

ВСТУП

Робоча програма дисципліни «Безпека інформаційних систем» призначена для здобувачів другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології», спеціальності 124 «Системний аналіз», освітньої програми «Інформаційні технології та бізнес-аналітика (Data Science)».

Дисципліна «Безпека інформаційних систем» належить до переліку вибіркових освітніх компонент. Робочу програму підготовлено з урахуванням вимог Стандарту вищої освіти КНТЕУ та освітньо-професійної програми «Інформаційні технології та бізнес-аналітика (Data Science)».

Розроблена програма складається з таких розділів:

1. Структура дисципліни та розподіл годин за темами
2. Тематика та зміст лекційних, практичних занять, самостійної роботи студентів.
3. Список рекомендованих джерел

1. СТРУКТУРА ДИСЦИПЛІНИ ТА РОЗПОДІЛ ГОДИН ЗА ТЕМАМИ

Назва теми	***Кількість годин***				***Форми контролю***
	Усього годин/кредитів	***За формами занять***			
		Лекції	***Практичне заняття***	***Самостійна робота студентів***	
Тема 1. Основні положення теорії безпеки інформаційно-телекомунікаційних систем	12	2		10	УО ІЗ
Тема 2. Шкідливе програмне забезпечення і захист від руйнуючих програмних дій	24	2	4	18	УО Пр
Тема 3. Правове забезпечення кібербезпеки	18	2	2	14	УО, ІЗ, Пр
Тема 4. Адміністративне та організаційне забезпечення інформаційно-телекомунікаційних систем	18	2	2	14	УО, ІЗ, Пр
Тема 5. Інженерно–технічне забезпечення інформаційно-телекомунікаційних систем	18	2	2	14	ІЗ, Пр
Тема 6. Апаратні та програмні засоби захисту	18	2	2	14	УО ПО
Тема 7. Основи криптографічного захисту інформації	18	2	2	14	УО, ІЗ, Пр
Тема 8. Технології безпеки на основі фільтрації та моніторингу мережевого трафіку	24	2	4	18	УО, ІЗ, Пр
Тема 9. Протоколи захисту в телекомунікаційних мережах	18	2	2	14	УО, ІЗ, Пр
Тема 10. Безпечна робота в комп’ютерних мережах	12	2		10	УО, ІЗ, Пр
Разом	**180/6**	**20**	**20**	**140**	
Підсумковий контроль семестру - екзамен					

Умовні позначення:

УО – усне опитування ІЗ – перевірка індивідуальних завдань

ПО – письмове опитування Т – тестування

Пр. – презентація індивідуального завдання

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

Результати навчання	***Навчальна діяльність***	***Робочий час студента год***	***Оцінювання у балах***
Знати: основні концептуальні положення системи захисту інформаційних систем і мереж; **Вміти:** визначати порушення в роботі інформаційних систем вибирати засоби безпеки інформаційних систем	**Тема 1.** Основні положення теорії безпеки інформаційно-телекомунікаційних 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. **Самостійна робота студентів** Вивчення та доповнення 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 **Література** Основна: 2, 3, 4 Додаткова: 10, 11	12 2 10	
Знати: - класифікацію та особливості комп’ютерних вірусів; - правила захисту від шкідливого програмного забезпечення	**Тема 2.** Шкідливе програмне забезпечення і захист від руйнуючих програмних дій **Лекція 2**. 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* **Практичне заняття №1.** *Тема:*Робота з	24 2 2	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
Вміти: -захищати комп'ютер від шкідливого програмного забезпечення; - організовувати безпечну роботу в комп'ютерних мережах; - використовувати електронну пошту для захищеного обміну інформацією;	антивірусними програмами різних типів. Завдання до заняття: 1. Вивчення можливостей налаштування програми DrWeb.. 2. Запустити програму з командного рядка з об'єктами та ключами згідно індивідуального завдання. 3. Виконати перевірку файлів за алгоритмом перевірки і контрольованими змінами згідно індивідуального завдання. 4. За результатами перевірки скласти звіт. **Практичне заняття №2.** *Тема:* Дослідження системи захищеного електронного листування PGP Завдання до заняття: 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 **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Правила використання стороннього програмного забезпечення. 2. Спам і засоби боротьби з ним. **Література:** Основна: 2, 3, 4 Додаткова: 9, 12, 13	2	10
Знати: особливості законодавчого рівня забезпечення інформаційн	**Тема 3.** Правове забезпечення кібербезпеки **Лекція 3.** Законодавство по захисту інформації в інформаційних системах **План лекції** 1. Правові норми забезпечення безпеки і захисту інформації.	18 2	

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
ої безпеки **Вміти:** застосовувати положення правових актів для забезпечення інформаційної безпеки	2. Українське законодавство в галузі інформаційної безпеки. 3. Зарубіжне законодавство в галузі інформаційної безпеки. 4. Міжнародні стандарти інформаційної безпеки. **Практичне заняття №3.** *Тема:* Нормативно-правове забезпечення по захисту інформації в Україні. Завдання до заняття: 1. Проаналізувати та систематизувати необхідну законодавчу та нормативну документацію по безпеці інформаційних систем у певній сфері (за варіантом). 2. Привести обґрунтування результату аналізу нормативно-правової бази України в сфері безпеки інформації. Результат аналізу та систематизації оформити у вигляді інтегральної оцінки нормативно-правової бази України (за варіантом). 3. Описати, яким чином зібрані законодавчі та нормативні акти дозволять уникнути організаційних труднощів, фінансових та інших законодавчих санкцій у господарчій діяльності (виробництві, формуванні послуг, реалізації продукції та послуг). **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Правові норми забезпечення безпеки і захисту інформації. **Література:** Основна: 1,2 Додаткова: 6, 7	2 14	10
Знати: - особливості адміністративних методів захисту	**Тема 4.** Адміністративне та організаційне забезпечення інформаційно-телекомунікаційних систем **Лекція 4**. Організаційний захист інформації в інформаційних системах	18 2	

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
інформаційних систем і мереж; - особливості організаційних заходів щодо захисту інформації в інформаційних системах **Вміти:** розробляти основні положення політики безпеки і програму її реалізації;	**План лекції** 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. **Практичне заняття №4.** *Тема:* Створення політики інформаційної безпеки для організації Завдання до заняття: 1. Проаналізувати та систематизувати існуючи методики розробки політик безпеки на підприємстві (за варіантом). 2. Створити документ с викладенням політики інформаційної безпеки (за варіантом). 3. Підготувати звіт-презентацію по розробці, розгортанню та ефективному використанню політики інформаційної безпеки. 4. Скласти план захисту інформації в інформаційній системі **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з 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 **Література:** Основна: 2, 3, 4 Додаткова: 9	2 14	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
Знати: Канали витоку інформації в інформаційних системах **Вміти:** реєструвати порушення режиму безпеки і складати звіти	**Тема 5.** Інженерно–технічне забезпечення інформаційно-телекомунікаційних систем **Лекція 5**. 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. **Практичне заняття №5.** *Тема:* Засоби несанкціонованого доступу до інформації Завдання до заняття: 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. **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з 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	18 2 2 14	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	Література: Основна: 2, 3, 4 Додаткова: 9, 12		
Знати: методи і засоби блокування каналів витоку інформації. **Вміти:** створювати захист інформації за допомогою технічних засобів	**Тема 6. Апаратні та програмні засоби захисту** **Лекція 6**. 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 **Практичне заняття №6.** *Тема:* Методи і засоби технічного захисту інформації Завдання до заняття: 1. Проаналізувати та систематизувати існуючи засоби захисту інформації від витоку (за варіантом): - по акустичних каналах ; - через лінії електроживлення та заземлення; - через лінії зв'язку; *через візуально-оптичні канали;* - через побічні електромагнітні випромінювання та наводки. - засоби телевізійної охорони. 2. Підготувати звіт-презентацію по розглянутих технічних засобах захисту інформації. **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Системи технічної та фізичної охорони	18 2 2 14	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	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 **Література:** Основна: 1,2 Додаткова: 1		
Знати: основні поняття криптографічного і стеганографічного захисту інформації; основні поняття криптографічного і стеганографічного захисту інформації **Вміти:** розробляти індивідуальн	**Тема 7.** Основи криптографічного захисту інформації **Лекція 7**. Принципи криптографії **План лекції** 1. Основні терміни та поняття криптографії. 2. Історія та законодавча база криптографії. 3. *Перші методи шифрування перестановки та заміни.* 4. Симетричні криптосистеми. Стандарт шифрування даних DES. 5. Асиметричні криптосистеми. Стандарт шифрування даних RSA. **Практичне заняття №7.** *Тема:* Створення алгоритму криптографічного захисту Завдання до заняття: 1. Ознайомитися з методом шифрування за варіантом. 2. Розробити блок-схему алгоритму шифрування та розшифровування. 3. Реалізувати формальні моделі у вигляді	18 2 2	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
і системи управління доступом і захистом інформаційних систем	двох підсистем модуля з мінімальним інтерфейсом. 4. Описати особливості реалізації завдання та варіанти застосування розробленого модуля. **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Одноалфавітні системи шифрування 2. Багатоалфавітні системи шифрування 3. Захист документів Microsoft Office від несанкціонованого доступу 4. Шифруюча файлова система **Література:** Основна: 2, 3, 4 Додаткова: 8, 9, 12, 13	14	
Знати: особливості інженерно-технічного рівня захисту інформаційних систем і мереж **Вміти:** використовувати системні ресурси для захисту інформації; захищати інформаційні системи за допомогою програмних засобів	**Тема 8.** Технології безпеки на основі фільтрації та моніторингу мережевого трафіку **Лекція 8**. Ідентифікація і автентифікація. **План лекції** 1. Ідентифікація, автентифікація та авторизація суб'єктів інформаційної системи. 2. Сутність методів ідентифікації та автентифікації. 3. *Біометрична автентифікація* **Практичне заняття №8.** *Тема:* Безпека зберігання даних в ОС Microsoft Windows Завдання до заняття: 1. Підготувати віртуальну машину з ОС Windows Server для виконання лабораторної роботи. 2. Створити тіньові копії спільних каталогів. 3. Виконати повну й додаткову архівацію за допомогою програми Backup. 4. Виконати відновлення даних за допомогою програми Backup.	24 2 2	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	5. Створити дзеркальні тома в ОС Windows Server 6. Підготувати звіт про виконання лабораторної роботи **Практичне заняття №9.** *Тема:* Організація безпеки механізму автентифікації Завдання до заняття: 1. Підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи. 2. Створити на робочій станції кілька локальних користувачів із паролями різної довжини й складності. 3. Запустити програму перехоплення й розшифровки парольних хешей. 4. Здійснити перебір паролів (методом, залежно від варіанта). 5. Протестувати пароль, за допомогою команди Test Password. 6. Підготувати звіт про виконання лабораторної роботи **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Апаратні засоби автентифікації. 2. Мережева автентифікація в ОС Windows. **Література:** Основна: 1,2 Додаткова: 1	2 18	10
Знати: особливості інженерно-технічного рівня захисту інформаційних систем і мереж	**Тема 9.** Протоколи захисту в телекомунікаційних мережах **Лекція 9**. Управління доступом і аудит **План лекції** 1. Поняття розмежування доступу до інформації і об'єктів інформаційної системи. 2. Дискреційне і мандатне управління	18 2	

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
Вміти: створювати захист інформації за допомогою програмних засобів	доступом к об'єктам комп'ютерних систем 3. Рольове керування доступом 3. Реєстрація подій і аудит безпеки. **Практичне заняття №10.** *Тема:* Парольний захист Завдання до заняття: 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. **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Функціональне призначення та реалізація парольного захисту. 2. Паролі в ОС Windows **Література:** Основна: 1,2 Додаткова: 1	2 14	10
Знати: особливості використання електронного цифрового підпису;	**Тема 10.** Безпечна робота в комп'ютерних мережах **Лекція 10.** 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. **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з	12 2 10	

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	питань: 1.Стеганографічні методи захисту інформації **Література:** Основна: 2, 3, 4 Додаткова: 9, 12, 13		
Разом за семестр		***180***	***100***

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», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека. Харків : ХНЕУ, 2013. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 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, 2013. – 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.

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