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. № 2 від 04.06.2021 р.)
Ректор

_____ А. А. Мазаракі

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

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

Автор: В.І. Пашорін, канд. техн. наук, проф. кафедри інженерії програмного забезпечення та кібербезпеки
В. П. Звєрєв, канд. техн. наук., доц. 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: Рзаєва С.Л., канд. техн. наук, доцент,
Бабенко Б.Т., технічний директор CIO, Softorino Inc.

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

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 інтернет-ресурсів» 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 інтернет-ресурсів» 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)».

Одним із напрямків кібербезпеки є забезпечення захисту інтернет-ресурсів. Кількість інтернет-ресурсів (серверів різноманітного призначення та інфраструктури глобальних мереж) збільшується щороку, все ширше використовуються хмарні технології і віддалений доступ до ресурсів, а значить і зростає кількість інформації, яка локалізується на таких ресурсах і в глобальних мережах. Прагнення незаконно використовувати цю інформацію, спотворювати її, або умисно блокувати доступ до неї стимулює зростання атак на інтернет-ресурси, що приводить не тільки до економічних, а й політичних і соціальних наслідків. Атаки на державні та урядові інтернет-ресурси взагалі розглядається як елемент поширення гібридних війн у світі.

Таким чином, напрямок кібербезпеки, який стосується захисту інтернет-ресурсів, стає все більш актуальним, особливо з урахуванням постійного вдосконалення методів та інструментів атак. Дисципліна «Безпека інтернет-ресурсів» покликана надати більш детальний розгляд по цьому напрямку. Змістовна частина дисципліни включає вивчення сучасних методів та засобів захисту интернет-ресурсів. Як засоби для забезпечення безпеки інтернет-ресурсов використовуються: антивірусні програми, міжмережеві екрани, віртуальні приватні мережі (VPN), засоби мережевої аутентифікації, авторизації і шифрування, засоби захисту мережевих ресурсів на основі розмежування повноважень користувачів, засоби активного дослідження захищеності ресурсів, засоби попередження про мережеві атаки і засоби виявлення таких атак.

Робоча 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. Основи мережевої безпеки	26	4	2	20	УО ІЗ
Тема 2. Технології фільтрації мережевого трафіку	36	4	4	28	УО Пр
Тема 3. Основи технології віртуальних приватних мереж	36	4	4	28	УО, ІЗ, Пр
Тема 4. Протоколи мережевої безпеки	26	2	4	20	УО, ІЗ, Пр
Тема 5. Безпека інтернет-ресурсів на прикладному рівні	20	2	2	16	ІЗ, Пр
Тема 6. Аналіз безпеки інтернет-ресурсів	36	4	4	28	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

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

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
Знати: основні положення, організацію та моделі систем захисту інтернет-ресурсів; класифікацію атак на інтернет-ресурси та міри протидії **Вміти:** здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі	**Тема 1. Основи мережевої безпеки** **Лекція 1. План лекції** 1. Розподілені ресурси: механізми безпеки і управління 2. Мережева безпека: терміни та визначення **Лекція 2. План лекції** 1. Класифікація мережевих загроз та атак на інтернет-ресурси 2. Шляхи вирішення проблем захисту інтернет-ресурсів **Практичне заняття №1.** *Тема: Засоби мережного аудиту* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2.Запустити утиліту TCPView. Ознайомтеся з основними пунктами меню 3. Занести до протоколу результати сканування відкритих з'єднань 4. Відкрийте утиліту XSpider. Вивчіть основні пункти меню, скориставшись документацією з меню «Довідка» 5. Запустити програму сканування 6. Виконати сканування по окремих сервісах 7. Проаналізуйте результати сканування вашого завдання. Занесіть до звіту результат сканування. 8. Занесіть до звіту порівняльну характеристику, отриманих вами	26 2 2 2	10

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	результатів за допомогою утиліт TCPView і XSpider **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції з питань: 1. Нормативні документи по безпеці в глобальних мережах 2. Технології виявлення віддалених атак 3. Соціальна інженерія **Список рекомендованих джерел** Основний: 2, 3, 4 Додатковий: 10, 11	20	
Знати: технологію та правила експлуатації міжмережевих екранів **Вміти:** встановлювати і налагоджувати міжмережеві екрани; аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них	**Тема 2. Технології фільтрації мережевого трафіку** **Лекція 3. План лекції** 1. Фільтрація трафіку. Фільтрація Web-змісту (WCF) 2. Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT) 3. Міжмережеві екрани (МЕ): класифікація та функції МЕ **Лекція 4. План лекції** 1. Схеми мережевого захисту на базі МЕ 2. Довірена мережа та DMZ мережі **3.** Формування політики міжмережевої взаємодії **Практичне заняття №2.** *Організація мережевої безпеки за допомогою міжмережевого екрана Outpost Firewall* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити програму Outpost Firewall. Вивчите функціональні можливості вкладок контекстного меню	36 2 2 2	16

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	«Параметри» 3. Налаштувати функції програми Outpost Firewall, залежно від вимог, зазначених у варіанті 4. Налаштувати журнал програми Outpost Firewall, для відображення тільки необхідної інформації, обумовленої завданням 5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями		
	Практичне заняття №3. *Організація мережевої безпеки при використанні засобів виявлення мережевих атак* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити утиліту APS, для виявлення факту сканування портів по протоколах TCP, UDP і розсилання UDP broadcast пакетів для заданих портів 3. Налаштувати утиліту APS за наданим варіантом 4. Налаштувати системи імітації сервісів TCP 5. Підготувати звіт за результатами роботи програми й виконаними налаштуваннями	2	14
	Самостійна робота студентів Вивчення та доповнення матеріалу лекції: 1. Варіанти виконання МЕ 2. Персональні і розподілені мережеві екрани 3. Основні схеми підключення МЕ 4. Проблеми безпеки МЕ 5. Інтерфейс та функціональні можливості	28	

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	програми Outpost Firewall **Список рекомендованих джерел:** Основний: 2-7 Додатковий: 8,9,10		
Знати: основи технології віртуальних захищених мереж VPN **Вміти:** використовувати VPN-рішення для побудови захищених мереж; захищати за допомогою програмних засобів	**Тема 3. Основи технології віртуальних приватних мереж** **Лекція 5. План лекції** *Концепція побудови віртуальних приватних мереж VPN* 1. Основні поняття і функції мережі VPN 2. Варіанти побудови віртуальних захищених каналів **Лекція 6. План лекції** 1. Класифікація мереж VPN 2. Основні варіанти архітектури VPN **Практичне заняття №4.** *Організація мережевої безпеки при використанні засобів VPN* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows 7 для виконання лабораторної роботи 2. Використовуючи **Центр управления сетями и общим доступом** створити нове з'єднання і налаштувати VPN тунель 3. Встановити та підготувати віртуальну машину з ОС Windows 10 для виконання лабораторної роботи 4. Використовуючи аплет **Мережі та Інтернет** створити VPN підключення 5. Встановити та налаштувати VPN – сервіс за варіантом 6. Підготувати звіт про виконання лабораторної роботи **Самостійна робота студентів**	36 2 2 4 28	14

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Засоби забезпечення безпеки VPN Методи вкладення інформації у комп'ютерні файли 2. VPN-рішення для побудови захищених мереж **Список рекомендованих джерел:** Основний: 3,4,5 Додатковий: 9,10		
Знати: основи забезпечення захисту в мережевих протоколах передачі **Вміти:** організовувати безпечну роботу в глобальних мережах	**Тема 4. Протоколи мережевої безпеки** **Лекція 7. План лекції** *Протоколи захисту інтеренет-ресурсів* 1. Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) 2. Захист інтернет-ресурсів на мережевому рівні (протокол IPSec) 3. Особливості реалізації засобів IPSec 4. Протоколи захисту у безпроводових мережах **Практичне заняття №5.** *Організація шифрування трафіку при використанні утиліти IPSec* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити консоль керування IPSec на комп'ютері 3. Створити свій список фільтрів, зазначений, залежно від варіанта 4. Створити власну дію фільтра, зазначену, залежно від варіанта 5. Створити свою політику IPSec 6. Додати до створеної політики,	26 2 4	16

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	правило за зазначеними критеріями, залежно від варіанта 7. Підготувати звіт про виконання лабораторної роботи **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Стандарт мережі з підвищеною безпекою WPA2 2. Основні схеми застосування IPSec **Список рекомендованих джерел:** Основний: 2,4,5,6 Додатковий: 9,12	20	
Знати: технологію та правила мережевої автентифікації ресурсів і користувачів **Вміти:** розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів	**Тема 5. Безпека інтернет-ресурсів на прикладному рівні** **Лекція 8. План лекції** *Управління мережевою ідентифікацією і доступом* 1. Захищений видалений доступ до мережі 2. Функціонування системи управління доступом. Протоколи автентифікації видалених користувачів 3. Централізований контроль доступу. Протокол Kerberos **Практичне заняття №6.** *Організація безпеки механізму мережевої автентифікації* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Встановити та запустити програму . Cain&Abel. Ознайомитись з можливостями основних пунктів меню програми	20 2 2	16

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	3. Виконати сканування MAC-адрес робочих станцій у локальній мережі 4. Виконати завдання за варіантом 5. Підготувати звіт про виконання лабораторної роботи **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Особливості управління видаленим доступом **Список рекомендованих джерел:** Основний: 5,6 Додатковий: 8,9	16	
	Тема 6. Аналіз безпеки інтернет-ресурсів **Лекція 9. План лекції** *Концепція адаптивного управління безпекою* 1. Технології виявлення атак. Класифікація систем виявлення атак IDS 2. Компоненти і архітектура IDS **Лекція 10. План лекції** 1. Системи попередження атак IPS Методи реагування систем на атаки. 2. Безпека Web-серверів **Практичне заняття №7.** *Побудова віртуальної машини з ОС Windows* Завдання до заняття: 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Встановити та запустити програму *ESET Smart Security.* Ознайомитись з можливостями основних пунктів меню програми 3. Виконати налаштування сервісів програми за варіантом	36 2 2 4	14

Результати навчання	*Навчальна діяльність*	*Робочий час студента год*	*Оцінювання у балах*
	4. Підготувати звіт про виконання лабораторної роботи **Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до практичного заняття з питань: 1. Засоби аналізу захищеності мережевих протоколів і сервісів 2. Безпечна мережева інфраструктура для Web-сервера **Список рекомендованих джерел:** Основний: 5,6 Додатковий: 8,9	28	
Разом за семестр		***180***	***100***

5. 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. Навчальний посібник Чернівці.- Видавничий дом «Родовід», 2017. – 471с.
3. Кавун С.В. Інформаційна безпека. Навчальний посібник Харків: ХНЕУ, 2016. -213с.
4. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль – К., 2015. – 435 с., іл.160.
5. *Зубок М. І. Інформаційна безпека : Навчальний посібник для студентів вищих навч.закладів / М. І. Зубок. – К. : КНТЕУ, 2009. – 132с.*
6. *КавунС. В. Інформаційна безпека підручник / С. В. Кавун. – Харків : ХНЕУ, 2016. – 368с.*
7. 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, 2015. – 632с.

Додатковий

8. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
9. 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.
10. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
11. *Кормич Б. А. Інформаційна безпека:організаційно-правові основи: навч. посібник для студентів вузів / Б. А. Кормич. – К. : Кондор, 2015. – 384с.*
12. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*

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

.
13. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*

Internet-ресурси

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