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 програмної інженерії та кібербезпеки

СИЛАБУС

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології** / Information Technology
спеціальність	**121 Інженерія програмного забезпечення** / Software Engineering
спеціалізація	**Інженерія програмного забезпечення /** Software Engineering

Гарант освітньо-професійної програми "Інженерія програмного забезпечення" другого (магістерського) рівня вищої освіти

Завідувач кафедри програмної інженерії та кібербезпеки, д.т.н., проф. Криворучко О.В.

Київ 2019

Автори: В.І. Пашорін, канд.техн.наук, проф.

Силабус розглянуто і затверджено на засіданні кафедри програмної інженерії та кібербезпеки 10 вересня 2019 р., протокол № 3.

СИЛАБУС

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

SYLLABUS

освітній ступінь	**магістр /** master
галузь знань	**12 Інформаційні технології** / Information Technology
спеціальність	**121 Інженерія програмного забезпечення** / Software Engineering
спеціалізація	**Інженерія програмного забезпечення** / Software Engineering

АНОТАЦІЯ КУРСУ

1. **Викладачі**:
   1.1. **Лектор**: Пашорін Валерій Іванович,
   - к.т.н., професор кафедри програмної інженерії та кібербезпеки;
   - *педагогічний стаж* – 35 років;
   - *контактиний телефон:* +38(098)244-09-47;
   - *e-mail:* vpashorin@knute.edu.ua
   - *наукові інтереси*: безпека інформацйних систем, операційні системи, комп'ютерні мережі
   - *стажування та підвищення кваліфікації*: Проходив підвищення кваліфікації в Центрі сертифікаційного навчання «ПРОКОМ» (м. Київ, сертифікати по різним модулях «1С: Підприємство» в 2017р.

2. **Дисципліна**: «Безпека інтернет-ресурсів»,
   - рік навчання: II
   - семестр навчання: III
   - кількість кредитів: 6
   - кількість годин за семестр:
     - лекційних: 14
     - лабораторних: 28
     - на самостійне опрацювання: 138
   - кількість аудиторних годин на тиждень:
     - лекційних: 2
     - лабораторних: 4

3. **Час та місце проведення:**
   - аудиторні заняття - відповідно до розкладу КНТЕУ з врахуванням специфіки дисципліни передбачено аудиторіях: 504, 514;
   - поза аудиторна робота - самостійна робота студента, результат виконання якої висвітлено засобами Office 365;

4. **Пререквізити та постреквізити навчальної дисципліни:**
   - **пререквізити:** «Безпека інформаційних систем і мереж», «Методи і засоби захисту інформації», «Операційні системи», «Архітектура комп'ютера».
   - **постреквізити:** (дициплiни та компетентності, які необхідні в трудовій діяльності фахівця

5. **Характеристика дисципліни:**

5.1. Призначення навчальної дисципліни: Основу дисципліни «Безпека інтернет-ресурсів» становить вивчення технологій захисту інформації в мережевих інфрастркутурах інформаційних систем. Володіння сучасними технологіями роботи та методами її практичного використання в професійній

діяльності стало необхідним елементом підготовки кваліфікованого інженера з інфокомунікацій. Дана дисципліна формує інженерний світогляд фахівця в галузі ІТ.

5.2. **Мета вивчення дисципліни:** формування теоретичних знань та практичних навичок необхідних для безпечного використання інтернет-ресурсів і безпечній роботі в глобальних мережах.

5.3. **Задачі вивчення дисципліни:** полягають у тому, щоб ознайомити студентів і надати їм навички в роботі по установці, настройці, експлуатації і підтримки в працездатному стані системи захисту ітернет-реурсів і безпечній роботі при використані глобальних мереж.

5.4. **Зміст навчальної дисципліни:** відповідає навчальній та робочій програмі, визначеній науковими досягненнями як наукові досягнення вітчизняних та закордонних вчених, а також запитам стейкхолдерів.

5.5. **План вивчення дисципліни**

Результати навчання	Навчальна діяльність	Робочий час студента (год.)	Оцінювання (бал)
1	2	3	4
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики.	**Тема 1. Основи мережевої безпеки**		
Знати: основні положення, організацію та моделі систем захисту інтернет-ресурсів; класифікацію атак на інтернет-ресурси та міри протидії	**Лекція 1. План лекції** 1. Розподілені ресурси: механізми безпеки і управління 2. Мережева безпека: терміни та визначення 3. Класифікація мережевих загроз та атак на інтернет-ресурси 4. Шляхи вирішення проблем захисту інтернет-ресурсів **Список рекомендованих джерел** Основний: 2, 3, 4 Додатковий: 10, 11	2	
Вміти: здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі	**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	24	2
Вміти:	**Лабораторна робота № 1** *Засоби мережного аудиту*	4	8

1	2	3	4
здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі	Завдання на лабораторну роботу: 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 результатів за допомогою утиліт TCPView і XSpider		
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 2. Технології фільтрації мережевого трафіку**		
Знати: технологію та правила експлуатації міжмережевих екранів	**Лекція 2. 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 **Список рекомендованих джерел:** Основний: 2-7 Додатковий: 10	2	
Вміти: встановлювати і налагоджувати міжмережеві екрани	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції: 1. Варіанти виконання МЕ 2. Персональні і розподілені мережеві екрани 3. Основні схеми підключення МЕ	20	4
Знати: технологію та правила експлуатації міжмережевих екранів	**Лекція 3. План лекції** 1. Схеми мережевого захисту на базі МЕ 2. Довірена мережа та DMZ мережі **3.** Формування політики міжмережевої взаємодії **Список рекомендованих джерел:** Основний: 2-7 Додатковий: 8,9,10	2	
Вміти:	**Самостійна робота студентів**	18	4

1	2	3	4
аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них	Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Проблеми безпеки МЕ 2. Інтерфейс та функціональні можливості програми Outpost Firewall.		
Вміти: встановлювати і налагоджувати міжмережеві екрани	**Лабораторна робота № 2** *Організація мережевої безпеки за допомогою міжмережевого екрана Outpost Firewall* **Завдання на лабораторну роботу:** 1. Встановити та підготувати віртуальну машину з ОС Windows для виконання лабораторної роботи 2. Запустити програму Outpost Firewall. Вивчите функціональні можливості вкладок контекстного меню «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	4	8
Вміти: аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них	**Лабораторна робота № 3** *Організація мережевої безпеки при використанні засобів виявлення мережевих атак* **Завдання на лабораторну роботу:** 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	4	8
SoftSkills*:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 3. Основи технології віртуальних приватних мереж**		
Знати: основи технології	**Лекція 4. План лекції**	2	

1	2	3	4
віртуальних захищених мереж VPN	*Концепція побудови віртуальних приватних мереж VPN* 1. Основні поняття і функції мережі VPN 2. Варіанти побудови віртуальних захищених каналів 3. Класифікація мереж VPN 4. Основні варіанти архітектури VPN **Список рекомендованих джерел:** Основний: 3,4,5 Додатковий: 9,10		
Вміти: використовувати VPN-рішення для побудови захищених мереж; захищати за допомогою програмних засобів	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Засоби забезпечення безпеки VPN Методи вкладення інформації у комп'ютерні файли 2. VPN-рішення для побудови захищених мереж	24	2
Вміти: використовувати VPN-рішення для побудови захищених мереж; захищати за допомогою програмних засобів	**Лабораторна робота 4** *Організація мережевої безпеки при використанні засобів VPN* **Завдання на лабораторну роботу:** 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	4	8
SoftSkills: комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 4. Протоколи мережевої безпеки**		
Знати: основи забезпечення	**Лекція 5. План лекції** 1. Протоколи захисту інтеренет-ресурсів	2	

1	2	3	4
захисту в мережевих протоколах передачі	2. Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) 3. Захист інтернет-ресурсів на мережевому рівні (протокол IPSec) 4. Особливості реалізації засобів IPSec 5. Протоколи захисту у безпроводових мережах **Список рекомендованих джерел:** Основний: 2,4,5,6 Додатковий: 9,12		
Вміти: організовувати безпечну роботу в глобальних мережах	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Стандарт мережі з підвищеною безпекою WPA2 2. Основні схеми застосування IPSec	24	2
Вміти: організовувати безпечну роботу в глобальних мережах	**Лабораторна робота 5** *Організація шифрування трафіку при використанні утиліти IPSec* **Завдання на лабораторну роботу:** 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, правило за зазначеними критеріями, залежно від варіанта 7. Підготувати звіт про виконання лабораторної роботи	4	8
SoftSkills*:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 5. Безпека інтернет-ресурсів на прикладному рівні**		
Знати: технологію та правила мережевої автентифікації ресурсів і користувачів	**Лекція 6. План лекції** *Управління мережевою ідентифікацією і доступом* 1. Захищений віддалений доступ до мережі 2. Функціонування системи управління доступом. Протоколи автентифікації віддалених користувачів	2	

1	2	3	4
	3. Централізований контроль доступу. Протокол Kerberos **Список рекомендованих джерел:** Основний: 5,6 Додатковий: 8,9		
Вміти: розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів	**Самостійна робота студентів** Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Особливості управління віддаленим доступом	24	6
Вміти: розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів	**Лабораторна робота 6** *Організація безпеки механізму мережевої автентифікації* **Завдання на лабораторну роботу:** 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 3. Виконати сканування MAC-адрес робочих станцій у локальній мережі 4. Виконати завдання за варіантом 5. Підготувати звіт про виконання лабораторної роботи	4	8
SoftSkills*:* комунікативні навички, робота в команді, творчі навички, сприйняття конструктивної критики, колективний тайм менеджмент	**Тема 6. Аналіз безпеки інтернет-ресурсів**		
Знати: організацію і правила безпеки при роботі в глобальних мережах	**Лекція 7. План лекції** *Концепція адаптивного управління безпекою* 1. Технології виявлення атак. Класифікація систем виявлення атак IDS 2. Компоненти і архітектура IDS 3. Системи попередження атак IPS Методи реагування систем на атаки. 4. Безпека Web-серверів **Список рекомендованих джерел:** Основний: 5,6 Додатковий: 8,9	2	
Вміти:	**Самостійна робота студентів**	24	8

1	2	3	4
створювати захист за допомогою програмних засобів; організовувати безпечну роботу в глобальних мережах	Вивчення та доповнення матеріалу лекції, підготовка до лабораторного заняття з питань: 1. Засоби аналізу захищеності мережевих протоколів і сервісів 2. Безпечна мережева інфраструктура для Web-сервера		
Вміти: створювати захист за допомогою програмних засобів; організовувати безпечну роботу в глобальних мережах	**Лабораторна робота 7** **Завдання на лабораторну роботу:** 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 4. Підготувати звіт про виконання лабораторної роботи	4	8
Разом за семестр		***180***	***100***

6. Список рекомендованих джерел

Основний

1. *Вольфенгаген, В. Э. Реляционные методы проектирование банка данных / В. Э. Вольфенгаген, Л. Т. Кузин, В. И. Саркисян. – К. : Вища школа, 1979. – 192с.*
2. *Лима, Т. Введение в dBASE IV. [Текст] / Т. Лима ; Пер. с англ. М.: Радио и связь, 1993. 304с.*
3. *Романов, Б. А. dBASE IV. Назначение,функции,применение [Текст] / Б. А. Романов, А. С. Кушнирепко. М. : Радио и связь, 1991. 384с.*
4. Петренко А. И. Применение Grid технологий в науке и образовании / А. И. Петренко – Львов : Изд-во Политехника", 2009 –144 с.
5. Сафонов В. Платформа облачных вычислений Microsoft Windows Azure: Учебное пособие. / В. Сафонов. – М. : Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2013. – 240 с.

Додатковий

6. Абламейко С.В. "Облачные" технологии в образовании / С. В. Абламейко, Ю.И. Воротницкий, Н.И. Листопад // Электроника: ежемесячный журнал для специалистов. – Минск, 2013. – №9. – С. 30- 34.
7. Биков В.Ю. Хмарна комп'ютерно-технологічна платформа відкритої освіти та відповідний розвиток організаційно-технологічної будови іт-підрозділів навчальних закладів / В.Ю. Биков // Теорія і практика управління соціальними системами. – 2013. – № 1. – с. 81-98.

8. Вакалюк Т.А. Можливості використання хмарних технологій в освіті / Т.А. Вакалюк // Актуальні питання сучасної педагогіки. Матеріали міжнародної науково-практичної конференції (м. Острог, 1-2 листопада 2013 року). – Херсон: Видавничий дім "Гельветика", 2013. – С. 97–99.
9. Лотюк Ю.Г. Хмарні технології у навчальному процесі внз / Ю.Г. Лотюк // Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ. – 2013. – Вип. 1. – С. 61-67.
10. Листопад Н.І. Модели функционирования "облачной" компьютерной системы / Н.И. Листопад, Е.В. Олизарович. – Доклады БГУИР. – №3 (65). – 2012. – С. 23-29.
11. Морзе Н. В. Педагогічні аспекти використання хмарних обчислень / Н. В. Морзе, О. Г. Кузьмінська // Інформаційні технології в освіті. – 2011. – № 9. – С. 20– 29.
12. Олексюк В.П. Досвід інтеграції хмарних сервісів Google Apps у інформаційноосвітній простір вищого навчального закладу / В.П. Олексюк // Інформаційні технології і засоби навчання. – 2013. – Том 35. – № 3. – С. 64-73.
13. Сейдаметова З.С. Облачные сервисы в образовании / З.С. Сейдаметова, С. Н. Сейтвелиева // Інформаційні технології в освіті. – 2011. – Вип. 9. – С. 104-110.
14. Chao L. Cloud Computing for Teaching and Learning: Strategies for Design and Implementation./ L.Chao – University of Houston-Victoria, 2012. – ISBN 978-1-4666-0957-0. – 357 p
15. Shor R.M. Cloud computing for learning and performance professionals . – American Society for Training & Development, 2011. – 20 p.
16. Warschauer M. Learning in the Cloud: How (and Why) to Transform Schools with Digital Media./ M. Warschauer – New York: Teachers College, 2011. – 68 p.

Інтернет ресурси:

1. Портал довідкових ресурсів Майкрософт – Режим доступу: https://www.microsoft.com/uk-ua
2. Портал навчальних ресурсів Майкрософт – Режим доступу: https://education.microsoft.com/
3. Портал хмарного сервісу Azure Microsoft – Режим доступу: https://azure.microsoft.com/en-us/training/
4. Облік SaaS бухгалтерія онлайн – Режим доступу: https://ioblik.com/uk
5. Enterprise Cloud Strategy e-Book – Режим доступу: https://info.microsoft.com/enterprise-cloud-strategy-ebook.html

****Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ***

7. **Контроль та оцінювання результатів навчання:** положення про оцінювання результатів навчання студентів і аспірантів наказ КНТЕУ №2891 від 16.09.2019р.

Під час вивчення дисципліни «Безпека інтернет-ресурсів» викладачем здійснюється поточний та підсумковий контроль. Поточний контроль та оцінювання передбачає:

- перевірку рівня засвоєння теоретичного матеріалу (тестування за матеріалами лекції, який здійснюється на початку кожної наступної лекції з використанням 365 Office);
- захист лабораторних робіт (проходить під час наступної лабораторної роботи);
- перевірка засвоєння матеріалу, що винесений на самостійне опрацювання під час фронтального опитування на лекції.

8. Політика навчальної дисципліни:

8.1. **Відвідування лекційних та лабораторних занять:** відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).

8.2. **Відпрацювання пропущених занять:** відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).

8.3. **Правила поведінки під час занять:** обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем).

8.4. **За порушення академічної доброчесності** студенти будуть притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження навчального курсу.