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. п. 6 від «04» 05 2021 р.)
Ректор
_____ А.А. Мазаракі

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ / INTERNET RESOURCE SECURITY

ПРОГРАМА / COURSE SUMMARY

Київ 2021

Розповсюдження і тиражування без офіційного дозволу КНТЕУ заборонено

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

Програму розглянуто і затверджено на засіданні кафедри програмної інженерії програмного забезпечення та кібербезпеки 20 квітня 2021 р., протокол №8.

Рецензенти: Рзаєва С.Л., канд. техн. наук, доцент,
Бабенко Б.Т., технічний директор CIO, Softorino Inc.

БЕЗПЕКА ІНТЕРНЕТ-РЕСУРСІВ /
INTERNET RESOURCE SECURITY

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Програма дисципліни «Безпека інтернет-ресурсів» призначена для здобувачів другого рівня вищої освіти «Магістр» галузі знань 12 «Інформаційні технології», спеціальності 124 «Системний аналіз», спеціалізації «Інформаційні технології та бізнес-аналітика (Data Science)».

Програму підготовлено відповідно до вимог Стандартів вищої освіти України зі спеціальності 124 «Системний аналіз» та освітньо-професійної програми КНТЕУ «Інформаційні технології та бізнес-аналітика (Data Science)» другого (магістерського) рівня вищої освіти.

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.

Програма та робоча програма складається з таких розділів:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТДИСЦИПЛІНИ

Метою викладання дисципліни є формування теоретичних знань та практичних навичок необхідних для безпечного використання інтернет-ресурсів і безпечній роботі в глобальних мережах.

Предметом вивчення дисципліни є вивчення основних положень і принципів, покладених в безпеку функціонування інтернет-ресурсів, та програмних і технічних засобах що їх реалізують.

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.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

Знати:

- вимоги нормативних документів України по безпеці в глобальних мережах;
- основні положення, організацію та моделі систем захисту інтернет-ресурсів;
- класифікацію атак на інтернет-ресурси та міри протидії;
- технологію та правила мережевої аутентифікації ресурсів і користувачів;
- організацію і правила безпеки при роботі в глобальних мережах;
- технологію та правила експлуатації міжмережевих екранів;
- основи технології віртуальних захищених мереж VPN;
- основи забезпечення захисту в мережевих протоколах передачі.

Вміти:

- визначати загрози інтернет-ресурсам;
- здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі;
- організувати захищений видалений доступ до інтернет-ресурсів;
- аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них;
- встановлювати і налагоджувати міжмережеві екрани;
- реєструвати порушення режиму безпеки і складати звіти;
- розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів;
- створювати захист за допомогою програмних засобів;
- організовувати безпечну роботу в глобальних мережах;

– використовувати VPN-рішення для побудови захищених мереж;
– управляти засобами безпеки інтеренет-ресурсів.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека інтернет-ресурсів», як вибіркова компонента освітньої-наукової програми «Інформаційні технології та бізнес-аналітика (Data Science)», забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за освітньо-професійними програмами:

Інформаційні технології та бізнес-аналітика (Data Science)

ОС «Магістр»

Номер в освітній програмі	**Зміст компетентності**	**Номер теми, що розкриває зміст компетентності**
Загальні компетентності		
ЗК3.	Здатність до пошуку, оброблення та аналізу інформації з різних джерел	1, 2, 3, 6
Спеціальні (фахові, предметні) компетентності		
СК2.	Здатність проєктувати архітектуру інформаційних систем.	4, 5, 6
СК3.	Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи.	4, 5, 6
СК7.	Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.	2,3,4
СК13.	*Здатність розробляти і впроваджувати моделі задач інтелектуального аналізу даних засобами комп'ютерного моделювання.*	1,5,6
Програмні результати навчання		
РН 1.	Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.	1, 2, 4

РН 4.	Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи.	4, 5, 6
РН 5.	Використовувати міри оцінювання ризиків та застосовувати їх при аналізі багатофакторних ризиків в складних системах.	2, 3, 5
РН 8.	Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об’єктів керування.	5, 6

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Основи мережевої безпеки

Розподілені ресурси: механізми безпеки і управління. Мережева безпека: терміни та визначення. Нормативні документи по безпеці в глобальних мережах. Стандарти безпеки мереж і їх компонентів. Класифікація мережевих загроз та атак на інтернет-ресурси. Технології виявлення віддалених атак. Соціальна інженерія. Шляхи вирішення проблем захисту інтернет-ресурсів.

Список рекомендованих джерел:
Основний: 4,6,7,8
Додатковий: 12, 13

Тема 2. Технології фільтрації мережевого трафіку

Фільтрація трафіку. Фільтрація Web-змісту (WCF). Віртуальні локальні мережі (VLAN). Технологія перетворення мережевих адрес (NAT). Міжмережеві екрани (МЕ): класифікація та функції МЕ. Варіанти виконання МЕ. Схеми мережевого захисту на базі МЕ. Основні схеми підключення МЕ. Персональні і розподілені мережеві екрани. Довірена мережа та DMZ мережі. Формування політики міжмережевої взаємодії. Проблеми безпеки МЕ.

Список рекомендованих джерел:
Основний: 4,5,6,7,8
Додатковий:11, 12

Тема 3. Основи технології віртуальних приватних мереж

Концепція побудови віртуальних приватних мереж VPN. Основні поняття і функції мережі VPN. Варіанти побудови віртуальних захищених каналів. Засоби забезпечення безпеки VPN. VPN-рішення для побудови захищених мереж. Класифікація мереж VPN. Основні варіанти архітектури VPN.

Список рекомендованих джерел:
Основний: 4,5,6,7
Додатковий: 11,12,13

Тема 4. Протоколи мережевої безпеки

Протоколи захисту інтеренет-ресурсів на канальному рівні (протокол PPTP, L2TP). Протоколи формування захищених каналів на сеансовому рівні (протоколи SSL/TLS, SOCKS) . Захист інтернет-ресурсів на мережевому рівні (протокол IPSec). Особливості реалізації засобів IPSec. Основні схеми застосування IPSec . Протоколи захисту у безпроводних мережах. Механізм шифрування WEP. Специфікація WPA. Стандарт мережі з підвищеною безпекою WPA2.

Список рекомендованих джерел:
Основний: 4,5,7
Додатковий: 11,12

Тема 5. Безпека інтернет-ресурсів на прикладному рівні

Управління мережевою ідентифікацією і доступом. Особливості управління доступом. Функціонування системи управління доступом. Організація захищеного видаленого доступу. Протоколи аутентифікації видалених користувачів. Централізований контроль видаленого доступу. Протокол Kerberos. Інфраструктура управління відкритими ключами PKI.

Список рекомендованих джерел:
Основний: 4,5,6,7,10
Додатковий: 11,12

Тема 6. Аналіз безпеки інтернет-ресурсів

Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Засоби аналізу захищеності мережевих протоколів і сервісів. Технології виявлення атак. Класифікація систем виявлення атак IDS. Компоненти і архітектура IDS. Системи попередження атак IPS. Методи реагування систем на атаки. Безпечне розгортання сервісів DNS. Безпека Web-серверів. Безпечна мережева інфраструктура для Web-сервера.

Список рекомендованих джерел:
Основний: 4,5,6,7
Додатковий: 11,13

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*

ЛИСТ ПОГОДЖЕННЯ

програми дисципліни «Безпека інтернет-ресурсів»

Погоджено

Завідувач кафедри інженерії програмного забезпечення та кібербезпеки

_____ О. В. Криворучко

«_____»_____ 2021р.

Погоджено

Гарант освітньої програми ДТЕУ, спеціалізація «Інформаційні технології та бізнес-аналітика (Data Science)»

_____ А.А. Роскладка

«_____»_____ 2021р.

Погоджено

Заступник декана з наукової і методичної роботи

_____ К. В. Хорольська

«_____»_____ 2021р.