МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
інформаційних систем.
Протокол № 1 від 27.08.2024 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

_____ Каріна НЕМАШКАЛО

БЕЗПЕКА ІС

робоча програма навчальної дисципліни (РПНД)

Галузь знань	12 "Інформаційні технології"
Спеціальність	126 «Інформаційні системи та технології»
Освітній рівень	другий (магістерський)
Освітня програма	"Інформаційні системи та технології"

Статус дисципліни	обов'язкова
Мова викладання, навчання та оцінювання	українська

Розробник:
к.т.н., доцент підписано КЕП Андрій ПОЛЯКОВ

Завідувач кафедри
інформаційних систем _____ Дмитро БОНДАРЕНКО

Гарант програми підписано КЕП Олександр КОЛГАТІН

Харків
2024

ВСТУП

Навчальна дисципліна "Безпека ІС" є ключовою у формуванні компетентностей у галузі захисту інформаційних систем і технологій. В умовах сучасного інформаційного суспільства, де обсяги даних зростають експоненціально, а інформаційні технології проникають у всі сфери людської діяльності, значення надійної інформаційної безпеки важко переоцінити. Зростання числа кібератак, їхньої складності та потенційних збитків вимагає від фахівців глибоких знань і навичок у захисті інформаційних активів. Дисципліна спрямований на розробку, аналіз і застосування комплексних заходів захисту, які забезпечують цілісність, конфіденційність і доступність інформації. Особлива увага приділяється сучасним стандартам та методологіям, криптографічному захисту даних, методам пом’якшення погроз безпеки, побудови безпечного процесу розробки та розгортання програмного забезпечення, а також стратегіям управління ризиками та контролю доступу, що є невід'ємною частиною сучасних інформаційних систем.

Вивчення дисципліни "Безпека ІС" передбачає опанування знань з основних положень кібербезпеки; стандартів безпеки по обробці та зберіганню персональних даних; застосування методів криптографічної безпеки; безпека розглядається як проблема бізнесу; освоєння опанування навичок з використання засобі; дослідження сучасні погрози відносно Web-, мобільних застосунків та API, а також створення безпечного циклу розробки програмного забезпечення. Окрім того, важливо набути вміння проектувати та розробляти застосунки до ІС, з урахуванням вимог безпеки та захисту від сучасних погроз.

Метою викладання навчальної дисципліни "Безпека ІС" є набуття здобувачами глибоких теоретичних знань та практичних навичок у сфері захисту інформаційних систем, включаючи ідентифікацію та аналіз загроз, розробку та впровадження комплексних заходів безпеки, а також управління ризиками і контролю доступу. Курс також спрямований на оволодіння здобувачами сучасними технологіями та методологіями захисту даних, криптографічним захистом інформації, забезпеченням безпеки мережевих інфраструктур та безпеки при розробці програмного забезпечення.

Завданнями навчальної дисципліни є:

- надання здобувачам необхідних теоретичних знань про методи та засоби безпеки в інформаційних системах;
- розвиток практичних навичок використання криптографічних засобів безпеки;
- навчання здобувачів навичкам захисту Web-застосунків та дослідження атак з підробкою запитів;
- формування системи знань щодо сучасного стану погроз, атак та послуг безпеки;
- формування системи знань щодо міжнародних стандартів та фреймворків із забезпечення безпеки даних та механізмів безпеки;
- засвоєння принципів побудови, призначення, структури процесу безпечної розробки програмного забезпечення;

− засвоєння основних практик проектування та розробки багаторівневих Web- орієнтованих програмних компонентів з забезпеченням вимог безпеки;

− розуміння основних криптографічних методів та протоколів симетричного / асиметричного шифрування, цифрового підпису, забезпечення цілісності даних, управління ключами, blockchain;

− оволодіння навичками моделювання погроз інформаційної системи.

Предметом навчальної дисципліни "Безпека інформаційних систем" є вивчення методів, технологій, стандартів та процедур, які забезпечують захист інформаційних ресурсів від несанкціонованого доступу, змін, розголошення та інших загроз. Основна увага приділяється аналізу та оцінці ризиків, управлінню доступом, криптографічному захисту даних, а також безпеці мереж і розробці програмного забезпечення.

Об'єктом дисципліни є інформаційні системи та мережі, їх інфраструктура, дані, програмне забезпечення та операційні процедури, що потребують захисту від внутрішніх та зовнішніх загроз.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	Компетентності, якими повинен оволодіти здобувач вищої освіти
РН03.	СК06.
РН10.	ЗК05, СК03, СК06
РН12.	СК06.

де, РН03 Приймати ефективні рішення з проблем розвитку інформаційної інфраструктури, створення і застосування ІСТ;

РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

РН12. Удосконалювати інформаційну систему на основі аналізу бізнес-процесів.

ЗК05. Здатність оцінювати та забезпечувати якість виконуваних робіт.

СК03. Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної / недостатньої інформації та суперечливих вимог.

СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Методи і стандарти безпеки даних та систем

Тема 1. Ідентифікація та управління доступом

1.1. Принципи безпеки. Ідентифікація, автентифікація, авторизація: ідентифікатори, слабка / сильна автентифікація, біометрична автентифікація: статична/динамічна, токен аутентификации, смарт-карта, сертифікат, security identifier (SID). Протоколи автентифікації.

1.2. Моделі контролю доступу. виборче управління доступом, мандатне управління доступом, управління доступом на основі ролей, управління доступом на основі атрибутів.

1.3. Методи та технології контролю доступу, правила розмежування, пароль, маркер(авторизація), двофакторна аутентифікація, мультифакторна аутентифікація.

1.4. Загрози контролю доступу: стійкість паролю, загрози подолання парольного захисту, отримання привілеїв, сховані канали.

1.5. Моніторинг контролю доступу. журналювання, журнальована файлова система, аудит, логування.

Тема 2. Стандарти безпеки

2.1. Політика, стандарти, рекомендації та процедури. Міжнародні стандарти: ISO/IEC 27001:2013/27002:2013/27005:2015/27006:2015/27005.

2.2. NIST Cybersecurity Framework

2.3. Управління ризиками: Основні критерії, критерії оцінки ризиків, критерії впливу, критерії визнання ризиків, застосування та межа організаційної структури управління ризиками, аналіз ризиків, ідентифікація ризику вимір ризику

2.4. Моделювання загроз: Аналіз ризиків, ідентифікація загроз, ідентифікація вразливості ідентифікації активів.

2.5. Фреймворки управління ризиками.

Тема 3. Визначення та поняття криптографії

3.1. Методи шифрування: сучасні стандарти симетричного шифрування, стійкість методів симетричного шифрування, режими шифрування;

3.2. Основні принципи асиметричної криптографії, схеми асиметричного шифрування RSA/ECES, Схема асиметричного шифрування Рабіна, Схема асиметричного шифрування Ель Гамаля, Протокол Діффі-Хеллмана.

3.3. Цілісність повідомлення: Ключові та без ключові геш-функції, MAC/HMAC, Електронний цифровий підпис ECDSA, Груповий цифровий підпис. Сліпий цифровий підпис. Разовий цифровий підпис. Стандарти цифрового підпису на еліптичній кривій.

3.4. Інфраструктура відкритих ключів: Політика використання сертифікатів. Сертифікати відкритих ключів X.509. Компоненти і сервіси інфраструктури відкритих ключів. Списки скасованих сертифікатів. Політика ІВК. Проблеми та ризики технології ІВК.

3.5. Криптографічні атаки: Модель порушника. Вимоги до сучасних криптоалгоритмів. Факторизація. Метод факторизації загальне решето числового поля. Методи розв'язання дискретний логарифму в групі точок еліптичній кривій.

Безпека інформаційної системи підприємства

Тема 4. Комунікаційна та мережева безпека

4.1. *Мережева модель OSI*: Рівні моделі OSI, Прикладний рівень, Транспортний рівень, Міжмережевий рівень, Рівень доступу до середовища передачі, (Network Access Layer), Взаємодія рівнів.

4.2. *Модель TCP/IP*: Порівняння з моделлю OSI, розподіл протоколів за рівнем TCP/IP.

4.3. *Мережеві організації*. Інтернет-провайдер, Root DNS.

4.4. *Мережеві пристрої*: міст, комутатор, маршрутизатор, proxy, vlan.

4.5. *Бездротові мережі*: IEEE 802.11, організація мереж Wi-Fi, Прямі та непрямі погрози, автентифікація, шифрування в мереж Wi-Fi.

4.6. *Шифрування мережі*. Побудова VPN мереж. Шифрування трафіку в протоколі IPSec. Шифрування трафіку та забезпечення цілісності даних в протоколі SSL. Шифрування трафіку та забезпечення цілісності даних в протоколі TLS. Керування ключами в протоколі IPSec. Перевірка дійсності сертифікатів TLS/SSL. Цілісність та автентичність в протоколах прикладного рівня моделі OSI. Протокол SSH.

4.7. *Мережеві атаки*: DoS-атака, схеми DNS-атак. Атакі типа DNS-флуд, Атака на кеш DNS-сервера.

Тема 5. Безпека розробка Web- та мобільних застосунків

5.1. Погрози та методи нападу у Web- та мобільних застосунків. OWASP

5.2. Атака міжсайтових скриптинг: Cross-Site Scripting (XSS)

5.3. Атака міжсайтового підроблення запиту Cross-Site Request Forgery (CSRF)

5.4. Атака зовнішнього об'єкту XML XML External Entity (XXE).

5.5. Атаки типу ін'єкція: SQL ін'єкції, ін'єкція коду, ін'єкція команд

5.6. Використання сторонніх залежностей: методи інтеграції, менеджери пакетів, база даних вразливостей та ризиків

Тема 6. Безпека розробки програмного забезпечення

6.1. *Моделі розробки програмного забезпечення*: каскадна модель, спіральна модель, нефункціональних вимог до системи.

6.2. Життєвий цикл розробки програмного забезпечення (Software DLC).

6.3. *Інтегрування безпеки у SDLC*: статичний аналіз коду, динамічний аналіз коду, аналіз складу програмного забезпечення, інтерактивне тестування безпеки додатків.

6.4. *Мобільний код*: вимоги щодо безпеки мобільних програмних додатків.

6.5. *Управління базами даних*: вимоги безпеки для баз даних,

6.6. *Зловмисне програмне забезпечення*: різні типи зловмисних програм , атаки та способи захисту ІТ-системи від зловмисного програмного забезпечення.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2.

Таблиця 2

Перелік лабораторних занять

Назва теми	Зміст
Тема 1	Дослідження методів розмежування доступу в системі Linux.
Тема 2-3	Дослідження сучасних криптографічних стандартів симетричної криптографії.
Тема 2-3	Дослідження сучасних криптографічних стандартів асиметричної криптографії.
Тема 4	Дослідження роботи FireWall та методи його обходу
Тема 5	Дослідження сучасних атак на Web застосунки: атака CSS.
Тема 5	Дослідження сучасних атак на Web застосунки: атаки CSRF та SQL ін’єкція.
Тема 6	Дослідження методів динамічного та статичного аналізу коду програмного забезпечення.

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3.

Таблиця 3

Перелік самостійної роботи

Назва теми	Зміст
Тема 1 – 6	Вивчення лекційного матеріалу
Тема 1 – 6	Підготовка до лабораторних занять
Тема 1 – 6	Підготовка до поточних контрольних робіт

Кількість годин лекційних та лабораторних занять, а також годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:

Словесні (лекція (Тема 1 – 4), проблемна лекція (Тема 4 – 6), лекція-візуалізація (Тема 1 – 6)).

Наочні (демонстрація (Тема 5 – 6)).

Лабораторна робота (Тема 1 – 6), кейс-метод (Тема 4 – 6).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних та практичних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів:

− для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формі диференційованого заліку або заліку.

Підсумкова оцінка за навчальною дисципліною визначається:

− для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

Поточний контроль: захист лабораторних робіт (60 балів), поточні контрольні роботи (20 балів), презентацій (20).

Семестровий контроль: Залік

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

ОСНОВНА

1. В.І. Гур'єв Інформаційна безпека держави: навч. посіб. для студ. спец. «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. — Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2018.

2. Довгань О. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / О. Довгань, Л. Литвинова, С. Дорогих. — К. : Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського, 2023. — 300 р.

3. Ю.Г. Даник ОСНОВИ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. — Одеса : ОНАЗ ім. О.С. Попова, 2019. — 320 р.

ДОДАТКОВА

4. Ю. І. Горбенко Прикладна криптологія. Теорія. Практика. Застосування / Ю. І. Горбенко, І. Д. Горбенко. — Харків : Видавництво «Форт», 2012. — 870 р.

5. Домарев, В. В. Безпека інформаційних технологій. Системний підхід / В. В. Домарев. - К .: ДиаСофт, 2004.

6. R. Ross, M. McEvilley and J. C. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, 2016.

7. Ross R. Developing Cyber-Resilient Systems:: A Systems Security

Engineering Approach / R. Ross, V. Pillitteri, R. Graubart, [та ін.]. — Gaithersburg, MD : National Institute of Standards and Technology, 2021. — NIST SP 800-160v2r1 p.

8. ДСТУ ISO/IEC 15946-3:2006 Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Встановлення ключів (ISO/IEC 15946-3:2002, IDT).

9. В. Ю. Зубок, Кібербезпека топології INTERNET : монографія / В. Ю. Зубок,, В. В. Мохор. — К. : ІПМЕ ім. Г.Є.Пухова, 2022. — 191 р.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

10. Cybersecurity Framework / NIST. — 2024. Available at: https://www.nist.gov/cyberframewor.

11. TechRepublic: News, Tips & Advice for Technology Professionals [Електроний ресурс] // TechRepublic. — Електрон. дані. — Режим доступу: https://www.techrepublic.com/.

12. Основні ресурси | Ваша повна бібліотека з кібербезпеки [Електронний ресурс] // KnowledgeFLOW. — Електрон. дані. — Режим доступу: https://knowledgeflow.org/uk/resources/.

13. Index Top 10 - OWASP Top Ten 2021 : Related Cheat Sheets [Електроний ресурс] // OWASP Cheat Sheet Series. — Електрон. дані. — Режим доступу: https://cheatsheetseries.owasp.org/IndexTopTen.html.

14. OWASP WSTG - Web Security Testing Guide [Електронний ресурс] // Latest | OWASP Foundation. — Електрон. дані. — Режим доступу: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/.

15. Server Side Request Forgery [Електронний ресурс] // OWASP Foundation. — Електрон. дані. — Режим доступу: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery.

16. Server Side Request Forgery Prevention [Електронний ресурс] // OWASP Cheat Sheet Series. — Електрон. дані. — Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html.