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

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**12 "Інформаційні технології"**
Спеціальність	**121 "Інженерія програмного забезпечення"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"Інженерія програмного забезпечення"**

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

Розробник(и):
д.т.н., проф. підписано КЕП Сергій СЕМЕНОВ

Завідувач кафедри
кібербезпеки та
інформаційних технологій
д.т.н., проф. Ольга СТАРКОВА

Гарант програми
к.т.н., доц. Олег ФРОЛОВ

Харків
2024

ВСТУП

Захист інформації перетворюється сьогодні на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише у захищеному вигляді в інформаційних системах (ІС).

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів та медичних карт, студентських квитків та залікових книжок; зрештою все більше державних установ та приватних підприємств переходять на електронний документообіг, який до того ж, вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Метою викладання дисципліни є навчання здобувачів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Завданнями навчальної дисципліни є отримання навичок: аналізу потенційних загроз для основних послуг безпеки інформації, оцінки та управління ефективного захисту інформації та інформаційних систем в сучасному цифровому середовищі.

Предметом навчальної дисципліни є безпека програм та даних.

Об'єктом навчальної дисципліни є технічні засоби, програмні продукти, процеси та методи, які використовуються для забезпечення безпеки інформації в системах.

Результатами вивчення даної дисципліни є придбання навичок з використання методів шифрування інформації для подальшої передачі її телекомунікаційними каналами зв'язку.

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

Таблиця 1

Компетентності та результати навчання за дисципліною

Результати навчання	Компетентності, якими повинен оволодіти здобувач вищої освіти
РН13	СК 6
РН 21	ЗК 2, СК 6, СК 7, СК 10

де ЗК 2. Здатність застосовувати знання у практичних ситуаціях.

СК 6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

СК 7. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

СК 10. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.

РН 13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.

РН 21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Тема 1. Основні поняття та визначення кібербезпеки

1.1. Роль інформації у світі, значення захисту.

1.2. Послуги та механізми захисту інформації.

Тема 2. Основи криптографії. Прості алгоритми шифрування

2.1. Термінологія.

2.2. Історія криптографії.

2.3. Сучасна криптографія.

2.4. Шифрування і розшифрування.

Тема 3. Протоколи аутентифікації. Цифровий підпис.

3.1. Класична задача криптографії.

3.2. Криптоаналіз.

Тема 4. Система PGP.

4.1. Коротка характеристика функцій системи PGP

4.2. Принцип роботи системи.

4.3. Надсилання та отримання повідомлень PGP.

4.4. Загальний формат повідомлення PGP.

Тема 5. Алгоритми забезпечення цілісності даних

5.1. Зв'язки особистих-відкритих ключів.
5.2. Ступені довіри у системі PGP
5.3. Надсилання та отримання повідомлень PGP

Тема 6. Забезпечення безпеки даних на мережевому рівні

6.1. Надмірність коду.
6.2. Код із перевіркою на парність.
6.3. Код Хеммінгу.

Тема 7. Забезпечення безпеки даних на мережевому рівні

7.1. Технології та стандарти фізичного рівня 802.11
7.2. Безпека бездротових мереж
7.3. Вразливість алгоритму WEP
7.4. Базова автентифікація

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

Таблиця 2

Перелік лабораторних занять

Назва завдання	Зміст
Тема 1. Лабораторна робота 1. Найпростіші шифри.	Основні принципи роботи найпростіших шифрів; елементи криптоаналізу, зокрема частотного аналізу криптограм.
Тема 2. Лабораторна робота 2. Блочно симетричні шифри.	Забезпечення конфіденційності та цілісності інформації за допомогою блокових симетричних шифрів;
Тема 3. Лабораторна робота 3. Асиметричні криптосистеми.	Використання механізмів асиметричного шифрування для забезпечення конфіденційності повідомлень.
Тема 4. Лабораторна робота 4. Алгоритм цифрового підпису	Застосування й дослідження системи цифрового підпису з використанням несиметричних крипто перетворень.
Тема 5. Лабораторна робота 5. Стеганографічні методи захисту інформації	Основні методи стеганографічного захисту інформації, використання відповідних програмних засобів.
Тема 6. Лабораторна робота 6. Використання програми PGP для шифрування повідомлень електронної пошти	Програмні засоби забезпечення безпеки електронної пошти за допомогою шифрування та цифрового підпису.
Тема 7. Лабораторна робота 7. «Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST STS»	Методика досліджень статистичних властивостей генераторів випадкових та псевдовипадкових послідовностей.

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

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1. Завдання 1	Основні поняття та визначення кібербезпеки
Тема 2. Завдання 2.	Основи криптографії. Прості алгоритми шифрування
Тема 3. Завдання 3.	Протоколи автентифікації. Цифровий підпис
Тема 4. Завдання 4.	Система PGP
Тема 5. Завдання 5.	Дослідження системи PGP
Тема 6. Завдання 6.	Алгоритми забезпечення цілісності даних
Тема 7. Завдання 7.	Забезпечення безпеки даних на мережевому рівні Мережі стандарту 802.11.

Кількість годин лекційних та лабораторних занять та 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 (лекції 1-7), проблемна лекція (Тема 1).

Наочні (демонстрація (Тема 1-7)).

Практичні (лабораторні роботи (Теми 1-7)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

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

Поточний контроль здійснюється під час проведення лекційних, лабораторних 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 заліку.

Підсумкова оцінка за навчальною дисципліною визначається сумуванням всіх балів, отриманих під час поточного контролю.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

Поточний контроль: Індивідуальні навчально-дослідні (лабораторні) завдання (60 балів), дві письмові контрольні роботи (40 балів).

Семестровий контроль: Залік.

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

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Лісовська, Ю. П. Інформаційна безпека України : навчальний посібник для студентів вищих навчальних закладів / Ю. П. Лісовська. - Київ : Кондор, 2020. - 170 с.
2. Michael E. Whitman Principles of Information Security 6th Edition / Michael E. Whitman, Herbert J. Mattord - Cengage Learning; 6th edition (March 13, 2017) 656 p.
3. Richard E. Smith Elementary Information Security 3rd Edition / Jones & Bartlett Learning; 3rd edition (October 28, 2019) – 708 p.
4. Євсеєв, С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. Електрон. текстові дан. (12,3 МБ). Харків : ХНЕУ ім. С. Кузнеця, 2020. 221 с.: іл. Загол. з титул. екрану. Бібліогр.: с. 211-213. http://repository.hneu.edu.ua/handle/123456789/24508
5. Milov O. Self-organizing organizational structures of cybersecurity systems / O. Milov, V Aleksiyev. // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. Vienna: Premier Publishing s.r.o., 2020. P. 65-78. http://repository.hneu.edu.ua/handle/123456789/24816

Додаткова

6. Jason Andress Foundations of Information Security: A Straightforward Introduction / No Starch Press (October 7, 2019) – 248 p.
7. Якименко І.З. // Опорний конспект лекцій з дисципліни „Безпека програм та даних„ ‖, для студентів спеціальності „Кібербезпека„‖. – Тернопіль, 2019. – 50 с.
8. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
9. Martovytskyi V. Technology for monitoring the functioning state of distributed computer systems / V. Martovytskyi, Y. Koltun, D. Holubnychyi et al. // Системи управління, навігації та зв'язку : зб. наук. пр. – 2022. – Вип. 1 (67). – С. 75-80. http://www.repository.hneu.edu.ua/handle/123456789/27369.

Інформаційні ресурси.

10. EVE - віртуальне середовище в області мереж, безпеки та DevOps https://www.eve-ng.net/
11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Захист інформації" https://pns.hneu.edu.ua/course/view.php?id=8937