Силабус освітнього компонента
Програма навчальної дисципліни

Основи кібербезпеки

Шифр та назва спеціальності
122 – Комп’ютерні науки

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма
Комп’ютерні науки та інтелектуальні системи

Кафедра
Програмна інженерія та інтелектуальні технології управління (321)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
6

Мова викладання
Українська, англійська

Викладачі, розробники

Євсеєв Сергій Петрович
serhii_yevseiev@khpi.edu.ua
Доктор технічних наук, проф., професор кафедри ПІІТУ НТУ «ХПІ»

Підготував і опублікував понад 295 наукових та навчально-методичних праць (Google Scholar: https://scholar.google.com/citations?user=g-HezNwAAAAJ; ORCID https://orcid.org/0000-0003-1647-644; Scopus: https://www.scopus.com/authid/detail.uri?authorId=57190440690; Publons: https://publons.com/researcher/1527869/serhii-yevseiev/).
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Ознайомлення студентів з принципами побудови систем захисту інформації; ознайомлення студентів з основними механізмами послуг безпеки; вивчення студентами менеджменту інформаційної безпеки; навчання студентів основам аудиту інформаційної безпеки; вивчення студентами спеціальних механізмів кіберзахисту.

Мета та цілі дисципліни

Навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.

Формат занять

Лекції, лабораторні заняття. Поточний контроль – лабораторні роботи, проміжний модульний контроль. Підсумковий контроль – екзамен.

Компетентності

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Результати навчання

ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредитів ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 42 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика
Комп'ютерні мережі
Основи веб-розробки

Особливості дисципліни, методи та технології навчання

Методи викладання та навчання:
інтерактивні лекції з презентаціями, дискусії, лабораторні заняття, командна робота, кейс-метод, метод зворотного зв'язку з боку студентів, проблемне навчання.
Форми оцінювання:
письмові індивідуальні завдання до лабораторних робіт (CAS), оцінювання знань на лабораторних заняттях (CAS), експрес-опитування (CAS), онлайн-тести (CAS), підсумковий/семестровий контроль у формі семестрового екзамену, відповідно до графіку навчального процесу (FAS).

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Поняття кібербезпеки держави та складових національних інтересів України в кібербезпеки
Основні етапи проведення внутрішнього аудиту з інформаційної безпеки.
Тема 2. Аналіз ризиків в області кібербезпеки. Класифікація кіберзагроз. Практичні моделі розмежування прав доступу
Ознайомлення з основними каналами витоку інформації. Основні принципи формування класифікаторів комп'ютерних інцидентів, кіберзагроз.
Тема 3. Механізми забезпечення конфіденційності та цілісності даних
Основні механізми забезпечення цілісності в інформаційних системах.
Тема 4. Механізми забезпечення автентифікації
Основні спеціальні геш-функції. Стандарти цифрового підпису, їх класифікація.
Тема 5. Основні напрямки розвитку сучасної криптографії
Методи стеганографії у просторової та частотної області.
Тема 6. Механізми та протоколи керування ключами в ІВК
Основні протоколи PKI на основі симетричної та несиметричної криптографії.
Тема 7. Технології аналізу ризиків
Методики аналізу ризиків.
Тема 8. Аналіз ризиків в управлінні неформаційною безпекою
Методики аналізу ризиків.

Теми практичних занять

Практичні заняття в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та інформаційних систем
Тема 2. Інструменти прихованого збору технічної інформації з інформаційної системи або комп'ютерної мережі
Тема 3. Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування
Тема 4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA. Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus
Тема 5. Стеганографічні методи захисту інформації
Тема 6. Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST
Тема 7. Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega
Тема 8. Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng

Самостійна робота

Індивідуальних завдань не передбачено навчальним планом.
Студентам рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та опрацювання.

Література та навчальні матеріали

Основна література

1. Євсеєв С.П, Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.
2. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
3. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, "Забезпечення інформаційної безпеки держави", К: ПВП "Задруга", 2013.

Додаткова література

4. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том I. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
6. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
7. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
8. Doctrine of information security of Ukraine, approved by Decree of the President of Ukraine dated February 25, 2017 No. 47/2017. [Electronic resource]. Available: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.
9. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016).

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

100% підсумкове оцінювання у вигляді екзамену (36%) та поточного оцінювання (64%).
36% екзамен
64% поточне оцінювання:
Модуль №1 (12%)
Модуль №2 (12%)
Лабораторні роботи (40%)
Лабораторна робота № 1 (5%)
Лабораторна робота № 2 (5%)
Лабораторна робота № 3 (5%)
Лабораторна робота № 4 (5%)
Лабораторна робота № 5 (5%)
Лабораторна робота № 6 (5%)
Лабораторна робота № 7 (5%)
Лабораторна робота № 8 (5%)

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	08.06.2023	Завідувач кафедри Ігор ГАМАЮН
	08.06.2023	Гарант ОП Андрій КОПП