Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ЦТЕ

Кафедра цифрових технологій в енергетиці

Безпека інформаційних систем

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Цифрові технології в енергетиці*
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*4/120 год 36лек 18лаб 66СРС*
Семестровий контроль/ контрольні заходи	*М.к.р., екзамен*
Розклад занять	*http://roz.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доцент, к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com,* *Лабораторні роботи: доцент, к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com,*
Розміщення курсу	*https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity* *https://campus.kpi.ua*

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Навчальна дисципліна **«Безпека інформаційних систем»** покликана сформувати у студентів знання та компетентності, необхідні для ефективної організації та реалізації захисту інформаційних та телекомунікаційних систем/мереж, комплексного забезпечення інформаційної безпеки систем та мереж, вивчення принципів та одержання практичних навичок створення безпечної мережевої інфраструктури.

Програмою дисципліни передбачається вивчення інструментів, основних концепцій та механізмів інформаційної безпеки систем та мереж. Особлива увага приділяється особливостям побудови захищених систем та мереж, моделям та програмним комплексам оцінки характеристик стану безпеки інформаційних систем та мереж. В ході вивчення дисципліни також досліджуються особливості удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем та безпечного функціонування об'єктів критичної інфраструктури.

Метою навчальної дисципліни є формування у студентів компетентностей у відповідності до ОПП.

ЗК 2	Здатність застосовувати знання у практичних ситуаціях
ФК 14	Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

Основні завдання навчальної дисципліни.

Згідно з вимогами освітньо-професійної програми студенти після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання:

ПР 16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни необхідні знання та уміння за такими дисциплінами як «Комп'ютерна схемотехніка та архітектура» та «Комп'ютерні мережі».

Після вивчення дисципліни студенти зможуть використати набуті знання та вміння при вивченні: «Методи та системи штучного інтелекту», «Моделювання систем в енергетиці».

3. Зміст навчальної дисципліни

Тема 1. Вступ до безпеки інформаційних систем;

Тема 2. Правові аспекти безпеки інформаційних систем;

Тема 3. Стратегії захисту інформації;

Тема 4. Основи мережевої безпеки та протоколи безпеки;

Тема 5. Захист від вторгнень;

Тема 6. Основи криптографічного захисту;

Тема 7. Безпека мобільних пристроїв та хмарних обчислень;

Тема 8. Безпека IoT;

Тема 9. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем.

4. Навчальні матеріали та ресурси

Базова література:

1. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Терейковський І.А., Гнатюк С.О. Захист інформації в компютерних системах. / І.А. Терейковський, С.О.Гнатюк. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 135 с.
3. Бурячок В. Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ. ДУТ. 2015. 449 с.
4. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі. Частина 1. Навчальний посібник. Київ. КПІ ім. Ігоря Сікорського. 2020. 328 с.
5. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К. 2015. 220 с.
6. Беседовський О.М., Золотарьова І.О., Євсеєв С.П. Сучасні методи та моделі обробки даних в інформаційних системах. Х. ХНЕУ ім. С. Кузнеця. 2013. 540 с.
7. Корченко О.Г. Прикладна криптологія: системи шифрування. К. ДУТ. ТОВ «Наш формат». 2014. 448 с.

Додаткова література

1. Chris Carthern, William Wilson, Noel Rivera. Cisco Networks. Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress, 2018.1117p.
2. Joseph Muniz, Gary McIntyre, Nadhem AlFardan. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2020. 448 p.
3. Omar Santos, Panos Kampanakis, Aaron Woland. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press. 2016. 368 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

Тема 1. Вступ до безпеки інформаційних систем	
1	*Лекція 1.* Вступ до безпеки інформаційних систем. Види загроз і ризиків для інформаційних систем. Основні принципи інформаційної безпеки. Методи ІБ. Виклики в області інформаційної безпеки. Поняття «Кіберпростір». Міжнародні організації, світові ІТ гіганти

	та консорціуми: спеціальні міжнародні структури у складі збройних сил країн світу. Поняття «Кіберборотьба». Головні проблеми забезпечення кібернетичної безпеки.
Тема 2. Правові аспекти безпеки інформаційних систем	
2	*Лекція 2.* Міжнародні закони, положення і стандарти, що регулюють сферу кібербезпеки. Міжнародна співпраця в сфері кібербезпеки.
3	*Лекція 3.* Українське законодавство в сфері регулювання питань інформаційної та кібернетичної безпеки. Закон України «Про кібербезпеку», Закон України «Про інформацію». Закон України «Про захист інформації в інформаційних системах», Закон України «Про інформаційні ресурси інформаційного суспільства».
Тема 3. Стратегії захисту інформації	
4	*Лекція 4.* Стратегії захисту інформації. Компоненти стратегії захисту інформації Механізми безпеки комп'ютерних мереж. Механізми забезпечення контролю доступу, автентифікації. Механізми забезпечення конфіденційності, цілісності та доступності даних.
Тема 4. Основи мережевої безпеки та протоколи безпеки	
5	*Лекція 5.* Загальні принципи побудови та організації комп'ютерних мереж. Особливості функціонування комп'ютерних мереж. Вивчення різних типів мережевого обладнання, (маршрутизатори, комутатори та файрволи). Дослідження алгоритмів маршрутизації (RIP, OSPF, IGRP/EIGRP, BGP).
6	*Лекція 6.* Виявлення та захист від мережевих загроз. Аналіз різновидів мережевих загроз (віруси, черв'яки, шкідливі програми, DDoS-атаки тощо). Порівняльний аналіз методів виявлення та захисту від загроз з використанням продуктів різних виробників ПЗ та сучасного обладнання.
7	*Лекція 7.* Забезпечення безпеки на рівнях моделі OSI. Основні характеристики та принципи протоколів безпеки на рівнях моделі OSI (IPSec, SSL/TLS, SSH, мережеві файрволи тощо)
Тема 5. Захист від вторгнень	
8	*Лекція 8.* Поняття вторгнень у системи та їх види. Атаки на периметр мережі, атаки на додатки, атаки на внутрішній рівень та соціально інженерні атаки. Системи виявлення та запобігання вторгнень (IDS/IPS). Поняття «сигнатури».
9	*Лекція 9.* Програмно-апаратні комплекси для виявлення та запобігання вторгнень. Дослідження принципів роботи систем виявлення вторгнень на основі сигнатур та систем на основі аналізу поведінки. Стратегії реагування на вторгнення та відновлення після атаки
Тема 6. Основи криптографічного захисту	
10	*Лекція 10.* Принципи криптографії та її роль у безпеці інформаційних систем. Типи шифрування та криптографічні алгоритми. Аутентифікація і цифровий підпис. Використання криптографії для захисту даних. Криптографія в інформаційних системах, Легісляція і стандарти.
11	*Лекція 11.* Визначення стеганографії та порівняння з криптографією. Роль стеганографії у забезпеченні конфіденційності інформації. Принципи та методи стеганографії. Огляд стандартних алгоритмів та програмних засобів для стеганографії.
Тема 7. Безпека мобільних пристроїв та хмарних обчислень	
12	*Лекція 12.* Загрози безпеці мобільних пристроїв та методи їх запобігання. Дослідження сучасних методів захисту від вірусів, шкідливих програм та атак на мобільні пристрої. Розгляд засобів моніторингу та виявлення порушень на мобільних пристроях. Шифрування та захист даних на мобільних пристроях.
13	*Лекція 13.* Концепція BYOD, переваги та ризики. Розгляд стратегій та практик для впровадження BYOD в організаціях.
14	*Лекція 14.* Безпека хмарних обчислень. Поняття хмарних обчислень, переваги та обмеження. Дослідження загроз безпеці, пов'язаних із хмарними обчисленнями (атаки на

	конфіденційність, цілісність та доступність даних). Механізми аутентифікації та авторизації в хмарних сервісах.
15	*Лекція 15.* Захист віддалених користувачів. Сценарії роботи віддалених користувачів. Дослідження методів захисту віддалених з'єднань та віддалених робочих станцій. Методи моніторингу та аудиту активності віддалених користувачів для виявлення аномальних дій та порушень безпеки.
Тема 8. Безпека IoT	
16	*Лекція 16.* Захист від загроз IoT-мереж. Огляд загроз та вразливостей. Атаки, методи моніторингу та виявлення загроз у IoT-мережах. Стандарти та регулювання в області безпеки IoT. GDPR та інші регуляторні вимоги щодо захисту особистих даних в IoT-мережах.
17	*Лекція 17.* Протоколи безпеки IoT. Огляд протоколів безпеки (MQTT, CoAP, DTLS, OAuth). Методи інтеграції та використання протоколів безпеки в IoT-сценаріях. Криптографічні методи та інструменти для безпеки IoT. Генерація ключів, управління ключами та аутентифікація. Дослідження архітектурних рішень IoT.
Тема 9. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем	
18	*Лекція 18.* Процес аналізу інцидентів безпеки. Аналіз типових загроз та інцидентів безпеки. Виявлення, відновлення та реагування на інциденти. Поняття аудиту безпеки та його роль. Аналіз стандартів та методологій аудиту безпеки (ISO 27001 та NIST SP 800-53).

Лабораторні заняття

№ з/п	Назва	Кількість год.
1	Дослідження та виявлення атак соціальної інженерії, мережевих атак та особливостей аудиту безпеки	4
2	Дослідження особливостей налаштування автентифікації на маршрутизаторах Cisco	2
3	Дослідження особливостей налаштування сценаріїв ACL	2
4	Дослідження особливостей налаштування системи запобігання вторгненням (IPS)	2
	Модульна контрольна робота	1
5	Дослідження особливостей налаштування безпеки VLAN	4
6	Дослідження особливостей налаштування IPSec VPN	3
	Всього	**18**

6. Самостійна робота студента

Тема 2. Правові аспекти безпеки інформаційних систем
Стандарти ISO/IEC з кібербезпеки (ISO/IEC 27001 та ISO/IEC 27002).
Основні принципи Будапештської Конвенції про кіберзлочинність (Budapest Convention).
Декларація з міжнародної кібербезпеки (The Paris Call for Trust and Security in Cyberspace).
Стандарти NIST (National Institute of Standards and Technology).
Особливості Міжнародної телекомунікаційної співдружності (ITU-T) для сфери кібербезпеки.
Тема 4. Основи мережевої безпеки та протоколи безпеки
Моделі управління мережевими ресурсами.
Виявлення мережевих атак шляхом аналізу трафіка.
Команди налаштування протоколів STP, RSTP, MSTP.
Налаштування QoS. Пріоритезація трафіка.
Команди управління таблицями MAC, IP, ARP.
Тема 5. Захист від вторгнень

Команди налаштування асиметричних VLAN і сегментації трафіку.
Методика створення списків управління доступом (ACL).
Списки керування доступом (Access Control List).
Тема 7. Безпека мобільних пристроїв та хмарних обчислень
Особливості реалізації статичних і динамічних VLAN.
Обмеження адміністративного доступу до керування комутатором.
Налаштування та дослідження засобів протидії атакам MAC-flooding та MAC-Spoofing у мережі на базі комутаторів Cisco.
Принципи та методи надання доступу до інформаційних ресурсів.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- Відвідування лекцій, а також відсутність на них, не оцінюється. Відвідування лабораторних занять є обов'язковою складовою вивчення матеріалу;
- При захисті лабораторних робіт студент має продемонструвати виконані завдання. У випадку дистанційної форми навчання захист відбувається на відповідній конференції шляхом демонстрації екрана;
- Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code;
- Норми етичної поведінки Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

1) Рейтинг студента з кредитного модуля складається з балів, що він отримує за:
– виконання та захисту 6 лабораторних робіт;
– виконання 1 модульної контрольної роботи;
– відповідь на екзамені.

Максимальна кількість балів за всі завдання, виконані в семестрі, дорівнює:

8 балів х 6 (лабораторні роботи) +7балів (МКР) = 55 балів.

Максимальна кількість балів за кредитний модуль дорівнює:

55 балів (завдання, виконані в семестрі) + 45 балів (екзамен) = 100 балів.

2) Критерії нарахування балів за виконання лабораторних робіт

2.1. Ваговий бал за виконання завдань лабораторних робіт складає 8 балів. Мінімальна кількість для зарахування лабораторної роботи складає 4 бали.

2.2. Максимальна кількість балів за модульну контрольну роботу дорівнює 7 балів. На модульну контрольну роботу виноситься два теоретичних питання.

Модульна контрольна робота оцінюється наступним чином:

1. Коректність та повнота відповіді на 2 теоретичні питання - 6 балів(по 3 бали за кожне теоретичне питання);

2. Надання прикладу з теоретичного питання – 1 бал.

Наявність позитивних оцінок захисту всіх лабораторних робіт, а також відповідей модульної контрольної роботи, є умовою допуску до екзамену. Максимальна кількість балів, отриманих в семестрі, дорівнює 55. Мінімальна кількість набраних балів – 33 (60%).

2.3. На екзамені студенти виконують письмову контрольну роботу. Екзаменаційний білет складається з двох теоретичних питань та одного практичного завдання. Ваговий бал кожного питання – 15.

Максимальна кількість балів за складання екзамену дорівнює 15 балів х 3 = 45 балів.

Теоретична частина оцінюється наступним чином:

- «відмінно» , правильна чітко викладена, повна відповідь – (не менше 90% потрібної інформації) – 14-15 балів;
- «добре», достатньо повна відповідь (не менше 75% потрібної інформації) – 11-13 балів;
- «задовільно», неповна відповідь (не менше 60% потрібної інформації) – 9-10 балів;
- «незадовільно», незадовільна відповідь – 0 балів.

Практичне завдання оцінюється наступним чином:
- «відмінно», повне, безпомилкове розв'язування завдання – 14-15 балів;
- «добре», повне, розв'язування завдання із несуттєвими неточностями – 11-13 балів;
- «задовільно», завдання виконане з певними недоліками – 9-10 балів;
- «незадовільно», завдання не виконано.

Студент, який у семестрі отримав менш ніж 33 бали, не отримує допуск на екзамен.

Сума стартових балів, отриманих студентом протягом семестру, і балів, отриманих на екзамені, визначає оцінку згідно з таблицею:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9.Додаткова інформація з дисципліни (освітнього компонента)

Тема 4 та Тема 5 можуть бути зараховані за наявності сертифікату з оволодіння основ інформаційної безпеки, наприклад, сертифікат курсу «Introduction to Cybersecurity» представленого Cisco Networking Academy.

Тема 7 та Тема 8 можуть бути зараховані за наявності сертифікату з оволодіння основ інформаційної безпеки IoT, наприклад, сертифікат курсу «IoT Fundamentals: IoT Security» представленого Cisco Networking Academy.

.

Перелік питань, які виносяться на екзамен:

1. Види загроз і ризиків для інформаційних систем;
2. Основні принципи інформаційної безпеки;
3. Виклики в області інформаційної безпеки;
4. Поняття «Кіберпростір» та «кібероборотьба»;
5. Міжнародні організації та консорціуми, що здійснюють регулювання в сфері інформаційної безпеки;
6. Головні проблеми забезпечення кібернетичної безпеки;
7. Правові аспекти безпеки інформаційних систем;
8. Міжнародні закони, положення і стандарти, що регулюють сферу кібербезпеки;
9. Міжнародна співпраця в сфері кібербезпеки;
10. Українське законодавство в сфері регулювання питань інформаційної та кібернетичної безпеки;
11. Закон України «Про кібербезпеку»;
12. Закон України «Про інформацію»;
13. Закон України «Про захист інформації в інформаційних системах»;
14. Закон України «Про інформаційні ресурси інформаційного суспільства»;
15. Стратегії захисту інформації;
16. Значення та компоненти стратегії захисту інформації;
17. Механізми безпеки комп'ютерних мереж;
18. Основи мережевої безпеки та протоколи безпеки;
19. Виявлення та захист від мережевих загроз;
20. Загальні принципи побудови та організації комп'ютерних мереж;

21. Особливості функціонування комп’ютерних мереж;
22. Модель OSI;
23. Безпека на рівнях моделі OSI;
24. Основні характеристики та принципи протоколів безпеки на рівнях моделі OSI;
25. Активне та пасивне мережеве устаткування;
26. Міжмережевий екран як комплекс апаратних/програмних засобів захисту об’єктів критичної інфраструктури;
27. Дослідження алгоритмів маршрутизації (RIP, OSPF, IGRP/EIGRP, BGP);
28. Поняття вторгнень у системи та їх види;
29. Системи виявлення та запобігання вторгнень (IDS/IPS);
30. Програмно-апаратні комплекси для виявлення та запобігання вторгнень;
31. Пом’якшення наслідків вторгнень;
32. Поняття «сигнатури»;
33. Основи криптографічного захисту;
34. Принципи криптографії та її роль у безпеці інформаційних систем;
35. Типи шифрування та криптографічні алгоритми;
36. Використання криптографії для захисту даних;
37. Безпека мобільних пристроїв та хмарних обчислень;
38. Шифрування та захист даних на мобільних пристроях;
39. Захист від загроз IoT-мереж та протоколів;
40. BYOD;
41. Безпека хмарних обчислень;
42. Основи хмарних обчислень та їх безпека;
43. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем;
44. Виявлення, відновлення та реагування на інциденти;
45. Поняття аудиту безпеки та його роль;
46. Методи проведення аудиту безпеки інформаційних систем.

Робочу програму навчальної дисципліни (силабус):

Складено доц. кафедри ЦТЕ к.т.н., доц.Довженко Надією Михайлівною

Ухвалено кафедрою ЦТЕ (протокол № 20 від 10.05.2023р)

Погоджено Методичною комісією НН ІАТЕ КПІ ім. Ігоря Сікорського (протокол № 9 від 26.05.2023 р.)