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	*2 курс, весняний семестр*
Обсяг дисципліни	*4/120 год 18лек 36лаб 66СРС*
Семестровий контроль/ контрольні заходи	*Залік/МКР*
Розклад занять	*Науково-педагогічний працівник*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com, тел.063-863-97-30* Лабораторні заняття : *к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com, тел.063-863-97-30*
Розміщення курсу	*Кампус*

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 ОНП.

ЗК 1	Здатність до абстрактного мислення, аналізу та синтезу
ЗК 2	Здатність застосовувати знання у практичних ситуаціях
ЗК 10	Здатність бути критичним і самокритичним
ЗК 13	Здатність діяти на основі етичних міркувань
ЗК 14	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
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:

ПР1	Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.
ПР 16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.
ПР 24	Розуміти і реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності вільного демократичного суспільства, верховенства права, прав і свобод людини і громадянина в Україні, дотримуватися академічної доброчесності.

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», «Технологія розробки програмного забезпечення».

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. Безпека на рівнях моделі OSI;
Тема 6. Захист від вторгнень;
Тема 7. Основи криптографічного захисту;
Тема 8. Безпека мобільних пристроїв та хмарних обчислень;
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. Бурячок В. Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ. ДУТ. 2015. 449 с.
3. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі. Частина 1. Навчальний посібник. Київ. КПІ ім. Ігоря Сікорського. 2020. 328 с.
4. 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.
5. 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.
6. 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	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 «Кібероборотьба». Головні проблеми забезпечення кібернетичної безпеки.
Тема 2. Правові аспекти безпеки інформаційних систем	
2	Міжнародні закони, положення і стандарти, що регулюють сферу кібербезпеки. Міжнародна співпраця в сфері кібербезпеки. 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	
3	Значення 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	
4	Виявлення та захист від мережевих загроз. Загальні принципи побудови та організації комп’ютерних мереж. Особливості функціонування комп’ютерних мереж. Дослідження складових елементів. Продукти компанії Cisco для мережевої безпеки.
Тема 5. Безпека на рівнях моделі OSI	
5	Забезпечення безпеки на рівнях моделі OSI. Основні характеристики та принципи протоколів безпеки на рівнях моделі OSI. Дослідження алгоритмів маршрутизації (RIP, OSPF, IGRP/EIGRP, BGP).
Тема 6. Захист від вторгнень	
6	Поняття вторгнень у системи та їх види. Системи виявлення та запобігання вторгнень (IDS/IPS). Програмно-апаратні комплекси для виявлення та запобігання вторгнень. Пом’якшення наслідків. Поняття «сигнатури». Port mirroring.
Тема 7. Основи криптографічного захисту	
7	Принципи криптографії та її роль у безпеці інформаційних систем. Типи шифрування та криптографічні алгоритми. Використання криптографії для захисту даних.
Тема 8. Безпека мобільних пристроїв та хмарних обчислень	
8	Загрози безпеці мобільних пристроїв та методи їх запобігання. Шифрування та захист даних на мобільних пристроях. Захист від загроз IoT-мереж та протоколів. BYOD. Безпека хмарних обчислень. Основи хмарних обчислень та їх безпека.
Тема 9. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем	
9	Процес аналізу інцидентів безпеки. Виявлення, відновлення та реагування на інциденти. Поняття аудиту безпеки та його роль. Методи проведення аудиту безпеки інформаційних систем.

Лабораторні заняття

№ з/п	Назва	Кількість ауд. годин
1	Дослідження та виявлення атак соціальної інженерії та дослідження мережевих атак та особливостей аудиту безпеки	6

2	Налаштування автентифікації AAA на маршрутизаторах Cisco в середовищі Cisco Packet Tracer	4
3	Налаштування розширених сценаріїв ACL в середовищі Cisco Packet Tracer	4
4	Налаштування функціонування системи запобігання вторгненням IOS (IPS) за допомогою CLI в середовищі Cisco Packet Tracer	6
5	Налаштування безпеки VLAN для рівня 2 в середовищі Cisco Packet Tracer	4
6	Налаштування IPSec VPN в середовищі Cisco Packet Tracer	6
7	Налаштування основних параметрів безпеки для брандмауера ASA в середовищі Cisco Packet Tracer	6
	Всього	**36**

6. Самостійна робота студента

№ з/п	Назва теми, що виноситься на самостійне опрацювання	Кількість годин СРС
1	Стандарти ISO/IEC з кібербезпеки (ISO/IEC 27001 та ISO/IEC 27002).	2
2	Основні принципи Будапештської Конвенції про кіберзлочинність (Budapest Convention).	3
3	Декларація з міжнародної кібербезпеки (The Paris Call for Trust and Security in Cyberspace).	3
4	Стандарти NIST (National Institute of Standards and Technology).	4
5	Особливості Міжнародної телекомунікаційної співдружності (ITU-T) для сфери кібербезпеки.	2
6	Моделі управління мережевими ресурсами.	4
7	Виявлення мережевих атак шляхом аналізу трафіка.	6
8	Команди налаштування протоколів STP, RSTP, MSTP.	2
9	Налаштування QoS. Пріоритезація трафіка.	4
10	Команди управління таблицями MAC, IP, ARP.	3
11	Команди налаштування асиметричних VLAN і сегментації трафіку.	2
12	Методика створення списків управління доступом (ACL).	5
13	Списки керування доступом (Access Control List).	4
14	Особливості реалізації статичних і динамічних VLAN.	5
15	Обмеження адміністративного доступу до керування комутатором.	5
16	Налаштування та дослідження засобів протидії атакам MAC-flooding та MAC-Spoofing у мережі на базі комутаторів Cisco.	6
17	Принципи та методи надання доступу до інформаційних ресурсів.	6
	Всього	**66**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Для успішного проходження курсу та складання контрольних заходів необхідним є вивчення навчального матеріалу за кожною виокремленою темою. Специфіка курсу передбачає вивчення інструментів, основних концепцій та механізмів інформаційної безпеки систем та мереж. Особлива увага приділяється особливостям побудови захищених систем та мереж, моделям та програмно-апаратним комплексам протидії внутрішнім та зовнішнім загрозам безпеці інформаційних систем та мереж. Кожен студент повинен ознайомитися і слідувати Положенню про академічну доброчесність, Статуту і розпорядку дня університету.

Для успішного засвоєння програмного матеріалу студент зобов’язаний:

– не запізнюватися на заняття;

– не пропускати заняття (в разі пропуску самостійно опрацювати матеріал пропущеного заняття та скласти відповідні контрольні заходи в індивідуальному порядку);

– брати активну участь у освітньому процесі;

– конструктивно підтримувати зворотній зв’язок на всіх заняттях;

– своєчасно і старанно виконувати завдання для самостійної роботи;

– бути доброзичливим до однокурсників та викладачів;

– за об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету);

– будь-яке копіювання або відтворення результатів чужої праці (у тому числі списування), якщо тільки робота не має груповий формат, використання чужих завантажених з мережі Інтернет матеріалів кваліфікується як порушення норм і правил академічної доброчесності та передбачає притягнення винного до відповідальності, у порядку, визначеному чинним законодавством та Положенням про академічну доброчесність університету. Результатом невиконання та/або недотримання правил може бути оцінка «не зараховано» за курс.

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

Максимальна кількість балів з кредитного модуля дорівнює 100.

Рейтинг студента з кредитного модуля складається з балів, отриманих за:

1) виконання та захист лабораторних робіт;

2) написання модульної контрольної роботи.

1.Виконання лабораторнбих робіт

Оцінюються 7 лабораторних робіт, передбачені програмою. Максимальний ваговий бал – 7*10 = 70 балів. Рейтингові бали кожної роботи складаються з балів за правильність виконання (від 0 до 5) та захист роботи (від 0 до 3), балів за оформлення протоколу роботи (від 0 до 2). За несвоєчасну здачу звіту з лабораторної роботи – штраф 5 балів.

3. Модульний контроль

Максимальний ваговий бал – 30.

Сума вагових балів контрольних заходів протягом семестру складає: R=70+30=100 балів

Необхідною умовою допуску до заліку є зарахування модульної контрольної роботи, а також стартовий рейтинг (rc) не менше 40% від **R**, тобто 40 балів.

Студенти, які набрали протягом семестру рейтинг з кредитного модуля менше 0,6R, зобов'язані виконувати залікову контрольну роботу.

Студенти, які набрали протягом семестру необхідну кількість балів (*RD≥0,6R*), мають можливості:

- отримати залікову оцінку (залік) так званим «автоматом» відповідно до набраного рейтингу (таблиця);

- виконувати залікову контрольну роботу з метою підвищення оцінки (у разі отримання оцінки, більшої ніж «автомат» з рейтингу, студент отримує оцінку за результатами залікової роботи).

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Бали	Оцінка
95 - 100	Відмінно
85 - 94	Дуже добре
75 - 84	Добре
65 - 74	Задовільно
60 - 64	Достатньо
Менше 60	Незадовільно
R < 40: незараховані лабораторні роботи або не виконані інші умови допуску	Не допущено

9.Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль:

1. Види загроз і ризиків для інформаційних систем;
2. Основні принципи інформаційної безпеки;
3. Виклики в області інформаційної безпеки;
4. Поняття «Кіберпростір» та «кіберборотьба»;

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) «Безпека інформаціних систем»:
Складено доц,кафедри ЦТЕ к.т.н., 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.)