СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНА БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖЕВИХ СИСТЕМ ID 470

Шифр, назва спеціальності та освітній рівень	174 Автоматизація, комп’ютерно-інтегровані технології та робототехніка (магістр)	Назва освітньої програми	Автоматизація та комп’ютерно-інтегровані технології (2023)
Тип програми	Освітньо-професійна	Мова викладання	Українська
Факультет	Факультет прикладних інформаційних технологій та електроінженерії (ФПТ)	Кафедра	Каф. комп'ютерно-інтегрованих технологій (КТ)

Викладач/викладачі

Микитишин Андрій Григорович, канд. техн. наук, доцент, завідувач кафедри, профіль на порталі "Науковці ТНТУ"

Загальна інформація про дисципліну

Мета курсу	Метою вивчення дисципліни «Комплексна безпека інформаційних мережевих систем» є надання студентам основних теоретичних положень щодо побудови та функціонування захищених комп'ютерних мереж, а також практичне ознайомлення із найпоширенішими технологіями та обладнанням комп'ютерних мереж, здатних підтримувати високі рівні безпеки розподілених автоматизованих систем.
Формат курсу	Змішаний курс (для очної, заочної та дистаційної форм навчання).
Компетентності ОП	Інтегральна компетентність. Здатність розв'язувати складні задачі і проблеми автоматизації та комп'ютерно-інтегрованих технологій у професійній діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або провадження інноваційної діяльності та характеризується комплексністю та невизначеністю умов і вимог. Загальні компетентності: • ЗК1 – здатність проведення досліджень на відповідному рівні; • ЗК2 – здатність генерувати нові ідеї (креативність); Спеціальні (фахові) компетентності: • СК1 – здатність здійснювати автоматизацію складних технологічних об'єктів та комплексів, створювати кіберфізичні системи на основі інтелектуальних методів управління та цифрових технологій з використанням баз даних, баз знань, методів штучного інтелекту, робототехнічних та інтелектуальних мехатронних пристроїв; • СК2 – здатність проектувати та впроваджувати високонадійні системи автоматизації та їх прикладне програмне забезпечення, для реалізації функцій управління та опрацювання інформації, здійснювати захист прав інтелектуальної власності на нові проектні та інженерні рішення; • СК7 – здатність застосовувати спеціалізоване програмне забезпечення та цифрові технології для розв'язання складних задач і проблем автоматизації та комп'ютерно-інтегрованих технологій; • СК8 – здатність розробляти функціональну, технічну та інформаційну структуру комп'ютерно-інтегрованих систем управління організаційно-технологічними комплексами із застосуванням мережевих та інформаційних технологій, програмно-технічних керуючих комплексів, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв та засобів людино-машинного інтерфейсу. • СК9 – здатність розробляти захищені мережі для організації комунікації між компонентами автоматизованих систем управління виробництвом.
	• РН01 – створювати системи автоматизації, кіберфізичні виробництва на основі використання інтелектуальних методів управління, баз даних та баз знань, цифрових та мережевих технологій, робототехнічних та інтелектуальних мехатронних пристроїв; • РН02 – створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки

Програмні результати навчання з ОП	програмних та технічних засобів; • РН09 – розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційно- технічними об’єктами, розробляти програмно-технічні керуючі комплекси із застосовуванням мережевих та інформаційних технологій, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв, засобів людино-машинного інтерфейсу та з урахуванням технологічних умов та вимог до управління виробництвом. • РН13 – проєктувати та застосовувати комп’ютерні мережі з комплексним захистом інформації для забезпечення надійного функціонування автоматизованих систем.
Обсяг курсу	**Очна (денна) форма здобуття освіти:** Кількість кредитів ECTS — 4; лекції — 14 год.; лабораторні заняття — 28 год.; самостійна робота — 78 год.; **Заочна форма здобуття освіти:** Кількість кредитів ECTS — 4; лекції — 10 год.; лабораторні заняття — 12 год.; самостійна робота — 98 год.;
Ознаки курсу	Рік навчання — 1; семестр — 2; Обов’язкова (для здобувачів інших ОП може бути вибірковою) дисципліна; кількість модулів — 2;
Форма контролю	Поточний контроль: Підсумковий контроль: екзамен
Компетентності та дисципліни, що є передумовою для вивчення	Загальні та спеціальні компетентності передбачені освітнім стандартом першого (бакалаврського) рівня вищої освіти за спеціальністю "Автоматизація та комп'ютерно-інтегровані технології"
Матеріально-технічне та/або інформаційне забезпечення	Лабораторія вивчення та дослідження комп'ютерних мереж з необхідним мережевим обладнанням (комутаторами, маршрутизаторами, бездротовими точками доступу та іншим обладнанням). Програмний продукт Cisco Packet Tracer для моделювання та візуалізації налаштувань мережі.

СТРУКТУРА КУРСУ

Лекційний курс	Годин ОФЗО	Годин ЗФЗО
Лекція 1. Основні поняття, концепції і принципи мережевої безпеки. Базові поняття інформаційної безпеки. Моделі інформаційної безпеки. Принципи безпеки мереж. Суб'єкти загроз. Засоби суб'єкта загроз. Мережеві атаки. Розвідувальні атаки. Атаки доступу. Атаки соціальної інженерії. Атаки відмови в обслуговуванні Усунення типових мережевих атак. Найкращі практики мережевої безпеки. Протоколи керування мережею. Захист пристроїв. Ієрархія засобів захисту від інформаційних загроз.	2	2
Лекція 2. Технології автентифікації, авторизації та обліку (AAA). Огляд технологій AAA. Автентифікація людини. Автентифікація інформації. Технології управління доступом. Системи автентифікації і управління доступом ОС. Централізовані системи автентифікації та авторизації. Концепція єдиного логічного входу. Налаштування локальної автентифікації на пристроях Cisco. Налаштування серверної автентифікації, авторизації та обліку (AAA).	2	1
Лекція 3. Технології міжмережевого екрану. Використання списків контролю доступу (ACL). Організація списків контролю доступу для IPv4. Налаштування стандартних ACL для IPv4. Налаштування розширених ACL для IPv4. Використання списків ACL для запобігання мережевих загроз. Використання ACL для IPv6. Огляд технологій міжмережевого екрану. Використання зональних міжмережевих екранів (ZPF).	2	1
Лекція 4. Технології систем виявлення та запобігання вторгненням. Характеристики систем IDS та IPS. Реалізації систем IPS. Технологія SPAN. Сигнатури IPS. Сигнал тривоги сигнатур IPS. Тригери сигнатур. Виявлення загроз на основі аномалій. Управління і моніторинг IPS. Конфігурація Cisco IOS IPS за допомогою інтерфейсу командного рядка (CLI).	2	1
Лекція 5. Технології безпеки LAN. Забезпечення безпеки кінцевих пристроїв в мережі без меж. Захист від шкідливого ПЗ. Захист електронної пошти і веб-трафіку. Безпека в LAN на базі хмарних технологій. Управління доступом до мережі. Загрози безпеці Рівня 2. Впровадження захисту портів. Стримування атак на VLAN. Нейтралізація ARP-атак. Нейтралізація STP-атак. Загрози та вразливості IP. Вразливості TCP та UDP. Загрози та вразливості IP-сервісів.	2	1

Теми занять, короткий зміст

Лекція 6. Технології криптографії. Криптографічні сервіси. Криптографічні хеш-функції. Забезпечення цілісності за допомогою алгоритмів MD5, SHA-1 і SHA-2. Автентифікація за допомогою алгоритму HMAC. Управління ключами. Симетричне шифрування. Альтернативні алгоритми шифрування (SEAL, RC). Обмін ключами методом Діффі-Геллмана (DH). Асиметричне шифрування. Цифрові підписи та цифрові сертифікати. Інфраструктура відкритих ключів (PKI).	2	2
Лекція 7. Технології формування захищених каналів. Принципи побудови захищеного каналу. Протокол SSL. Протокол TLS. Технологія VPN. Мережі GRE через IPSec VPN. Технологія MPLS VPN третього рівня. Технології IPSec. Інкапсуляція в протоколі IPSec. Безпечний обмін ключами за протоколом Діффі-Геллмана. Протоколи IPSec AH та ESP. Бази даних SAD і SPD. Протокол IKE. Налаштування мережі IPSec VPN між двома сайтами. Налаштування криптокарти для політики IPSec.	2	2
РАЗОМ:	14	10

Лабораторний практикум (теми)	**Годин** ОФЗО	ЗФЗО
Лабораторна робота №1. Використання протоколів керування мережею (CDP, LLDP та NTP).	2	0,5
Лабораторна робота №2. Налаштування безпечних паролів і SSH.	2	0,5
Лабораторна робота №3. Налаштування протоколів автентифікації PAP і CHAP.	2	1
Лабораторна робота №4. Налаштування автентифікації AAA.	2	1
Лабораторна робота №5. Налаштування стандартних ACL для IPv4.	2	1
Лабораторна робота №6. Налаштування розширених списків контролю доступу (ACL).	2	1
Лабораторна робота №7. Налаштування списків ACL для IP-адрес з метою нейтралізації атак.	2	1
Лабораторна робота №8. Налаштування зонального міжмережевого екрану (ZPF).	2	1
Лабораторна робота №9. Налаштування системи запобігання вторгнень (IPS).	2	1
Лабораторна робота №10. Реалізація захисту портів комутатора.	2	0,5

Лабораторна робота №11. Налаштування безпеки Рівня 2 на комутаторі.		2	1
Лабораторна робота №12. Забезпечення безпеки VLAN на 2-му рівні.		2	1
Лабораторна робота №13. Дослідження DNS-трафіку.		2	0,5
Лабораторна робота №14. Налаштування та перевірка IPSec VPN між двома сайтами.		2	1
	РАЗОМ:	28	12

ІНШІ ВИДИ РОБІТ

Теми, короткий зміст	Самостійна робота. Опрацювання теоретичного матеріалу. Тема №1. Ієрархія засобів захисту від інформаційних з3агроз. Адміністративний рівень. Засоби безпеки процедурного рівня. Засоби безпеки технічного рівня. Тема №2. Дискреційний метод управління доступом. Мандатний метод управління доступом. Рольовий метод управління доступом. Концепція єдиного логічного входу. Тема №3. Синтаксис ACL-списку для IPv6. Налаштування ACL-списків IPv6. Дизайн зональних міжмережевих екранів (ZPF). Тема №4. Вибір рішення системи запобігання вторгненням (IPS). Глобальна кореляція IPS. Репутаційні фільтри, чорні списки і фільтри трафіку. Тема №5. Застосування технології вдосконаленого захисту від шкідливого ПЗ (AMP) для кінцевих пристроїв. Безпека в LAN на базі хмарних технологій. Тема №6. Шифр Вернама. Вибір алгоритму симетричного шифрування. Альтернативні алгоритми симетричного шифрування. Класи цифрових сертифікатів. Тема №7. Динамічні багатоточкові VPN. Інтерфейс віртуального тунелю IPSec. Технологія MPLS VPN третього рівня. Бази даних SAD і SPD.

Інформаційні джерела для вивчення курсу

1. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
2. Микитишин А.Г. Комп'ютерні мережі. Книга 1.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 256 с.
3. Микитишин А.Г. Комп'ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.
4. Микитишин А.Г. Телекомунікаційні системи та мережі / Микитишин А.Г., Митник М.М., Стухляк. П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
5. Методичні вказівки до лабораторних робіт з курсу «Комплексна безпека інформаційних мережевих систем». Модуль 1. Для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» /укл. А. Г. Микитишин // ТНТУ. – 2023. – 73 с.
6. Методичні вказівки до лабораторних робіт з курсу «Комплексна безпека інформаційних мережевих систем». Модуль 2. Для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» /укл. А. Г. Микитишин // ТНТУ. – 2023. – 44 с.

Політики курсу

Політика контролю	Використовуються такі засоби оцінювання та методи демонстрування результатів навчання: поточне опитування; тестування; виконання індивідуальних завдань та презентацій; оцінювання результатів виконаних самостійних робіт; бесіди та обговорення проблемних питань; дискусії; індивідуальні консультації; екзамен. Можливий ректорський контроль.
Політика щодо консультування	Консультації при вивченні дисципліни проводяться згідно затвердженого на кафедрі КТ. Консультування передбачено як очно ,так і з використанням ресурсів електронного навчального курсу у середовищі електронного навчання університету.
Політика щодо перескладання	Студент має право на повторне складання модульного контролю з метою підвищення рейтингу протягом тижня після складання модульного контролю за графіком. Перескладання екзамену відбувається в терміни, визначені графіком освітнього процесу. Здобувач ВО має право на зарахування результатів навчання здобутих у неформальній чи інформальній освіті.
Політика щодо академічної доброчесності	При складанні усіх видів контролю у середовищі електронного навчання завжди активується система розпізнавання особи, що складає контроль. Усі практичні роботи у ЕНК перевіряються вбудованою системою Антиплагіат. При складанні усіх форм контролю забороняється списування, у тому числі з використанням сучасних інформаційних технологій.
Політика щодо відвідування	Відвідування занять є обов’язковим компонентом освітнього процесу. За наявності поважних причин (наприклад, хвороба, особливі потреби, відрядження, сімейні обставини, участь у програмах академічної мобільності тощо) навчання може здійснюватися за індивідуальним графіком, погодженим з деканом факультету.

СИСТЕМА ОЦІНЮВАННЯ

Розподіл балів, які отримують студенти за курс

Модуль 1			Модуль 2			Підсумковий контроль		Разом з дисципліни
Аудиторна та самостійна робота			Аудиторна та самостійна робота			Теоретичний курс	Практичне завдання	100
Теоретичний курс (тестування)	Лабораторна робота		Теоретичний курс (тестування)	Лабораторна робота				
15	25		15	20		15	10	
№ лекції	Види робіт	К-ть балів	№ лекції	Види робіт	К-ть балів			
Лекція 1	Лабораторна робота №1	4	Лекція 4	Лабораторна робота №9	4			
Лекція 2	Лабораторна робота №2	2	Лекція 5	Лабораторна робота №10	3			
Лекція 3	Лабораторна робота №3	2	Лекція 6	Лабораторна робота №11	3			
	Лабораторна робота №4	4	Лекція 7	Лабораторна робота №12	3			
	Лабораторна робота №5	3		Лабораторна робота №13	3			
	Лабораторна робота №6	3		Лабораторна робота №14	4			
	Лабораторна робота №7	3						
	Лабораторна робота №8	4						

Розподіл оцінок		
Сума балів за навчальну діяльність	**Шкала ECTS**	**Оцінка за національною шкалою**
90-100	A	Відмінно
82-89	B	Добре
75-81	C	Добре
67-74	D	Задовільно
60-66	E	Задовільно
35-59	FX	Незадовільно з можливістю повторного складання
1-34	F	Незадовільно з обов’язковим повторним вивченням дисципліни

Затверджено рішенням кафедри КТ, протокол №1 від «22» серпня 2023 року.

ПОГОДЖЕНО

Гарант освітньої програми канд. техн. наук, завідувач кафедри АВ

Володимир САВКІВ