СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Марченко Віталій Вікторович, доктор філософії з кібербезпеки.</td><td>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: nadezhdadovzhenko@gmail.com; сторінка курсу в Moodle – http://dn.dut.edu.ua/course/view.php?id=452</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 «Інформаційні технології»</td><td>Рівень вищої освіти</td><td colspan="2">Доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">Кібербезпека</td><td>Семестр</td><td colspan="2">2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Доктор філософії кібербезпеки</td><td>Тип дисципліни</td><td colspan="2">Професійної та практичної підготовки</td></tr>
<tr><td rowspan="3">Обсяг:</td><td rowspan="2">Кредитів ECTS</td><td rowspan="2">Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td>3</td><td>90</td><td>18</td><td>-</td><td>18</td><td>-</td><td>54</td></tr>
<tr><td colspan="8">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="8">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="5">Методологія наукових досліджень у кібербезпеці</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="5"></td></tr>
<tr><td>Мета курсу:</td><td colspan="7">Формування знань та вмінь застосування основних положень щодо організації та реалізації захисту інформації телекомунікаційних систем та мереж, одержання практичних навичок створення безпечної мережевої інфраструктури, набуття навичок практичного застосування комплексного підходу щодо забезпечення інформаційної безпеки систем та мереж.</td></tr>
<tr><td colspan="8">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4"></td><td colspan="4">ФК-4. Професійна компетентність
ФК-5. Загальнонаукова компетентність
ФК-6. Політехнічна компетентність
ФК-7. Інженерна компетентність</td></tr>
<tr><td colspan="8">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="8">ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.
ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.
ПРН-23. Бути здатним генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки.
ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.
ПРН-30. Бути здатним до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних</td></tr>
</table>

систем, до обробки та перетворення інформації тощо.
ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. Технології організації та забезпечення інформаційної безпеки мереж			
Тема 1. Інформаційні технології організації безпеки мережевої інфраструктури. ***Знати***: основи інформаційної безпеки, роль безпеки мережевої інфраструктури, як складової інформаційної безпеки. ***Вміти:*** реалізувати захист інформації телекомунікаційних систем та мереж. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6 ***Програмні результати навчання:*** ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1-6	Лекція 1 2 год	5	Лекція-візуалізація
	Практичне заняття 1 2 год		**Виявлення мережевих атак шляхом аналізу трафіку** 1. Основи захоплення та аналізу мережевого трафіку 2. Виявлення мережевих атак шляхом аналізу трафіку
Тема 1. Тенденції розвитку і застосування методів і засобів захисту інформації в телекомунікаційних системах **Тема 2. Комунікаційні сигнали та кодування**	Самостійна робота	2	
Тема 2. Моделі управління мережевими ресурсами. ***Знати***: принципи створення надійної та безпечної мережевої інфраструктури ***Вміти***: застосовувати системний підхід для запобігання загроз безпеці мережевої інфраструктури. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6 ***Програмні результати навчання:*** ПРН-26, ПРН-27, ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1–6	Лекція 2 2 год	5	Лекція-візуалізація
	Практичне заняття 2 2 год		**Профіль безпеки стандарту ISO/OSI** 1. Профіль безпеки для заданих сервісів безпеки їх комбінацій і додатків. 2. Обґрунтувати запропонованого профілю.
Тема 2. Комунікаційні сигнали та кодування **Тема 3. Варіанти застосування функції контролю підключення вузлів до портів комутатора** **Тема 4. Модель робочої групи (модель розподіленого управління)**	Самостійна робота	2	
	Лекція 3 2 год		Лекція-візуалізація

Тема 3. Програмні та апаратні засоби захисту в інформаційних системах ***Знати***: основи застосування інформаційних технологій та систем безпеки мережевої інфраструктури. ***Вміти***: здійснювати аналіз та оцінку загроз безпеці мережевої інфраструктури. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-23, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1-6	Практичне заняття 3 2 год	5	**Списки керування доступом (Access Control List).** 1. Налаштування обмеження доступу користувачів в Інтернет по MAC-адресі. 2. Налаштування функції CPU Interface Filtering
Тема 4. Модель робочої групи (модель розподіленого управління) **Тема 5. Модель домена (модель централізованого управління)**	Самостійна робота	2	
Тема 4. Технології захисту інформації при міжмережевій взаємодії ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: знаходити основні шляхи щодо реалізації методів та заходів забезпечення безпеки мережевої інфраструктури ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-23, ПРН-26, ПРН-27, ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1–6	Лекція 4 2 год	5	Лекція-візуалізація
	Практичне заняття 4 2 год		**Команди протоколу IEEE 802.1X.** 1. Вивчення команд протоколу 802.1X 2. Настроювання аутентификации 802.1X на основі портів 3. Настроювання аутентификации 802.1X на основі MAC-Адрес
Тема 6. Профіль безпеки стандарту OSI/ISO 15408. **Тема 7. Захист повідомлень при передачі каналами та лініями зв'язку**	Самостійна робота	2	
Змістовий модуль 2. Організація та забезпечення інформаційної безпеки мереж			
Тема 5. Технології захисту у мережах на основі протоколів TCP/IP ***Знати***: класифікацію мережевих екранів та систем виявлення й запобігання проникнень ***Вміти***: уміти знаходити підходи щодо оцінки рівня безпеки мережевої інфраструктури ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-19, ПРН-20, ПРН-23, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1–6	Лекція 5 2 год	5	Лекція-візуалізація
	Практичне заняття 5 2 год		**Команди настроювання протоколів єднального дерева STP, RSTP, MSTP.** 1. Настроювання протоколу RSTP (IEEE 802.1w) 2. Настроювання протоколу MSTP (IEEE 802.1s) для кожної VLAN 3. Настроювання протоколу MSTP (IEEE 802.1s) для балансування навантаження

Тема 9. Інформаційні технології та принципи організації інформаційної безпеки **Тема 10. Логіко-аналітичні методи контролю безпеки програм** **Тема 11. Принципи побудови мережевих екранів**	Самостійна робота	2	
Тема 6. Тенденції розвитку і застосування методів і засобів захисту інформації в телекомунікаційних системах ***Знати***: комплексне забезпечення інформаційної безпеки систем та мереж ***Вміти***: розробляти рекомендацій та застосовувати заходи із забезпечення захисту інформаційних систем та мереж ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-20, ПРН-23, ПРН-26, ПРН-27, ПРН-30 ***Рекомендовані джерела:*** 1–6	Лекція 6 2 год	5	Лекція-візуалізація
	Практичне заняття 6 2 год		**Команди VLAN на основі портів і стандарту IEEE 802.1Q** 1. Налаштування VLAN на основі портів 2. Налаштування VLAN на основі стандарту IEEE 802.1Q 3. Оптимізація налаштування комутаторів з великою кількістю VLAN
Тема 12. Реалізація загроз інформації у мережах на основі протоколів TCP/IP **Тема 13. Мережеві екрани у мережах на основі протоколів TCP/IP** **Тема 14. Тенденції розвитку методів і засобів захисту інформації**	Самостійна робота	2	
Тема 7. Захист інформації в корпоративних мережах ***Знати***: принципи створення безпечної мережевої інфраструктури ***Вміти***: нормативно і метрологічно забезпечити сертифікацію й атестацію технічних засобів захисту і контролювати їх ефективність ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-23, ПРН-26, ПРН-27, ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1-6	Лекція 7 2 год	4	Лекція-візуалізація
	Практичне заняття 7 2 год		**Команди налаштування функції Q-in-Q (Double VLAN)** 1. Настроювання функції Port-based Q-in-Q 2. Настроювання функції Q-in-Q qinq ports all
Тема 15. Принципи забезпечення доступу до інформаційних ресурсів **Тема 16. Технології захисту у мережах на основі протоколів TCP/IP** **Тема 17. Канальний рівень. Механізми доступу до середовища**	Самостійна робота	2	
Тема 8. Принципи та методи надання доступу до інформаційних ресурсів	Лекція 8 2 год	4	Лекція-візуалізація

Знати: моделі управління мережевими ресурсами ***Вміти***: реалізувати захист інформації телекомунікаційних систем та мереж. ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-23, ПРН-26, ПРН-27, ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1-6	Практичне заняття 8 2 год		**Контроль над підключенням вузлів до портів комутатора. Функція IP-MAC-port** 1. Настроювання роботи функції IP-MAC-port Binding у режимі ARP 2. Настроювання роботи функції IP-MAC-port Binding у режимі ACL
Тема 18. Принципи побудови мереж VPN **Тема 19. Доступ до середовища та фреймірування**	Самостійна робота	2	
Тема 9. Системи виявлення вторгнень ***Знати***: програмні та апаратні засоби захисту в інформаційних системах ***Вміти***: здійснювати шифрування даних (повідомлень) з використанням класичних шифрів ***Формування компетенцій:*** ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-23, ПРН-26, ПРН-27, ПРН-30, ПРН-32 ***Рекомендовані джерела:*** 1–6	Лекція 9 2 год	4	Лекція-візуалізація
	Практичне заняття 9 2 год		**Настроювання QoS. Пріоритезація трафіка** 1. Настроювання пріоритету за замовчуванням на портах комутаторів 2. Механізм обслуговування черг пріоритетів Weighted Round Robin
Тема 20. Приклади протоколів і служб **Тема 21-22. Процес створення профілю доступу**	Самостійна робота	2	

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, Cisco Packet Tracer, GNS3, мережа Інтернет ауд. 419.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. NIST SPECIAL PUBLICATION 800-30r1 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
2. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М.В. Бем, І.М.Городиський, Г.Саттон, О.М.Родіоненко – К.: К.І.С., 2015. – 220 с.
3. Сучасні методи та моделі обробки даних в інформаційних системах: монографія / О. М. Беседовський, І. О. Золотарьова, С. П. Євсеєв та ін. ; за заг. ред. докт. екон. наук, професора Пономаренка В. С. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2013. – 540 с.
4. CCNP Data Center Application Centric Infrastructure 300-620 DCACI Official Cert Guide / Ammar Ahmadi - 1st Edition, Cisco Press, 2021. – 550 p.
5. Method for Determination of Cyber Threats Based on Machine Learning for Real-Time Information System / V. Tolubko, V. Vyshnivskyi, V. Mukhin, H. Haidur, N. Dovzhenko, O. Ilin, V. Vasylenko / I.J. Intelligent Systems and Applications. – 2018. – № 8. – P. 11-18. (Scopus)
6. Design and Simulation of a Secure and Scalable Enterprise Network / A. F.Agbetuyi, O.B.Akinpelumi, A.A.Adewale - Published at Accepted International Conference Paper: 9th International Workshop on Security and High Performance Computing Systems. Retrieved from http://m.covenantuniversity.edu.ng/Profiles/ Adewale-Adeyinka-Ajao/Design-and-Simulation-of-a-Secure- and-Scalable-Enterprise-Network. November 3rd, 2018.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо аспірант відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання аспірантом 60 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 1 бал
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10-15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Аспірант демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка	Відмінно / Зараховано (А)

	дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	вивчається.	
82-89	Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Аспірант засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Аспірант має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*