

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МЕТОДОЛОГІЯ НАУКОВИХ ДОСЛІДЖЕНЬ У КІБЕРБЕЗПЕЦІ»

Лектор курсу			Гайдур Галина Іванівна, доктор технічних наук, професор.		Контактна інформація лектора (e-mail), сторінка курсу в Moodle		e-mail: ikbdut@gmail.com; сторінка курсу в Moodle – http://dn.dut.edu.ua/course/view.php?id=448	
Галузь знань			12 «Інформаційні технології»		Рівень вищої освіти		Доктор філософії	
Спеціальність			Кібербезпека		Семестр		1,2	
Освітня програма			Доктор філософії кібербезпеки		Тип дисципліни		Здобуття глибинних знань зі спеціальності	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
	4	120	Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
			18	-	36	-	66	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Основи наукових досліджень та організація науки					
Освітні компоненти для яких є базовою			Вибіркові компоненти, кваліфікаційна робота					
Мета курсу:	Формування знань та вмінь застосування методів дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з створенням методів і засобів забезпечення кібербезпеки на основі сучасних математичних методів, інформаційних технологій							
Компетентності відповідно до освітньої програми								
Soft- skills / Загальні компетентності (ЗК)					Hard-skills / Спеціальні компетентності (СК)			
					ФК-3. Організаційно-комунікативна компетентність ФК-4. Професійна компетентність ФК-5. Загальнонаукова компетентність ФК-6. Політехнічна компетентність ФК-7. Інженерна компетентність			
Програмні результати навчання (ПРН)								
ПРН-14. Володіти навиками роботи із спеціалізованими системами криптозахисту та криптоаналізу, управляти змінами при роботі з існуючими системами криптографічного захисту.								
ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.								
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-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.								
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 систем, до обробки та перетворення інформації тощо.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Змістовий модуль 1. Методологія реалізації систем виявлення вторгнень			
Тема 1. <i>Класифікація атак та механізми їх реалізації в інформаційній системі</i> Знати: класифікацію, основні визначення та механізми реалізації атак в інформаційних системах. Вміти: застосовувати основні етапи збору інформації та механізми для реалізації атак. Формування компетенцій: ФК-3, ФК-4, ФК-5 Програмні результати навчання: ПРН-18, ПРН-19 Рекомендовані джерела: 1-5	Лекція 1 2 год	7*	Лекція-візуалізація
	Практичне заняття 1 4 год		Створення моделі атак на основі основних механізмів реалізації атаки: вивчення навколишнього середовища, ідентифікації топології мережі, ідентифікації вузлів, ідентифікації сервісів, сканування портів, визначення ролі вузла в інформаційній системі. Види реалізації атаки: проникнення, встановлення контролю, визначення мети атаки. Етапи завершення атаки.
Тема 2. <i>Теоретичні основи побудови системи виявлення вторгнень (СВВ)</i> Знати: основні компоненти багаторівневого захисту інформаційних систем, класифікувати СВВ за принципом реалізації. Вміти: застосовувати статистичні та динамічні СВВ. Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-30 Рекомендовані джерела: 1-5	Лекція 2 2 год	7*	Лекція-візуалізація
	Практичне заняття 2 4 год		Вивчення основних методів та засобів побудови СВВ, їх призначення, функції та місце в інформаційній системі.
Тема 1. <i>Класифікація атак та механізми їх реалізації в інформаційній системі</i> Тема 2. <i>Теоретичні основи побудови системи виявлення вторгнень</i>	Самостійна робота		1. Етапи реалізації атак. 2. Проблема визначення аномалій в інформаційних системах організацій.
Змістовий модуль 2. Методи аналізу виявлення аномалій мережевого трафіку			

<p>Тема 3. Технології функціонування систем виявлення атак Знати: технології виявлення аномальної активності, сигнатурні методи, виявлення аномалій на основі протоколів. Вміти: користуватись базами виявлення аномалій. Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 Рекомендовані джерела: 1-5</p>	<p>Лекція 3 2 год</p> <p>Практичне заняття 3 4 год</p>	<p>8*</p>	<p>Лекція-візуалізація</p> <p>Вивчення основних баз виявлення аномальних даних в інформаційній системі. Методи виявлення вторгнень Bro, OSSEC, STAT, Prelude, Snort, SnortNet, AAFID</p>
<p>Тема 4. Технології аналізу мережевого трафіка. Знати: Програми аналізу та моніторингу мережевого трафіку, програми-аналізatori мережевого трафіку, алгоритм проведення аналізу. Вміти: застосовувати програми аналізатори мережевого трафіку Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 Рекомендовані джерела: 1-5</p>	<p>Лекція 4 2 год</p> <p>Практичне заняття 4 4 год</p>	<p>8*</p>	<p>Лекція-візуалізація</p> <p>Установка, налаштування програм аналізаторів трафіка: система моніторингу Cacti, DUTrffic Bandwidth Monitor Pro, Wireshark</p>
<p>Тема 4. Технології аналізу мережевого трафіка Тема 3. Технології побудови систем виявлення атак</p>	<p>Самостійна робота</p>		<ol style="list-style-type: none"> 1. Концепції виявлення загроз. 2. Програми аналізу та моніторингу трафіка
Змістовий модуль 3. Методи виявлення аномалій в інформаційних системах			
<p>Тема 5. Методи виявлення аномальної поведінки процесів функціонування інформаційних систем. Знати: основні методи виявлення невідомих атак та вторгнень, формувати образ нормального функціонування інформаційної системи, оптимальний набір для параметрів оцінки, визначати показник аномальності. Вміти: визначати основні показники нормального функціонування</p>	<p>Лекція 5 2 год</p>	<p>8*</p>	<p>Лекція-візуалізація,</p>

<p>інформаційної системи. Проводити оцінку ефективності алгоритмів виявлення аномальної поведінки.</p> <p>Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7</p> <p>Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30</p> <p>Рекомендовані джерела: 1–5</p>	<p>Практичне заняття 5 4 год</p>		<p>Модель нормального функціонування ІС, визначення параметрів оцінки, показники аномальності</p>
<p>Тема 6. Виявлення аномальних викидів трафіку методами кратномасштабного аналізу</p> <p>Знати: знати основи теорії вейвлетов, неперервне та дискретне вейвлет перетворення</p> <p>Вміти: виконувати згортку, застосовувати швидке вейвлет перетворення.</p> <p>Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7</p> <p>Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30</p> <p>Рекомендовані джерела: 1–5</p>	<p>Лекція 6</p>	<p>8*</p>	<p>Лекція-візуалізація</p> <p>Моделювання вейвлет перетворювань</p>
<p>Тема 7. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу</p> <p>Знати: напрями використання методів фрактального аналізу</p> <p>Вміти: здійснювати виявлення DoS- і DdoS-атак</p> <p>Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7</p> <p>Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30</p> <p>Рекомендовані джерела: 1-5</p>	<p>Лекція 7 2 год</p>	<p>8*</p>	<p>Лекція-візуалізація</p>
<p>Тема 5. Методи виявлення аномальної поведінки процесів функціонування інформаційних систем.</p> <p>Тема 6. Виявлення аномальних викидів трафіку методами кратномасштабного аналізу</p> <p>Тема 7. Виявлення DoS- і DdoS-атак методами мультифрактального аналізу.</p>	<p>Практичне заняття 7 4 год</p>		<p>Проводити моделювання DoS- і DdoS-атак</p>
	<p>Самостійна робота</p>		<ol style="list-style-type: none"> 1. Міжнародний NIST 800-31 2. Дискретне вейвлет-пакетне перетворення. 3. Виявлення DoS- и DdoS-атак методами мультифрактального аналізу.
<p>Змістовий модуль 4. Методи забезпечення безпеки на базі штучного інтелекту</p>			

<p>Тема 8. Методологія побудови інтелектуальних систем захисту. Знати: системні принципи захисту інформації, функції безпеки, поняття функції інтелектуалізації захисту, структуру інтелектуальної машини, нейромережеві системи виявлення атак. Вміти: використовувати нейромережеві системи виявлення атак, алгоритми штучних імунних систем. Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 Рекомендовані джерела: 1-5</p>	<p>Лекція 8 2 год</p> <p>Практичне заняття 8 4 год</p>	<p>8*</p>	<p>Лекція-візуалізація</p> <p>Моделювання інтелектуальних систем захисту.</p>
<p>Тема 9. Штучний інтелект в системах захисту інформації Знати: роль та місце штучного інтелекту в системах захисту інформації, механізми функціонування. Вміти: застосовувати методи виявлення аномалій на основі механізмів штучного інтелекту. Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27, ПРН-30 Рекомендовані джерела: 1–5</p>	<p>Лекція 9 2 год</p> <p>Практичне заняття 9 4 год</p>	<p>8*</p>	<p>Лекція-візуалізація</p> <p>Когнітивне моделювання</p>
<p>Тема 9*. Сучасні системи криптографічного захисту даних. Елементи криптоаналізу шифрів. Знати: проблематику криптографії та сучасні криптографічні системи, принципи побудови шифрів та методи їх криптоаналізу. Вміти: оцінювати секретність криптоалгоритму та його стійкість, розробляти операційні блоки, застосовувати методи криптоаналізу для підтвердження стійкості шифрів. Формування компетенцій: ФК-4, ФК-5, ФК-6, ФК-7 Програмні результати навчання: ПРН-14, , ПРН-22, ПРН-23, ПРН-30 Рекомендовані джерела: 6</p>			
<p>Тема 8. Методологія побудови інтелектуальних систем захисту. Тема 9. Штучний інтелект в системах захисту інформації</p>	<p>Самостійна робота</p>		<p>1. Нейромережеві системи виявлення атак 2. Практичне застосування штучного інтелекту в системах виявлення аномалій</p>
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
<p>Комп'ютерне обладнання, мережа Інтернет ауд. 420.</p>			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			

1. NIST SPECIAL PUBLICATION 800-94 <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf>
2. Monowar H. Bhuyan Network Traffic Anomaly Detection and Prevention Concepts, Techniques, and Tools. / Monowar H. Bhuyan, Dhruva K. Bhattacharyya, Jugal K. Kalita Springer. 2017. 278p. ISBN 978-3-319-65188-0 (eBook)
3. N. N. R. Ranga Suri Athithan Outlier Detection: Techniques and Application./ N. N. R. Ranga Suri, Narasimha Murty M, G. - Springer Nature Switzerland. 2019. 227p.
4. Гайдур Г.І., Гахов С.О. Теоретичний підхід до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи. Телекомунікаційні та інформаційні технології. 2021. № 1 (70). С. 79-87.
5. Гахов С. О. Застосування положень імунології в теорії захищених інформаційних систем. Сучасний захист інформації. 2018. № 2. С. 59 – 64.

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 70 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	<i>Робота на заняттях, у т.ч.:</i>	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• 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.	Звільняється від екзамену
ПІДСУМКОВЕ ОЦІНЮВАННЯ екзамен	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /затис в екзаменаційній відомості
------	---------------------	-----------------------	--

90-100	<p>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.</p> <p>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.</p> <p>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 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.</p>	<p>Високий</p> <p>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 вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.</p>	Відмінно / Зараховано (А)
82-89	<p>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.</p> <p>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.</p>	<p>Достатній</p> <p>Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни</p>	Добре / Зараховано (В)
75-81	<p>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.</p>	<p>Достатній</p> <p>Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.</p>	Добре / Зараховано (С)
64-74	<p>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 розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.</p>	<p>Середній</p> <p>Забезпечує достатньо надійний рівень відтворення основних положень дисципліни</p>	Задовільно / Зараховано (D)
60-63	<p>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.</p>	<p>Середній</p> <p>Є мінімально допустимим у всіх складових навчальної програми з дисципліни</p>	Задовільно / Зараховано (E)

35-59	<p>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.</p>	<p>Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни</p>	<p>Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється</p>
1-34	<p>Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.</p>	<p>Незадовільний Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни</p>	<p>Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не представляється</p>