

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ПРОВЕДЕННЯ НАУКОВИХ ДОСЛІДЖЕНЬ В КІБЕРБЕЗПЕЦІ»

Лектор курсу		Гахов Сергій Олександрович, кандидат військових наук, доцент.		Контактна інформація лектора (e-mail), сторінка курсу в Moodle		e-mail: s.gakhov@duikt.edu.ua сторінка курсу https://classroom.google.com/c/NzI2Mzg4MTM3OTI4?cjc=cry7d6f	
Галузь знань		12 Інформаційні технології		Рівень вищої освіти		другий (магістерський) рівень	
Спеціальність		125 Кібербезпека та захист інформації		Семестр		2	
Освітня програма		Освітньо-професійна програма «Інформаційна та кібернетична безпека»		Тип дисципліни		Обов'язкова компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
	3	90	Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
			18	-	18	-	54
АНОТАЦІЯ КУРСУ							
Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню			Науково-технічний переклад, Прикладна загальна теорія систем інформаційної та кібербезпеки, Технології виявлення уразливостей мережевих ресурсів				
Освітні компоненти для яких є базовою			Науково-дослідна практика				
Мета курсу:	Формування знань та вмій фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.						
Компетентності відповідно до освітньої програми							
Soft- skills / Загальні компетентності (ЗК)				Hard-skills / Спеціальні компетентності (СК)			
К31. Здатність застосовувати знання у практичних ситуаціях. К32. Здатність проводити дослідження на відповідному рівні. К34. Здатність оцінювати та забезпечувати якість виконуваних робіт. К35. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності). К37. Володіння навичками критичного мислення. К38. Здатність використовувати інформаційні та комунікаційні технології. К39. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. К310. Здатність застосовувати кращі практики у професійній діяльності.				КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.			

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Програмні результати навчання (ПРН)

ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

PH23. Обґрунтувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
<p>Тема 1. Наука і наукове дослідження. Предмет дисципліни. Знати: поняття “наука”, поняття “наукове пізнання” та “знання”, компоненти наукового пізнання, поняття “наукова проблема” та її постановка, поняття “наукова теорія” та її структурні складники; поняття “наукове дослідження”, його основні ознаки та характеристики, форми наукових досліджень, класифікація наукових досліджень, етапи наукового дослідження; поняття “методологія”, принципи методології наукових досліджень, основні прийоми наукових узагальнень. Формування компетенцій: К32, К39, КФ3. Програмні результати навчання: PH3. Рекомендовані джерела: 1-3.</p>	Лекція 1 2 год		Лекція-візуалізація
<p>Тема 1. Інструменти проведення наукових досліджень в кібербезпеці. Знати: програмне забезпечення для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, а також його можливості; програмне забезпечення мови програмування Python 3.11.1; платформа Google Colab та програмне забезпечення Jupyter Notebook; бібліотека програм Scikit-learn; бібліотека програм Pandas; бібліотека програм NumPy; бібліотека програм Matplotlib; бібліотека програм Seaborn. Вміти: розгортати та застосовувати програмне забезпечення для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання. Формування компетенцій: К31, К32, К38, К39, К310, КФ3. Програмні результати навчання: PH3, PH17, PH19, PH20, PH23 Рекомендовані джерела: 1-3, 5, 8, 14-19.</p>	Практичне заняття 1 2 год	4	Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.
<p>Тема 1. Наука і наукове дослідження. Предмет дисципліни. Інструменти проведення наукових досліджень в кібербезпеці. Знати: поняття “наука”, поняття “наукове пізнання” та “знання”, компоненти наукового пізнання, поняття “наукова проблема” та її постановка, поняття “наукова теорія” та її структурні складники;</p>	Самостійна робота 1 6 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

<p>поняття “наукове дослідження”, його основні ознаки та характеристики, форми наукових досліджень, класифікація наукових досліджень, етапи наукового дослідження; поняття “методологія”, принципи методології наукових досліджень, основні прийоми наукових узагальнень; програмне забезпечення для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, а також його можливості; програмне забезпечення мови програмування Python 3.11.1; платформа Google Colab та програмне забезпечення Jupyter Notebook; бібліотека програм Scikit-learn; бібліотека програм Pandas; бібліотека програм NumPy; бібліотека програм Matplotlib; бібліотека програм Seaborn.</p> <p>Вміти: розгортати та застосовувати програмне забезпечення для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання.</p> <p>Формування компетенцій: К31, К38, К39, К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 1-3, 5, 8, 14-19.</p>			
<p>Тема 2 Науковий метод. Методи наукових досліджень та їх характеристика.</p> <p>Знати: поняття “науковий метод”, класифікація методів наукових досліджень залежно від сфери застосування та рівня узагальнення, методи теоретичного рівня пізнання, методи метатеоретичного рівня пізнання, послідовність застосування методів дослідження; методи емпіричних наукових досліджень та їх види, універсальні методи наукових досліджень, специфічні методи наукових досліджень, поняття “експеримент”.</p> <p>Формування компетенцій: К32, К39, КФ3.</p> <p>Програмні результати навчання: РН3.</p> <p>Рекомендовані джерела: 1-3</p>	<p>Лекція 2 2 год</p>		<p>Лекція-візуалізація</p>
<p>Тема 2. Набори даних Канадського інституту кібербезпеки для наукових досліджень.</p> <p>Знати: моделі інформаційних систем для отримання наборів даних для досліджень; моделі імітування кібератак на інформаційні системи, методи збирання даних щодо кібератак; зміст наборів даних.</p> <p>Вміти: застосовувати набори даних для проведення наукових досліджень в галузі кібербезпеки.</p> <p>Формування компетенцій: К31, К32, К38, К39, К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 5, 6, 20.</p>	<p>Практичне заняття 2 2 год</p>	<p>4</p>	<p>Ознайомлення з інформаційними ресурсами Канадського інституту кібербезпеки для наукових досліджень.</p>

<p>Тема 2. Науковий метод. Методи наукових досліджень та їх характеристика. Набори даних Канадського інституту кібербезпеки для наукових досліджень.</p> <p>Знати: поняття “науковий метод”, класифікація методів наукових досліджень залежно від сфери застосування та рівня узагальнення, методи теоретичного рівня пізнання, методи метатеоретичного рівня пізнання, послідовність застосування методів дослідження; методи емпіричних наукових досліджень та їх види, універсальні методи наукових досліджень, специфічні методи наукових досліджень, поняття “експеримент”; моделі інформаційних систем для отримання наборів даних для досліджень, моделі імітування кібератак на інформаційні системи, методи збирання даних щодо кібератак, зміст наборів даних.</p> <p>Вміти: застосовувати методи наукових досліджень; застосовувати набори даних для проведення наукових досліджень в галузі кібербезпеки.</p> <p>Формування компетенцій: К31, К32, К38, К39, К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 1-3, 5, 6, 20.</p>	<p>Самостійна робота 2 6 год</p>	<p>2</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 3. Абстрагування та ідеалізація. Модель (в науке). Математична модель. Моделювання. Експеримент.</p> <p>Знати: поняття “абстрагування” та “ідеалізація”; поняття “модель (в науці)” та “математична модель”; поняття “моделювання” та його зміст; поняття “експеримент” та його зміст.</p> <p>Формування компетенцій: К32, К39, КФ3.</p> <p>Програмні результати навчання: РН3.</p> <p>Рекомендовані джерела: 1-3.</p>	<p>Лекція 3 2 год</p>		<p>Лекція-візуалізація</p>
<p>Тема 3. Дослідницький аналіз даних (Exploratory Data Analysis) в Python. Попередня обробка даних (Preprocessing data). Практичне застосування дослідницького аналізу даних та підготовка даних.</p> <p>Знати: поняття “дослідницький аналіз даних”, його мета та зміст, мета та зміст однофакторного аналізу даних, мета та зміст двофакторного аналізу даних, мета та зміст багатфакторного аналізу даних, мета та зміст кореляційного аналізу даних, інструменти в для дослідницького</p>	<p>Практичне заняття 3 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>

<p>аналізу та візуалізації аналітичних даних; мета та зміст попередньої обробки даних, методи та інструменти підготовки даних.</p> <p>Вміти: застосовувати інструменти для дослідницького аналізу даних та їх попередньої обробки.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 4, 14-20</p>			
<p>Тема 3. Абстрагування та ідеалізація. Модель (в науці). Математична модель. Моделювання. Експеримент. Дослідницький аналіз даних (Exploratory Data Analysis) в Python. Попередня обробка даних (Preprocessing data).</p> <p>Знати: поняття “абстрагування” та “ідеалізація”; поняття “модель (в науці)” та “математична модель”; поняття “моделювання” та його зміст; поняття “експеримент” та його зміст; поняття “дослідницький аналіз даних”, його мета та зміст, мета та зміст однофакторного аналізу даних, мета та зміст двофакторного аналізу даних, мета та зміст багатофакторного аналізу даних, мета та зміст кореляційного аналізу даних, інструменти в для дослідницького аналізу та візуалізації аналітичних даних; мета та зміст попередньої обробки даних, методи та інструменти підготовки даних.</p> <p>Вміти: створювати моделі та проводити експерименти; застосовувати інструменти для дослідницького аналізу даних та їх попередньої обробки.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 1-4, 14-20.</p>	<p>Самостійна робота 3 6 год</p>	<p>2</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 4. Машинне навчання в кібербезпеці. Практичні варіанти застосування методів машинного навчання для виявлення шкідливих процесів.</p> <p>Знати: поняття “машинне навчання” та його зміст; можливості застосування машинне навчання в кібербезпеці; практичні варіанти застосування методів машинного навчання для виявлення шкідливих процесів.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Лекція 4 2 год</p>		<p>Лекція-візуалізація</p>

<p>Тема 4. Машинне навчання в кібербезпеці. Практичне застосування методу зменшення розмірності: методу головних компонент (Principal component analysis).</p> <p>Знати: призначення методу головних компонент (Principal component analysis) та порядок його застосування для зменшення розмірності даних.</p> <p>Вміти: застосовувати метод головних компонент (Principal component analysis) для зменшення розмірності даних.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 14-20.</p>	<p>Практичне заняття 4 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>
<p>Тема 4. Машинне навчання в кібербезпеці. Практичні варіанти застосування методів машинного навчання для виявлення шкідливих процесів. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод зменшення розмірності: метод головних компонент (Principal component analysis).</p> <p>Знати: поняття “машинне навчання” та його зміст; можливості застосування машинне навчання в кібербезпеці; практичні варіанти застосування методів машинного навчання для виявлення шкідливих процесів; призначення методу головних компонент (Principal component analysis) та порядок його застосування для зменшення розмірності даних.</p> <p>Вміти: застосовувати метод головних компонент (Principal component analysis) для зменшення розмірності даних.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Самостійна робота 4 6 год</p>	<p>2</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 5. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод опорних векторів (Support Vector Machines). Метод зменшення розмірності: метод головних компонент (Principal component analysis).</p> <p>Знати: призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод опорних векторів (Support Vector Machines) та його математичне визначення; метод зменшення розмірності: метод головних компонент (Principal Component Analysis) та його математичне визначення.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p>	<p>Лекція 5 2 год</p>		<p>Лекція-візуалізація</p>

<p><u>Програмні результати навчання:</u> PH3, PH17, PH19, PH20, PH23. <u>Рекомендовані джерела:</u> 8, 9, 12-20.</p>			
<p>Тема 5. Машинне навчання в кібербезпеці. Практичне застосування методу опорних векторів (Support Vector Machines). <u>Знати:</u> призначення методу опорних векторів (Support Vector Machines) та порядок його застосування для розв'язання задач класифікації та регресії. <u>Вміти:</u> застосовувати метод опорних векторів (Support Vector Machines) для розв'язання задач класифікації та регресії. <u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3. <u>Програмні результати навчання:</u> PH3, PH17, PH19, PH20, PH23. <u>Рекомендовані джерела:</u> 14-20.</p>	<p>Практичне заняття 5 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>
<p>Тема 5. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод опорних векторів (Support Vector Machines). Метод зменшення розмірності: метод головних компонент (Principal component analysis). <u>Знати:</u> призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод опорних векторів (Support Vector Machines) та його математичне визначення; метод зменшення розмірності: метод головних компонент (Principal Component Analysis) та його математичне визначення. <u>Вміти:</u> застосовувати метод опорних векторів (Support Vector Machines) для розв'язання задач класифікації та регресії. <u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3. <u>Програмні результати навчання:</u> PH3, PH17, PH19, PH20, PH23. <u>Рекомендовані джерела:</u> 8, 9, 12-20.</p>	<p>Самостійна робота 5 6 год</p>	<p>2</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 6. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод найближчих сусідів (Nearest Neighbors). <u>Знати:</u> призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод найближчих сусідів (Nearest Neighbors) та його математичне визначення. <u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3. <u>Програмні результати навчання:</u> PH3, PH17, PH19, PH20, PH23. <u>Рекомендовані джерела:</u> 8, 9, 12-20.</p>	<p>Лекція 6 2 год</p>		<p>Лекція-візуалізація</p>

<p>Тема 6. Машинне навчання в кібербезпеці. Практичне застосування методу найближчих сусідів (Nearest Neighbors).</p> <p>Знати: призначення методу найближчих сусідів (Nearest Neighbors) та порядок його застосування для розв'язання задач класифікації та регресії.</p> <p>Вміти: застосовувати метод найближчих сусідів (Nearest Neighbors) для розв'язання задач класифікації та регресії.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 14-20.</p>	<p>Практичне заняття 6 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>
<p>Тема 6. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод найближчих сусідів (Nearest Neighbors).</p> <p>Знати: призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод найближчих сусідів (Nearest Neighbors) та його математичне визначення.</p> <p>Вміти: застосовувати метод найближчих сусідів (Nearest Neighbors) для розв'язання задач класифікації та регресії.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Самостійна робота 6 6 год</p>	<p>2</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 7. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод дерев рішень (Decision Trees).</p> <p>Знати: призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод дерев рішень (Decision Trees) та його математичне визначення.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p> <p>Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.</p> <p>Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Лекція 7 2 год</p>		<p>Лекція-візуалізація</p>
<p>Тема 7. Машинне навчання в кібербезпеці. Практичне застосування методу дерев рішень (Decision Trees).</p> <p>Знати: призначення методу дерев рішень (Decision Trees) та порядок його застосування для розв'язання задач класифікації та регресії.</p> <p>Вміти: застосовувати метод дерев рішень для розв'язання задач класифікації та регресії.</p> <p>Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.</p>	<p>Практичне заняття 7 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>

<p>Програмні результати навчання: PH3, PH17, PH19, PH20, PH23. Рекомендовані джерела: 14-20.</p>			
<p>Тема 7. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання з вчителем (Supervised learning). Метод дерев рішень (Decision Trees). Знати: призначення методів класифікації та їх можливості для застосування в рішеннях кібербезпеки; метод дерев рішень (Decision Trees) та його математичне визначення. Вміти: застосовувати метод дерев рішень для розв'язання задач класифікації та регресії. Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3. Програмні результати навчання: PH3, PH17, PH19, PH20, PH23. Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Самостійна робота 7 6 год</p>	<p>4</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>
<p>Тема 8. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання без вчителя (Unsupervised learning). Кластеризація (Clustering). Метод K-means. Знати: призначення методів кластеризації та їх можливості для застосування в рішеннях кібербезпеки; метод K-means та його математичне визначення. Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3. Програмні результати навчання: PH3, PH17, PH19, PH20, PH23. Рекомендовані джерела: 8, 9, 12-20.</p>	<p>Лекція 8 2 год</p>		<p>Лекція-візуалізація</p>
<p>Тема 8. Машинне навчання в кібербезпеці. Практичне застосування методу K-means. Знати: призначення методу K-means та порядок його застосування для розв'язання задач кластеризації. Вміти: застосовувати метод K-means та порядок його застосування для розв'язання задач кластеризації. Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3. Програмні результати навчання: PH3, PH17, PH19, PH20, PH23. Рекомендовані джерела: 14-20.</p>	<p>Практичне заняття 8 2 год</p>	<p>4</p>	<p>Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.</p>
<p>Тема 8. Машинне навчання в кібербезпеці. Математичні моделі машинного навчання без вчителя (Unsupervised learning). Кластеризація (Clustering). Метод K-means.</p>	<p>Самостійна робота 8 6 год</p>	<p>4</p>	<p>Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.</p>

<p><u>Знати:</u> призначення методів кластеризації та їх можливості для застосування в рішеннях кібербезпеки; метод K-means та його математичне визначення.</p> <p><u>Вміти:</u> застосовувати метод K-means та порядок його застосування для розв'язання задач кластеризації.</p> <p><u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3.</p> <p><u>Програмні результати навчання:</u> РН3, РН17, РН19, РН20, РН23.</p> <p><u>Рекомендовані джерела:</u> 8, 9, 12-20.</p>			
<p><i>Тема 9. Машинне навчання в кібербезпеці. Методи вибору та оцінки моделі машинного навчання (Model selection and evaluation).</i></p> <p><u>Знати:</u> призначення та порядок перехресної перевірки: оцінка ефективності оцінювача (cross-validation: evaluating estimator performance); метрики та порядок оцінювання: кількісна оцінка якості прогнозів (metrics and scoring: quantifying the quality of predictions); призначення кривих перевірки: побудова балів для оцінки моделей (validation curves: plotting scores to evaluate models).</p> <p><u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3.</p> <p><u>Програмні результати навчання:</u> РН3, РН17, РН19, РН20, РН23.</p> <p><u>Рекомендовані джерела:</u> 8, 9, 12-20.</p>	Лекція 9 2 год		Лекція-візуалізація
<p><i>Тема 9. Машинне навчання в кібербезпеці. Практичне застосування методів вибору та оцінки моделі машинного навчання (Model selection and evaluation).</i></p> <p><u>Знати:</u> призначення методів вибору та оцінки моделі машинного навчання.</p> <p><u>Вміти:</u> застосовувати методи вибору та оцінки моделі машинного навчання.</p> <p><u>Формування компетенцій:</u> К31, К32, К34, К35, К37-К310, КФ3.</p> <p><u>Програмні результати навчання:</u> РН3, РН17, РН19, РН20, РН23.</p> <p><u>Рекомендовані джерела:</u> 14-20.</p>	Практичне заняття 9 2 год	4	Ознайомлення з програмним забезпеченням для проведення наукових досліджень, зокрема на базі мови програмування Python та методів машинного навчання, та його практичне застосування.
<p><i>Тема 9. Машинне навчання в кібербезпеці. Методи вибору та оцінки моделі машинного навчання (Model selection and evaluation).</i></p> <p><u>Знати:</u> призначення та порядок перехресної перевірки: оцінка ефективності оцінювача (cross-validation: evaluating estimator performance); метрики та порядок оцінювання: кількісна оцінка якості прогнозів (metrics and scoring: quantifying the quality of predictions); призначення кривих перевірки: побудова балів для оцінки моделей (validation curves: plotting scores to evaluate models).</p>	Самостійна робота 9 6 год	4	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Вміти: застосовувати методи вибору та оцінки моделі машинного навчання.
Формування компетенцій: К31, К32, К34, К35, К37-К310, КФ3.
Програмні результати навчання: РН3, РН17, РН19, РН20, РН23.
Рекомендовані джерела: 8, 9, 12-20.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет, програмне забезпечення мови програмування Python 3.11.1, платформа Google Colab або програмне забезпечення Jupyter Notebook, бібліотека програм Scikit-learn, бібліотека програм Pandas, бібліотека програм NumPy, бібліотека програм Matplotlib, бібліотека програм Seaborn, Canadian Institute for Cybersecurity datasets.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Данильян О. Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с.
2. Методологія та організація наукових досліджень (галузі знань: 05 – соціальні та поведінкові науки, 07 – управління та адміністрування) [Текст] : навч. посіб. / Л. Г. Ліпич, С. М. Бортнік, І. Г. Волинець та ін. ; за заг. ред. Л. Г. Ліпич. – Луцьк : Вежа-Друк, 2018. – 220 с.
3. Бхаттачарджи А., Ситник Н. Методологія та організація наукових досліджень: дослідження в соціально-економічних науках. Навч. посіб. 2-ге вид., перероб. і доп. К.: НТУУ «КПІ ім. Ігоря Сікорського», 2022. 173 с.
4. Stefanie Molin. Hands-On Data Analysis with Pandas. Efficiently perform data collection, wrangling, analysis and visualization using Python. Packt Publishing, 2019. – 723 p.
5. Aurélien Géron. Hands-on Machine Learning with Scikit-Learn, Keras and TensorFlow. Concepts, Tools, and Techniques to Build Intelligent Systems. Second Edition. O'Reilly Media, 2019. – 510 p.
6. Michael Collins. Network Security Through Data Analysis. From Data to Action. Second Edition. O'Reilly Media, 2017. – 427 p.
7. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel. Machine Learning Approaches in Cyber Security Analytics. Springer Singapore. 2020. – 217 p.
<https://doi.org/10.1007/978-981-15-1706-8>.
8. Machine Learning for Computer and Cyber Security. Principles, Algorithms, and Practices. Editors Brij B. Gupta, Michael Shen. CRC Press, 2019. – 365 p.
9. Clarence Chio and David Freeman. Machine Learning and Security. Protecting Systems with Data and Algorithms. Published by O'Reilly Media, Inc., 2018. – 385 p.
10. Securing Machine Learning Algorithms. ENISA. December 14, 2021. <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.
11. Andreas C. Müller and Sarah Guido. Introduction to Machine Learning with Python. A Guide for Data Scientists. O'Reilly Media, 2017. – 392 p.
12. Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity. Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing, 2019. – 331 p.
13. Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel. Machine Learning Approaches in Cyber Security Analytics. Springer Nature Singapore Pte Ltd. 2020. – 217 p.
<https://doi.org/10.1007/978-981-15-1706-8>.
14. Ankur A. Patel. Hands-On Unsupervised Learning Using Python. O'Reilly Media, Inc., Released February 2019. – 430 p.
15. Python 3.11.1 documentation. <https://docs.python.org/3/>.
16. scikit-learn 1.2.0. User Guide. https://scikit-learn.org/stable/user_guide.html.
17. pandas. User Guide. https://pandas.pydata.org/docs/user_guide/index.html.
18. Matplotlib 3.6.3 documentation. <https://matplotlib.org/stable/index.html>.
19. seaborn. User guide and tutorial. <https://seaborn.pydata.org/tutorial.html>.
20. NumPy documentation. Version: 1.24. <https://numpy.org/doc/stable/>.
21. Canadian Institute for Cybersecurity datasets. <https://www.unb.ca/cic/datasets/index.html>.

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 студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
-

*** КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

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

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КИТРОЛЬ	<ul style="list-style-type: none"> • Виконання практичних робіт 	36 балів
	<ul style="list-style-type: none"> • Самостійна робота 	24 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10-15 балів за рішення викладача
ПІДСУМКОВЕ ОЦІНЮВАННЯ залік	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій або усній формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка / запис в заліковій відомості
90-100	Студент 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 стосуються дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента 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.	Відмінно / Зараховано (А)

	складних практичних завдань.		
82-89	Студент 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 студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (B)
75-81	Студент 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)
67-74	Студент 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.	Середній Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Студент 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, студент 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	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутня.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	Незадовільний Студент 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 представляється

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.

