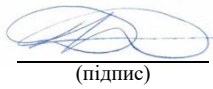
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)
(назва кафедри)

ЗАТВЕРДЖУЮ

Голова НМК



(підпис) Д.М. Крицький (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Великі дані для кібербезпеки
(назва навчальної дисципліни)

Галузь знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

Спеціальність:
(код та найменування спеціальності)

Освітні програми:
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Розробник: Фесенко Герман Вікторович, професор, д.т.н., професор _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » серпня 2023 року

Завідувач кафедри д.т.н., професор _____ В.С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="6">Галузь знань:
10 «Природничі науки», 11 «Математика та статистика»,
12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»</td><td>Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="2">Навчальний рік
2023/2024</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: немає</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 861)/150</td><td>1-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача – 5.4</td><td rowspan="10">Рівень вищої освіти:
другий (магістерський)</td><td>Лекції1)</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Практичні1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні1)</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить *64/86*.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета: надання знань і навичок зі створення, використання та аналізу індустріальних систем та Інтернету речей з урахуванням вимог до безпеки.

Завдання:

- придбання знань з основних принципів забезпечення кібербезпеки великих даних як послуги;
- придбання знань з основних принципів застосування технологій великих даних для забезпечення кібербезпеки безпеки систем різного призначення;
- отримання знань з використання архітектурних тактик для систем аналітики кібербезпеки на основі великих даних;
- отримання практичних знань з використання бібліотек високопродуктивної платформи розподілених обчислень Apache Spark для вирішення завдань аналітики кібербезпеки.

Компетентності, які набуваються: Здатність виявляти, ставити та вирішувати проблеми інженерного та дослідницького характеру під час забезпечення кібербезпеки рішень на основі великих даних і використання технологій великих даних для забезпечення кібербезпеки безпеки систем різного призначення.

Очікувані результати навчання. В результаті вивчення дисципліни здобувачі мають вміти застосовувати підходи, сервіси та інструментальні засоби для розв'язання складних задач забезпечення кібербезпеки рішень на основі великих даних і використання технологій великих даних для забезпечення кібербезпеки систем різного призначення.

Пререквізити: дисципліна є вибірковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки галузей знань 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво».

Кореквізіти: Відсутні.

3. Зміст навчальної дисципліни

Модуль 1

Змістовний модуль 1. Забезпечення кібербезпеки рішень на основі великих даних

Тема 1. Основи забезпечення безпеки та конфіденційності великих даних
Вплив безпеки і конфіденційності на характеристики великих даних. Таксономія аспектів безпеки та конфіденційності великих даних. Рівень безпеки та конфіденційності в еталонній архітектурі великих даних.

Тема 2. Безпека інфраструктури та платформи великих даних
Загрози та проблеми безпеки інфраструктури та платформи великих даних. Архітектура безпеки інфраструктури та платформи великих даних. Забезпечення безпеки інфраструктури та платформи великих даних на рівнях: джерел даних, обробки, застосунків, доступу. Особливості керування безпекою інфраструктури та платформи великих даних.

Тема 3. Забезпечення безпеки при керуванні життєвим циклом великих даних операторами телекомунікацій
Категорії даних. Життєвий цикл даних телекомунікаційних послуг на основі великих даних. Уразливості безпеки протягом життєвого циклу даних телекомунікаційних послуг на основі великих даних. Забезпечення послуг при керуванні життєвим циклом даних телекомунікаційних послуг на основі великих даних.

Тема 4. Забезпечення кібербезпеки фреймворка Hadoop
Вразливості фреймворка Hadoop, атаки та проблеми забезпечення безпеки. Використання протоколу безпеки Kerberos. Аутентифікація, авторизація, шифрування та адміністрування безпеки в Hadoop.

Змістовний модуль 2. Використання технологій великих даних для забезпечення кібербезпеки систем різного призначення

Тема 5. Системи аналітики кібербезпеки на основі великих даних
Основні характеристики та показники систем аналітики кібербезпеки на основі великих даних (BDCA-систем). Атрибути якості для BDCA-систем. Еталонна архітектура BDCA-системи.

Тема 6. Архітектурні тактики для систем аналітики кібербезпеки на основі великих даних
Архітектурні тактики, що відповідають атрибуту «Продуктивність». Архітектурні тактики, що відповідають атрибуту «Точність». Архітектурні тактики, що відповідають атрибуту «Масштабованість». Архітектурні тактики, що відповідають атрибуту «Надійність». Архітектурні тактики, що відповідають атрибуту «Безпека». Архітектурні тактики, що відповідають атрибуту «Зручність використання»

Тема 7. Забезпечення кібербезпеки систем з використанням аналітики великих даних
Вимоги до аналітики великих даних в контексті забезпечення кібербезпеки систем. Огляд існуючих рішень застосування аналітики великих даних для забезпечення кібербезпеки систем.

Тема 8. Забезпечення кібербезпеки систем з використанням Apache Spark
Особливості побудови системи виявлення вторгнень (IDS) на основі бібліотеки машинного навчання MLib Spark. Використання Spark для вирішення питань кібербезпеки на промисловому підприємстві.
.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Забезпечення кібербезпеки рішень на основі великих даних.					
Тема 1. Основи забезпечення безпеки та конфіденційності великих даних.	19	4		4	11
Тема 2. Безпека інфраструктури та платформи великих даних.	21	4		6	11
Тема 3. Забезпечення безпеки при керуванні життєвим циклом великих даних операторами телекомунікацій.	21	4		6	11
Тема 4. Забезпечення кібербезпеки фреймворка Hadoop.	18	4		3	11
Модульний контроль.	1			1	
Разом за змістовним модулем 1	80	16		20	44
Змістовний модуль 2. Використання технологій великих даних для забезпечення кібербезпеки систем різного призначення.					
Тема 5. Системи аналітики кібербезпеки на основі великих даних.	19	4		4	11

Тема 6. Архітектурні тактики для систем аналітики кібербезпеки на основі великих даних.	19	4		4	11
Тема 7. Забезпечення кібербезпеки систем з використанням аналітики великих даних.	18	4		3	11
Тема 8. Забезпечення кібербезпеки систем з використанням Apache Spark.	13	4			9
Модульний контроль.	1			1	
Разом за змістовним модулем 2	70	16		12	42
Усього годин	**150**	**32**		**32**	**86**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Програмування операцій зі стійкими розподіленими наборами даних (Resilient Distributed Datasets, RDD) з використанням Spark	4
2	Створення та робота з DataFrames з використанням Spark	6
3	Робота з графами з використанням Spark GraphX	6
4	Реалізація алгоритмів машинного навчання з використанням Spark MLlib і пакета spark.ml: статистичні обчислення і перевірка гіпотез	4
5	Реалізація алгоритмів машинного навчання з використанням Spark MLlib і пакета spark.ml: вилучення (TF-IDF, Word2Vec, CountVectorizer і CountVectorizerModel) і перетворення (Tokenizer, StopWordsRemover, n-gram, Binarizer, StringIndexer, IndexToString) ознак	4
6	Реалізація алгоритмів машинного навчання з використанням Spark MLlib і пакета spark.ml: перетворення (Interaction, MinMaxScaler, MaxAbsScaler, Bucketizer, ElementwiseProduct, SQLTransformer, VectorAssembler, Imputer) і вибір (VectorSlicer, MinHash) ознак	4
7	Реалізація алгоритмів машинного навчання з використанням Spark MLlib і пакета spark.ml: кластеризація і коллаборативна фільтрація	4
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Відпрацювання матеріалів лекційних занять за темою 1	11
2	Відпрацювання матеріалів лекційних занять за темою 2	11
3	Відпрацювання матеріалів лекційних занять за темою 3	11
4	Відпрацювання матеріалів лекційних занять за темою 4	11
5	Відпрацювання матеріалів лекційних занять за темою 5	11
6	Відпрацювання матеріалів лекційних занять за темою 6	11
7	Відпрацювання матеріалів лекційних занять за темою 7	11
8	Відпрацювання матеріалів лекційних занять за темою 8	9
	Разом	**86**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

10. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.14, 15).

11. Методи контролю

Проведення поточного контролю, електронного тестування, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних робіт	0...4	4	0...16
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних робіт	0...4	3	0...12
Модульний контроль	0…22	1	0…22
Усього за семестр			**0…100**

Білет для іспиту складається з двох теоретичних питань (30 балів за кожне питання) та практичного завдання (40 балів).

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять. Знати основи забезпечення безпеки та конфіденційності великих даних. Уміти оцінювати рівень забезпечення безпеки інфраструктури та платформи великих даних.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять. Знати ключові принципи використання технологій великих даних для забезпечення кібербезпеки систем різного призначення. Уміти застосовувати різні архітектурні тактики для систем аналітики кібербезпеки на основі великих даних.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти забезпечувати кібербезпеку систем з використанням аналітики великих даних. Вміти застосовувати алгоритми машинного навчання з використанням Spark MLlib для аналітики кібербезпеки.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор».

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=5964

14. Рекомендована література

Базова

1. Thuraisingham B., Masud M. M., Parveen P., Khan L. *Big Data Analytics with Applications in Insider Threat Detection*. USA, Boca Raton, FL : CRC Press, 2018. 579 p.
2. NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. [Ел. ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-4r2.pdf.

Допоміжна

1. Choo K.-K. R., Dehghantanha A. *Handbook of Big Data Privacy*. Switzerland, Cham : Springer Nature, 2020. 397 p.
2. Jiang R., Bouridane A., Li Ch.-T., Crookes D., Boussakta S., Hao F., Edirisinghe E. A. *Big Data Privacy and Security in Smart Cities*. Switzerland, Cham : Springer Nature, 2022. 248 p.

15. Інформаційні ресурси

1. Big Data Analytics in Cybersecurity: Role and Applications [Ел. ресурс]. URL: https://www.analyticssteps.com/blogs/big-data-analytics-cybersecurity-role-and-applications
2. Learning the Basics of Big Data Analytics for Cybersecurity [Ел. ресурс]. URL: https://www.orientsoftware.com/blog/data-analytics-cybersecurity
3. 5 Best Applications of Big Data Analytics in Cyber Security Industry [Ел. ресурс]. URL: https://www.ksolves.com/blog/big-data/5-best-applications-of-big-data-analytics-in-cyber-security-industry
4. Challenges of Big Data in Cybersecurity [Ел. ресурс]. URL: https://bigdataldn.com/news/challenges-of-big-data-in-cybersecurity/
5. How Can Big Data Help in Augmenting Cybersecurity? [Ел. ресурс]. URL: https://www.datatobiz.com/blog/big-data-analytics-in-cybersecurity/