ỨNG DỤNG AI TRONG ATTT (AI APPLICATIONS IN INFORMATION SECURITY)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: Ứng dụng AI trong ATTT (AI Applications in Information Security)

Course code: SEC1413_CLC

Course type: Selective

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with basic and advanced knowledge about artificial intelligence (AI), machine learning (ML), deep learning (DL) and the application of ML & DL in solving problems of information security.

Skills:

On successful completion of this course a student will be able to:
- Apply AI/ML/DL models to solve information security problems;
- Implement and evaluate AI applications in information security field.

Attitude:

Students are required to attend the classes and complete assignments/projects.

3. Abstracts

This course provides students with basic and advanced knowledge about AI, ML, DL and the application of ML & DL in solving information security problems. Specific topics of this course include overview of AI, ML and DL; traditional machine learning, deep learning and transfer learning models; data preprocessing techniques; traditional machine learning models for information security; deep and transfer learning models for information security.

4. Teaching and learning methods

Lectures:	24h
Exercises:	5h
Projects:	8h
Labs:	8h
Individual reading:	0h

5. Prerequisites: Fundamentals of Information Security - SEC1401_CLC, Python for information security - SEC1301_CLC

6. Learning outcomes

After completing this course, the student is able to:

[CLO1]: Explain the basic and advanced knowledge about AI, ML, DL;
[CLO2]: Apply AI models to solve information security problems;
[CLO3]: Implement and evaluate AI applications in information security field.

7. Assignment criteria

Learning outcomes	**Assignment criteria**
[CLO1]: Explain the basic and advanced knowledge about AI, ML, DL	Chapter 1, Chapter 2, Chapter 3
[CLO2]: Apply AI models to solve information security problems	Chapter 2, Chapter 3
[CLO3]: Implement and evaluate AI applications for information security fields	Chapter 2, Chapter 3

8. Outlines

Chapter 1 Basics of AI, machine learning, deep learning

1.1. Basic concepts of AI, ML and DL
1.2. Traditional machine learning models
1.3. Deep learning models
1.4. Transfer learning models
1.5. Generative AI models
1.6. Data preprocessing techniques
1.7. Evaluation of machine learning models
1.8. Python and machine learning libraries

Chapter 2 Traditional machine learning models for information security

2.1. Introduction to machine learning models for information security
2.2. Web attack detection
2.3. Phishing and malicious URL detection
2.4. Botnet domain name detection
2.5. Network traffic analysis

Chapter 3 Deep and transfer learning models for information security

3.1. Introduction to deep and transfer learning models for information security
3.2. Web defacement detection
3.3. Vulnerability detection in source code
3.4. Malware detection
3.5. Toxic news detection

9. Required Textbooks

[1] Andreas C. Müller and Sarah Guido. Introduction to Machine Learning with Python: A Guide for Data Scientists, 1st Edition, O'Reilly Media, 2016.
[2] Francois Chollet. Deep Learning with Python, 2nd Edition, Manning, 2021.

10. Suggested Textbooks

[3] Peng Liu, Zhilong Wang, Tao Liu. AI for Cybersecurity: A Handbook of Use Cases. Penn State Cyber Security Lab, 2024.
[4] Emmanuel Tsukerman. Machine Learning for Cybersecurity Cookbook. Packt Publishing, 2019.
[5] Ivan Vasilev, Daniel Slater, Gianmario Spacagna, Peter Roelants, Valentino Zocca. Python Deep Learning, 2nd Edition, Packt Publishing, 2019.
[6] Từ Minh Phương. Giáo trình Nhập môn trí tuệ nhân tạo, Học viện Công nghệ BCVT, 2015.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1 Basics of AI, machine learning, deep learning	8h lecture 3h exercise 2h project 2h lab	1.1. Basic concepts of AI, ML and DL 1.2. Traditional machine learning models 1.3. Deep learning models 1.4. Transfer learning models 1.5. Data preprocessing techniques 1.6. Evaluation of machine learning models 1.7. Python and machine learning libraries
Chapter 2 Traditional machine learning models for information security	8h lecture 1h exercise 3h project 3h lab	2.1. Introduction to machine learning models for information security 2.2. Web attack detection 2.3. Phishing and malicious URL detection 2.4. Botnet domain name detection 2.5. Network traffic analysis
Chapter 3 Deep and transfer learning models for information security	8h lecture 1h exercise 3h project 3h lab	3.1. Introduction to deep and transfer learning models for information security 3.2. Web defacement detection 3.3. Vulnerability detection in source code 3.4. Malware detection 3.5. Toxic news detection

12. Grading Policy

Attendance:	10%
Mid-term exam/exercises:	10%
Course projects:	30%
Final examination:	50%