# COURSE DESCRIPTION CARD - SYLLABUS

Course name
AI in multimedia cybersecurity [S1Cybez1>AIwC]

## Course

Field of study
Cybersecurity

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

## Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
16

## Number of credit points

5,00

## Coordinators

dr inż. Mateusz Lorkiewicz
mateusz.lorkiewicz@put.poznan.pl

dr hab. inż. Olgierd Stankiewicz prof. PP
olgierd.stankiewicz@put.poznan.pl

## Lecturers

## Prerequisites

A student entering this course should have basic knowledge of the fundamentals of programming, systems theory, signal theory, digital signal processing, machine learning, artificial intelligence and the basics of telecommunications. Student has a structured, mathematically supported knowledge of acquisition, human perception, quality assessment, processing, digital representation and compression of video and audio. Student is able to acquire information from literature and databases and other sources in Polish or English; Student can integrate obtained information, interpret it, draw conclusions and justify opinions. Knows the limitations of his/her own knowledge and skills, understands the necessity of further education. He is able to implement team projects

## Course objective

The subject aims to present how artificial intelligence and machine learning can be used in posing threats in cyber security, but also detecting these threats, security analysis and multimedia protection

## Course-related learning outcomes

Knowledge:
K1_W05 - Has advanced knowledge of complex data structures; knows the basics of the theory, knows the principles of data administration and related standards; knows the principles of cyber security and privacy used to manage the risks associated with the use, processing, storage and transmission of information or data
K1_W06 - Has advanced knowledge of the principle of computer program development, the structures of programming languages, their levels and the algorithms used; has advanced knowledge of software engineering;
K1_W09 - Has in-depth knowledge of the life cycle, design and use of attack-resistant software information systems; knows and understands the principle of their operation; knows the tools used to identify vulnerabilities in communication software; knows the impact of software configuration on security;
K1_W15 - Has knowledge of information technology supply chain security and supply chain risk management principles, requirements, and procedures; is aware of the need for regulations, policies, procedures, or management relevant to critical infrastructure cyber security; has knowledge of risk management processes (e.g., risk assessment and mitigation methods); is familiar with threat identification and risk/threat assessment methods; is familiar with risk mitigation methods.
K1_W16 - Has a basic knowledge of machine learning systems and artificial neural networks; has a structured knowledge of the principles and methods of solving decision-making and optimization problems using heuristic and non-heuristic state space search algorithms including methods with resource constraints; is familiar with artificial intelligence methods used in the field of study.
K1_W20 - Knows and understands the risks faced by modern civilization massively using digital services; is familiar with the latest development trends related to the studied field of study

Skills:
K1_U01 - Able to use literature sources, integrate acquired information, evaluate and interpret it and draw conclusions, in order to solve complex and unusual problems in the area of cyber security.
K1_U02 - Able to use appropriately selected methods and tools, including advanced information and communication techniques, as well as develop simple applications or configure a simple system, in order to simulate, analyze and design systems or applications relevant to the field of study.
K1_U07 - Can, when formulating and solving tasks related to cyber security, recognize their systemic and non-technical aspects, including ethical, economic and legal aspects.
K1_U12 - Can prepare and deliver a presentation on a task related to the field of study, communicates using specialized terminology, presents and justifies various opinions and positions

Social competences:
K1_K01 - Understands the importance of improving professional, personal and social competencies; is aware that knowledge and skills in the area of cyber security are rapidly evolving
K1_K02 - Understands the importance of knowledge in solving cyber security problems; is aware of the need to use expert knowledge when solving engineering tasks beyond his/her own competence
K1_K03 - Understands the need to formulate and communicate information and opinions to the public on the positive and negative aspects of cyber security, and is ready to act on behalf of the public interest

## Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. projects/seminars
Execution of a project and presentation of results at a project/seminar meeting. The grade depends on the complexity, sophistication of the project/seminar and the evaluation of the presentation.
2 Laboratories
Colloquium at the end of the semester and/or tests to check mastery of current material. The colloquium/tests will consist of several/several review questions, depending on the nature of the questions taken. The exact nature of the questions will be communicated to the students before the date of holding the colloquium/test
3 Lecture
Written and/or oral exam. The exam consists of several - several questions (depending on the adopted nature of the questions) and concerns the content presented during the lectures. The exact nature of the exam questions will be presented to the students during one of the last lectures.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a

prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

## Programme content

Basic knowledge of defining attacks on and with multimedia data. Examples of attack and data leakage scenarios. Use of artificial intelligence for content tampering and detection. Analysis of the mulimedia data stream for attack detection.

## Course topics

Defining an attack using/on multimedia data: Changing content, deleting content, generating fake content, destroying content, stealing content.
Example attack/data leakage scenarios: `fakenews` based on generated content, use of multimedia data to generate content used in scams, impersonation of entities by copying graphical interfaces, generation of false reports by provoking content.
Content interference. Application of AI in analysis and detection of multimedia threats : analysis of multimedia streams and their surveillance, detection of content interference, detection of sensitive data leaks, detection of intellectual property leaks.
Automatic differentiation of stream degeneration from attack : distinguishing technical problems from attempts to intentionally affect the content or operation of a multimedia system.
Selected attack techniques: phishing, theft of multimedia data used by AI tools, content generation by bots for disinformation purposes, attacks on CCTV.

## Teaching methods

1. projects/seminars - classes are based on discussion of selected topics related to the topic of multimedia cyber security. The main part of them is the analysis of the assigned problem and discussion of its solutions. As part of an individual or group project, students consider the given problem. Then, within the framework of the meetings, they refer to its analysis and proposed solutions. During the presentation, students answer questions related to the presented topic (the instructor or other students).
2.Laboratory exercises deal with selected issues discussed in lectures. Students have the opportunity to watch and listen to the results of simulated threats (audio and video). To some extent, they can shape the analyzed methods on their own - both attack and detection/prevention methods.
3. lecture - Classes with distinct elements of traditional lecture, problem lecture (discussion with students of a specific problem) and conversation lecture (mobilizing students to discuss a specific topic), depending on the content of the material presented. Selected content of the lecture is presented on a multimedia projector or blackboard. The discussion of issues is accompanied by information on their practical application.

## Bibliography

Basic:
Bhaskar Mondal, Shyam Singh Rajput, Multimedia Security Tools, Techniques, and Applications, CRC Press, ISBN: 9781774915028
Loveleen Gaur, DeepFakes Creation, Detection, and Impact, CRC Press, ISBN 9781032139234
Subhrajyoti Deb, Aditya Kumar Sahu, Securing the Digital World A Comprehensive Guide to Multimedia Security, CRC Press , ISBN 9781032663623

Additional:
Ian Goodfellow, Yoshua Bengio, Aaron Courville , Deep Learning, MIT Press Ltd, ISBN: 9780262035613
Marek Domański, Obraz cyfrowy. Reprezentacja, kompresja, podstawy przetwarzania. Standardy JPEG iMPEG, Wydawnictwa Komunikacji i Łączności, 2010, ISBN: 978-83-206-1795-5.
David Foster, Deep learning i modelowanie generatywne. Jak nauczyć komputer malowania, pisania, komponowania i grania, Helion, ISBN: 978-83-283-7283-2
D. Karwowski, Zrozumieć kompresję obrazu, 2019, ISBN: 978-83-953420-0-4.
T. Zieliński T. P. Korohoda, R. Rumian (red.), Cyfrowe przetwarzanie sygnałów w telekomunikacji, PWN, Warszawa 2014.

## Breakdown of average student's workload

| | Hours | ECTS |
|---|---|---|
| Total workload | 139 | 5,00 |
| Classes requiring direct contact with the teacher | 64 | 2,50 |
| Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation) | 75 | 2,50 |