COURSE DESCRIPTION CARD - SYLLABUS

Course name
Financial Sector Security [S1Cybez1>BSF]

Course

Field of study
Cybersecurity

Year/Semester
4/7

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
16

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

2,00

Coordinators

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

Basic knowledge of the functioning of IT systems and general understanding of cybersecurity.

Course objective

The aim of the course is to develop knowledge and skills related to security in the financial sector, with a particular focus on electronic payment systems. Students will explore the latest technologies, attack methods, and prevention measures, as well as the specifics of financial crime.

Course-related learning outcomes

Knowledge • Understands the mechanisms of electronic payment systems and cashless payment methods. [K1_W05]
• Recognizes threats related to electronic banking and payment systems in e-commerce. [K1_W17]
• Knows basic methods and tools used in social engineering attacks and ways to identify them. [K1_W20]
• Has knowledge of financial crimes such as phishing, malware, and money laundering. [K1_W20]
• Understands identity and access management (IAM) principles in the financial sector. [K1_W17]
Skills • Can identify symptoms indicating a potential attack on electronic payment systems. [K1_U04]
• Is able to analyze cases of attacks on electronic banking and design appropriate preventive measures.

[K1_U06]
• Develops multi-factor authentication procedures and manages access to critical resources.[K1_U02]
• Utilizes tools and methods of behavioral analysis to detect threats. [K1_U08]
Social competences • Understands the importance of financial and technological protection in the context of public security. [K1_K03]
• Is aware of the dynamic nature of threats in the financial sector and the necessity of continuously updating knowledge.[K1_K01]
• Collaborates in a team to analyze and prevent financial crimes. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

• Written Exam (Knowledge): Test and open-ended questions assessing understanding of payment system mechanisms, threats, and countermeasures.
• Laboratories (Skills): Case analysis, security design, and attack/defense simulations.
3
• Team Project (Social Competencies): Development of a financial system protection plan, including risk analysis.
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

Electronic Payment Systems
2. Threats to Financial Systems
3. Attacks on Financial Systems
4. Financial Sector Security Management
5. AI in the Financial Sector

Course topics

1: Introduction to Electronic Payment Systems (90 minutes)
• History and evolution of electronic payments.
• Types and forms of cashless payments: payment cards, electronic transfers, mobile payments.
• Overview of e-commerce systems: platforms and payment mechanisms.
• Digital wallets: functionality and examples (e.g., PayPal, Google Pay, Apple Pay).
2: Threats in Electronic Banking (90 minutes)
• Key threats for private and institutional users.
• Overview of attack methods: keylogger, man-in-the-middle, credential stuffing.
• Preventive measures for protecting electronic banking.
• Case study: common user errors leading to financial loss.
3: Financial Crimes in Cashless Transactions (90 minutes)
• Definitions and classification of financial crimes: phishing, malware, money laundering.
• Threat analysis related to malware targeting financial systems.
• Money laundering mechanisms using electronic payment systems.• Case study: analysis of detected fraud cases.
4: Attacks on Financial Systems – Stages and Methods (90 minutes)
• Attack preparation stages: reconnaissance, vulnerability identification.
• Security analysis and possible bypass methods.
• Social engineering in practice: phishing, spear phishing, vishing – definitions and differences.
• Examples of real financial sector incidents.
5: Security Management in the Financial Sector (Part 1) (90 minutes)
• Identity and access management (IAM): mechanisms and standards.
• Multi-factor authentication (MFA): techniques, advantages, and disadvantages.
• Managing critical assets and systems.
• Practical aspects of customer data protection in financial institutions.

6: Security Management in the Financial Sector (Part 2) (90 minutes)
• Behavioral analysis as a tool for detecting anomalies in financial systems.
• Network security in financial institutions: segmentation, monitoring, IDS/IPS systems.
• Security standards and regulations in the financial sector (e.g., PSD2, GDPR).
• Practical aspects of incident management in the financial sector.
7: Artificial Intelligence in the Financial Sector (90 minutes)
• Introduction to AI applications in financial transaction analysis.
• Fraud detection mechanisms using machine learning algorithms.
• AI's impact on automating financial security processes.
• Examples of AI-powered tools for financial system protection.
8: The Future of Financial Sector Security (90 minutes)
• Blockchain development and its impact on financial transaction security.
• Trends and challenges in financial system security.
• Overview of innovative technologies supporting financial sector protection.
• Summary and discussion on integrating technology and security processes.

Teaching methods

• Theoretical lectures with multimedia presentations in online mode.
• Practical laboratories: case analysis, security design.
• Discussions and crisis situation simulations.

Bibliography

1. Krzysztof Jajuga, Risk Management, PWN Scientific Publishing, Warsaw 2016. (ksiegarnia.pwn.pl)
2. William Stallings, Cryptography and Network Security: Principles and Practice, 8th edition, Pearson, 2020. (pearson.com)
3. Documentation and reports on financial crime, e.g., reports from the National Bank of Poland (NBP) and the Polish Financial Supervision Authority (KNF).
Additional
1. J. Czapska, Z. Rau, The Police in Civil Society, Kraków: Zakamycze, 1997.
2. A. Tyburska, Crisis Management: Organization, Planning, Response, Warsaw: PWN Scientific Publishing, 2012.
3. C. Hadnagy, Social Engineering: The Art of Human Hacking, Gliwice: Helion Publishing, 2012.
4. Articles and reports on cybersecurity published by CERT Polska, ENISA (European Union Agency for Cybersecurity), etc.
For item 4, due to its dynamic nature, it is recommended to follow the latest publications on the official websites of relevant institutions.

Breakdown of average student's workload

	Hours	ECTS
Total workload	57	2,00
Classes requiring direct contact with the teacher	32	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	25	1,00