LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES

Ref. No.: …
Copy No.:

CURRICULUM OF THE MASTER’S PROGRAM INTERNATIONAL CYBERSECURITY STUDIES

Validity:
From the academic year of 2024/2025 progressively

Decision of the Senate	Decision of the Board of Governors
Approved by Senate resolution No. ………………….	Approved by the Board of Governors resolution No. ………………….

Budapest, 2024.

Program director: Tamás SZÁDECZKY, associate professor

The following legislation and university regulations serve as the legal background for the curriculum:

1. Act CCIV of 2011 on National Higher Education
2. Act CXXXII of 2011 on the National University of Public Service and on Public Administration, Law Enforcement and Military Higher Education
3. Government Decree No. 87/2011. (IV. 9.) on the implementation of certain provisions of the Act CXXXII of 2011
4. Government Decree No. 363/2011. (XII. 30.) on the implementation of certain provisions of Act CXXXII of 2011 on the National University of Public Service and on Public Administration, Law Enforcement and Military Higher Education
5. ITM Decree 65/2021 (XII. 29.) on the list of qualifications and the establishment of new qualifications in higher education and the relevant Ministerial Communication on the training and outcome requirements for higher education vocational training, bachelor's and master's programmes;
6. NUPS Academic and Study Regulation
7. No. 26/2019. Rector’s decision on program procedures

Training authentication data

No. of Faculty Council resolution:	31/2023. (VII.11)
No. of Senate resolution:	
No. of Board of Governors Resolution	
MAB (Hungarian Accreditation Committee) Code:	Mi2115
No. of MAB resolution:	2023/10/VIII/3
Registration No. by OH (Educational Authority):	FNYF/12668/2023.
FIR Code of the Program	MSZKITN
First year of announcement:	2024/2025

Tartalomjegyzék

1. **Name of the program:**

   International Cyber Security Studies MA

2. **Field of education, defined by Section 3 of NUPS Act:**

   science of public governance, international and European public service

3. **Specializations of the program:**

   -

4. **Qualification:**

   master (magister; abbreviated: MA) level

5. **Degree and qualification to be obtained in the program as specified in the diploma**

   International Cybersecurity Expert

6. **Objectives of the program, professional competences to be acquired:**

   The aim of the training is to prepare professionals with higher education qualifications who are able to effectively plan, organise and manage cybersecurity tasks in managerial and expert positions in domestic and foreign public and international organisations and companies. The Master's programme focuses on the cybersecurity issues, current and future challenges facing both the public and private sectors and society. Students will acquire a broad knowledge of the theoretical and practical aspects of cybersecurity, its security, environmental, social and economic aspects. The differentiated professional curriculum will enable them to carry out research, development and planning tasks in their area of expertise, to analyse security problems in a scientific manner and to draw conclusions.
   The training will qualify the student for the roles of Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officer, and Cybersecurity Risk Manager, as defined in the European Cybersecurity Skills Framework.

   6.1. Common professional competences in the field of public administration at Master's level:

   6.1.1. Knowledge:
   - Knowledge of the general and specific characteristics, main directions and well-defined boundaries of the broad subject area of the field, the main contexts and theories of the field and the terminology that builds them up, the relationship of the field to related disciplines.
   - Knowledge of the specific methods of knowledge acquisition and problem-solving, abstraction techniques and ways of working out the practical implications of theoretical issues in the field.
   - Knowledge of the links between the use of basic environmental resources and socio-economic processes in the context of their field of specialisation.
   - Knowledge of digital technologies and how to communicate with them in the public service in their field of specialisation, and knowledge of digital communication tools appropriate to the context.
   - Have a command of a specialist language in at least one foreign language specific to the field.

   6.1.2. Ability to:
   - Ability to serve the public good and the public interest with the professional commitment and according to the professional and human standards expected in a career in the public service.
   - Have a broad approach, complex problem-solving skills and the ability to process information at a high level.
   - Ability to apply systems thinking, change and planning to support innovative problem solving.

- Proficient in the use of digital technologies in the civil service in the area of their specialisation. Ability to apply and comply with appropriate security standards and rules when using ICT systems.
- Ability to use at least one foreign language in an appropriate manner in his/her field of competence.

6.1.3. Attitude:
- Commitment to the public service, recognition of the responsibilities of the public service and ability to represent its ethos in an authentic manner.
- Commitment to democratic values and the rule of law, sustainability, social solidarity and equal opportunities.
- It has a well-developed professional identity and sense of vocation, which it shares with the professional and wider social community.
- He is a committed and responsible professional who takes part in the management of his organisation, in the development, discussion and implementation of professional concepts.
- He/she builds his/her career responsibly and supports the development of the professional careers of the staff he/she supervises.
- He/she deepens and consolidates his/her professional interests, continuously develops his/her self-learning, is open to new ideas and new approaches, and keeps abreast of and applies changes in legislation. He is committed to acquiring, evaluating and using the theoretical, scientific research and practical information necessary for the development of the methodology of the field.
- In carrying out his/her work, he/she is guided by professional standards and is committed to taking decisions in full compliance with the legislation and ethical standards in force.
- Possess the personal qualities required for management duties, such as independence of thought, problem awareness, responsibility, judgement and decision-making.
- Demonstrates initiative, personal responsibility and the ability to make the right decisions in solving problems related to his/her job. Professional commitment to quality work.
- Is self-critical in his/her work and is open to well-founded criticism, which contributes to the development of his/her professional values.
- He strives for results and community consensus when working together.

6.1.4. Autonomy and responsibility:
- Assumes responsibility for adhering to professional, legal and ethical standards and rules related to his/her work and conduct.
- Within the scope of his/her responsibilities, he/she is able to make proposals, assign tasks and prepare and manage their implementation independently, in accordance with his/her position and job description.
- Has a high degree of autonomy in developing, presenting and justifying professional opinions on general and specific professional issues.
- Ability to take independent initiative and personal responsibility for the environmental and social impact of decisions in planning and implementing professional tasks.
- Responsible for the division of tasks within the organisation, for the functioning and effectiveness of the organisation, for issuing management instructions, for managing autonomously and for working effectively at individual and organisational level.
- He/she takes responsibility for the effectiveness of professional cooperation in his/her area of competence and accepts the framework, roles, functions and responsibilities arising from such cooperation.

6.2. Common professional competences for international and European public higher education in Masters programmes:

6.2.1. Knowledge:
- In-depth knowledge of the context of international sectoral law and the system of international organisations related to the field.
- Knowledge of international sectoral models of public service systems.

- Knowledge of the principles and rules of operation of diplomatic relations, the rules and specificities of cooperation between the domestic and international institutional system in the sector.
- Mastery of the professional language required for the operation of his/her field of specialisation.

6.2.2. Ability to:
- Ability to work in an international, multicultural environment.
- Ability to participate at a high level in the activities of international organisations and institutions.
- Ability to understand the responsibilities, tasks and processes arising from international memberships, partnerships and other organisational relationships and to integrate them into decision-making processes.
- Ability to apply strategic planning, analysis and evaluation methods of the policy concerned and to participate in the implementation of strategies at government, sectoral and organisational level.

6.2.3. Attitude:
- Working in an international organisation, committed to the objectives and interests of the organisation.

6.2.4. Autonomy and responsibility:
- Depending on his/her position in the organisational structure, a constructive and strong advocate in forms of cooperation within and outside the institution, always giving priority to the objectives and interests of the international organisation, depending on the Hungary or the application.

6.3. Professional competences to be acquired:

6.3.1. Knowledge:
– Is familiar with cybersecurity policies.
– Is familiar with cybersecurity standards, methodologies and frameworks.
– Is familiar with cybersecurity recommendations and best practices.
– Is familiar with cybersecurity related laws, regulations and legislations.
– Is familiar with cybersecurity-related certifications.
– Is familiar with ethical cybersecurity organisation requirements.
– Is familiar with cybersecurity maturity models.
– Is familiar with procedures in case of cyber attacks.
– Is familiar with resource management.
– Is familiar with management practices.
– Is familiar with risk management standards, methodologies and frameworks.
– Is familiar with legal, regulatory and legislative compliance requirements, recommendations and best practices.
– Is familiar with privacy impact assessment standards, methodologies and frameworks.
– Is familiar with risk management tools.
– Is familiar with risk management recommendations and best practices.
– Is familiar with cyber threats.
– Is familiar with computer systems vulnerabilities.
– Is familiar with cybersecurity controls and solutions.
– Is familiar with cybersecurity risks.
– Is familiar with monitoring, testing and evaluating cybersecurity controls’ effectiveness.
– Is familiar with cybersecurity-related technologies.

6.3.2. Capability:
– Is capable of assessing and enhancing an organisation’s cybersecurity posture.
– Is capable of analysing and implementing cybersecurity policies, certifications, standards, methodologies and frameworks.
– Is capable of analysingand complying with cybersecurity-related laws, regulations and legislations.

– Is capable of implementing cybersecurity recommendations and best practices.
– Is capable of managing cybersecurity resources.
– Is capable of developing, championing and leading the execution of a cybersecurity strategy.
– Is capable of designing, applying, monitoring and reviewing Information Security Management System (ISMS) either directly or by leading its outsourcing.
– Is capable of reviewing and enhancing security documents, reports, SLAs and ensure the security objectives.
– Is capable of identifying and solving cybersecurity-related issues.
– Is capable of establishing a cybersecurity plan.
– Is capable of anticipating required changes to the organisation's information security strategy and formulate new plans.
– Is capable of defining and applying maturity models for cybersecurity management.
– Is capable of anticipating cybersecurity threats, needs and upcoming challenges.
– Is capable of comprehensive understanding of the business strategy, models and products and is able to factor into legal, regulatory and standards' requirements.
– Is capable of carrying out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy.
– Is capable of leading the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further of ensuring its acceptance, comprehension and implementation and communicate it between the involved parties.
– Is capable of conducting, monitoring and reviewing privacy impact assessments using standards, frameworks, acknowledged methodologies and tools.
– Is capable of explaining and communicating data protection and privacy topics to stakeholders and users.
– Is capable of understanding legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies.
– Is capable of implementing cybersecurity risk management frameworks, methodologies and guidelines and ensuring compliance with regulations and standards.
– Is capable of analysing and consolidating organisation's quality and risk management practices.
– Is capable of building a cybersecurity risk-aware environment.

6.3.3. Attitude:
– Influence an organisation's cybersecurity culture.
– Understand, practice and adhere to ethical requirements and standards.

6.3.4. Autonomy and responsibility:
– Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks.
– Communicate, present and report to relevant stakeholders.
– Communicate, coordinate and cooperate with internal and external stakeholders.
– Propose and manage risk-sharing options.

7. Factors of program schedule:

Program length in semesters:
2 semester

Detailed program schedule:

Number of credits necessary for obtaining the degree	60 credits
Students' study hours in total	630
Student workload in credits per semester:	30 credits on average
Number of classes per semester for full-time students:	315 classes on average

Number of weekly classes on average for full-time students:	19,5 classes on average, out of which the number of classes with credits on average: 19,5
Number of classes per semester for part-time students:	-
Length of internship:	-

8. Program structure

8.1. thesis/diploma work credits:
5 credits

8.2. minimum credit for practical training outside the university:
-

8.3. minimum credit for elective courses:
-

9. Class, credit and exam-plan

The class, credit and exam-plan contains the following information scheduled in terms of each subject (compulsory curricular activities – hereinafter together: subject):
a) Neptun code of subjects,
b) type of subject (compulsory, mandatorily selected, elective, compulsory curricular activity),
c) semester(s) the subject is offered,
d) number of lessons per week and semester, or semester as per the type of subject,
e) credit value of the subject,
f) type of performance assessment;
g) the department and lecturer responsible for the subject.

Types of lessons and their abbreviations:
- lecture: L
- seminar: S
- practice: P
- e-seminar: ES

The class, credit and exam-plan is included in Annex 1.

10. Previous study requirements

The curriculum defines previous or simultaneous study requirements of subjects (Previous study requirements). Previous study requirements are included in Annex 2.

11. The assessment system

Assessment can be carried out:
a) in the study period on the lessons in oral or written form by written (in-class) tests, home assignments or practical tasks as a mid-term mark;
b) by exams in the exam period;
c) by a mid-term mark and exam mark together.

In case of compulsory curricular activities without credits the requirement can solely be the lecturer’s signature.

Students finish their studies by taking the final examination. The final examination is to check and assess the knowledge, skills and abilities necessary for obtaining the diploma when students also have to prove they can apply their knowledge in practice.

Abbreviations of types of assessment:
- mid-term mark: MTM/ mid-term mark (((final exam subject ((MDM(F))
- term mark: TM / term mark (((final exam subject ((TM(F))
- exam: E/ exam (((final exam subject ((E(F))

- exam (three-scale) (E3)
- preliminary exam (PE)
- comprehensive exam (CE)
- complex exam (CXE)
- final examination (FE)

Detailed rules on assessment are defined by:
- the curriculums of subjects being part of the present curriculum, and
- Point 12 of the present section based on the relevant regulations and the Academic and Examination Regulations.

12. Final examination

12.1. Preconditions for starting the final examination

Preconditions for starting the final examination:
- obtaining the pre-degree certificate: the university issues a pre-degree certificate for students who have completed the study and exam requirements set in the curriculum (excluding the language exam requirements and the thesis/diploma work), the internship and acquired the necessary credits; the pre-degree certificate states that the student has fulfilled all the necessary study and exam criteria without qualification or assessment.
- thesis/diploma work already being evaluated.

12.2. Parts of the final examination

Parts of the final exam
- Defending the diploma work,
- Oral exam of the course-units
- Defending the diploma work successfully is a precondition of commencing the oral final exam.

12.3. The result of the final examination

The result of the final examination
The result of the final exam, based on the NUPS Regulations on Studies and Exams, is the simple average of the diploma work’s mark and the oral final exam’s mark as follows:

FE = (DW + OFE)/2

Failure to pass any part on any element will result in the failure of the final exam. Each element of the final exam must be awarded a separate grade. Unless otherwise stated, the calculation method specified in Article 54 (3) of the NUPS Regulations on Studies and Exams may be incorporated.

13. Thesis/diploma work

The preparation, content- and form-related requirements of the thesis/diploma work are defined in the Academic and Study Regulations.

Subjects of the Degree Thesis:
- ÁKIBTM021, Degree-thesis, 5 credits;

14. Diploma

14.1. Conditions for receiving the diploma

Detailed regulations on assessing the grade of the diploma.

14.2. Determining the grade of the diploma

Determining the grade of the diploma
Detailed regulations on assessing the grade of the diploma.
In lieu of a different regulation the calculation in Section 56. § (3)-(5) of the Academic and Study Regulations may prevail:
„(3) The Diploma grade, unless the course curriculum provides otherwise, shall consist of the simple average of the following:
a) the grade for the defence of the thesis/diploma work;

b) the grade for the oral part of the final examination (in the case of a multi-module examination the rounded average of the grades given for integer elements);
c) the grade for the final practical exam (if applicable);
d) the (two-decimal) average of the academic average of completed semesters:
(Th + Fe + Pr + ((A1 + ... + An) / n) / 4
If the final exam has no practical elements included:
(Th + Fe + ((A1 + ... + An) / n) / 3
(4) The degree classification shall be based on the following limits taking into account the value calculated with the use of the above method:
- outstanding, if the average is 5.00;
- excellent, if the average is: 4.51 to 4.99;
- good, if the average is: 3.51 to 4.50;
- satisfactory, if the average is: 2.51 to 3.50;
- pass if the average is 2.00 to 2.50;.
(5) The student with an outstanding diploma grade shall graduate with outstanding result. Those with excellent diploma qualifications and a minimum of 4.51 examination and practice average shall also graduate with outstanding results."

15. Internship

-

16. International student mobility period for partial studies abroad

International student mobility period for partial studies abroad
The Erasmus+ Programme provides students engaged in Bachelor or Master training with a possibility to gain an academic mobility or internship scholarship. Academic mobility enables scholarship recipients to spend a semester studying at a partner institution of the university, and to transfer credits for courses undertaken there to their studies in Hungary. The so-called exchange programme allows students to pursue studies at a given institute free of charge.
Applicants can travel to EU countries, Iceland, Lichtenstein, Norway, Turkey, Serbia and Northern Macedonia, to institutions with which the University has an inter-institutional agreement. A list of the available universities is available on the University's website. Within the framework of international credit mobility (non-European countries), the University provides links with partner institutions in the region, which vary from academic year to academic year and from application cycle to application cycle.
The number of bilateral inter-institutional agreements has been steadily increasing. Due to the training objectives, the Faculty encourages students to partake in international mobility programmes. Students conducting studies abroad shall be authorized for a reduced course load; furthermore, the Credit Transfer and Validation Committee recognizes a broad range of subjects completed abroad as equivalents of compulsory or elective subjects.
Due to the structure of the training, Term 1 and Term 2 are the most suitable for pursuing studies abroad.

17. Any other program-specific requirements

17.1. Conditions of choosing a specialization

-

17.2. Distinction/basic examination/complex examination

-

17.3. Criteria requirements

Szöveg beírásához kattintson vagy koppintson ide.

17.4. Requirements of attendance, acceptable absence, opportunity for compensating for missed classes

I. Courses accepted as prerequisites for entry to the Master's programme

I.1. The following may be taken into account for full credit: a Bachelor's or Master's degree in the field of Political Science, Law, Economics, or in one of the courses or branches of

study which can be classified as such but which have been discontinued or converted, or its foreign equivalent.
I.2. The master's degrees in business informatics, computer engineering, computer programming, autonomous systems informatics, defence information and communication systems design, and electrical engineering may be taken into account in the first instance when the credits specified in point II are completed.
I.3. In addition, the bachelor's and master's degree courses and the courses under Act LXXX of 1993 on Higher Education may be taken into account for the completion of the credits specified in point II, which are accepted by the CCEB on the basis of a comparison of the knowledge on which the credit is based.

II. Minimum conditions for admission to the Master cycle for holders of the degrees indicated in I.2 and I.3. The minimum number of credits required for admission to the Master's programme from previous studies is 460 credits in the following areas:
- computer science (20 credits): software engineering, systems engineering and databases and information systems, application of cryptography, information security, computer architecture and computer networks;

- Public and social sciences (40 credits): administrative law, constitutional law, criminal law, administrative criminal law, administrative criminal law, administrative regulation, European public law, international law, public administration, economics, political science, psychology, management and organisation theory, data protection.

To be admitted to the Master's programme, candidates must have at least 50 credits in the listed fields of study. Of the credits required for admission to the Master's programme, 25 credits may be credited on the basis of work experience or non-formal learning outcomes. The missing credits must be acquired in parallel with the Master's degree course as specified in the Study and Examination Regulations.

17.5. Specific teaching-learning methods, learning support tools, methodology, procedures

The subjects are a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

Requirements of attendance, acceptable absence, opportunity for compensating for missed classes:
Should the course description not regulate differently, the student is obliged to participate in 75% of the classes. Absence above that ratio may result in the refusal of signature. Absence over 75% may be justified in cases such as e. g. medical treatment, being in service, etc. This, however, has to be proven in the following class by providing the certificate to the lecturer and the course director, as well as via e-mail. The material of the classes missed this way should be learned privately.

Rules for the completion of subjects with a reduced timetable:
In the case of students studying under the preferential study regime as stipulated in § 20 of the NKE Study and Examination Regulations, unless otherwise specified in the course programme, the requirements for attendance in class, the acceptable level of absences and the possibility of making up for absences, the student must complete an assignment to be completed at home in a form agreed with the course instructor by the last working day before the end of the term. The student must contact the course instructor within 10 working days of receipt of the decision granting the reduced study arrangement to agree the conditions for the assignment to be completed at home.

Budapest, 2024

program director: Tamás SZÁDECZKY, PhD
associate professor

List of curriculums

I. Core studies

- Cybersecurity Regulations and Standards
- Introduction to Cybersecurity
- Cyber Warfare
- Applied Cybersecurity Technologies
- Personal Data Protection
- Risk Assessment, Risk Management
- Critical Information Infrastructure Protection
- Cybercrime
- IT System and Network Security
- Cyber Diplomacy
- Cybersecurity Strategy and Digital Transformation
- Crisis Management and Communications
- Human Factors of Cybersecurity
- Incident Management
- Cyber Threat Intelligence
- Security Testing and Forensics

II. Thesis/diploma work

III. Internship

IV. Elective courses

V. Criteria requirements

Szöveg beírásához kattintson vagy koppintson ide.

CURRICULUM OF THE MASTER’S PROGRAM INTERNATIONAL PUBLIC SERVICE RELATIONS

COURSE UNITS

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM014

2. Course title: Applied Cybersecurity Technologies

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Tamás SZÁDECZKY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The course shows students the application of security technologies, the techniques, and the threats of IT systems. The course introduces students to theoretical foundations of cyber defense processes, prevention and early warning, detection, response, and security incident management; and more deeply about the advantages, disadvantages, uses and limitations of logical protection technologies. The primary goal is to develop a complex approach to those techniques. In addition, the aim is to acquire practical knowledge in order to develop a team of professionals in the defense sector who can effectively translate their theoretical knowledge into practice.

9. Competences to be achieved:

Knowledge:
The student is familiar with the Cybersecurity controls and solutions.
The student is familiar with the Cybersecurity-related technologies.

Capabilities:
-

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Endpoint Security-Windows Systems;

11.2. Endpoint Security-Linux Systems ;

11.3. Endpoint Security- Mobile Devices ;

11.4. Endpoint Security-IoT and IIoT Devices ;

11.5. Cloud security;

11.6. Administrative Application Security;

11.7. Data Security;

11.8. Access control;

11.9. Basics of cryptography;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the presence and synchron online sessions. Absences may be made up in justified cases (medical, official), by individual arrangement. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare independently.
In the case of individual study: attendance is not required, but the mid-semester requirements and the colloquium must be fulfilled.

14. Term assignments, testing knowledge

During the course of the semester, students will write two online term papers. The first exam will cover the topics 13.1-13.8, the second exam will cover the topics 13.9-13.14. The final examination is graded on a five-point scale, ranging from 51% satisfactory, 63% moderate, 75% good, 87% excellent. Unsuccessful papers may be retaken in the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and a grade of at least satisfactory in each of the final examination papers are required.

15.2. Evaluation:
The requirement for the written colloquium is based on the knowledge covered in class and the required literature. Based on the successful term papers, a grade is offered based on their average. The student may take the written colloquium instead.
For the written colloquium, the assessment is based on the marks obtained by the student as follows:
0-50% = unsatisfactory (1)
51%-62% = satisfactory (2)

63%-74% = moderate (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits are awarded on the basis of a signature and at least a satisfactory colloquium.

16. Bibliography:

16.1. Compulsory readings:

1. Izzat Alsmadi , Robert Burdwell , Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Al-Qudah, Ahmad Al-Omari: Practical Information Security. A Competency-Based Education Course, Springer, 2017. ISBN: 978-331972119-4, 978-331972118-7, DOI 10.1007/978-3-319-72;

2. William Stallings, Lawrie Brown: Computer Security: Principles and Practice, Pearson, 2017. ISBN: 978-0134794105;

16.2. Recommended readings:

1. Schreiner, Lucas: Information technology: Acquisitions, operations, and cybersecurity, Nova Science Publishers, 2019. ISBN: 978-153616861-7;

2. Alexandrou, Alex: Cybercrime and Information Technology: Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices, Taylor and Francis, 2021. ISBN: 978-100042686-1, 978-036725157-4 DOI 10.4324/9780429318726;

Budapest, 2024

Tamás SZÁDECZKY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁTKTM90

2. Course title: Crisis Management and Communications

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: term mark

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Social Communication

6. Name, position, academic degree of tutor responsible for the curriculum:

Edina KRISKÓ, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (0 EA + 0 SZ + 28 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system. The course work with experiential learning and simulation.

8. The academic content of the subject:

The aim of the course is to acquaint students with the phenomenon of crisis management and crisis communication, its academic literature and techniques primarily through international case studies and media training simulations. After the crisis typologies and historical overview, students will get to know and master the management tasks in line with the stages of critical events, the operation of the media and the crisis management teams considering their responsibilities and effects on the outcomes. Incidents in the course material are all based on real media reports and highlight the specifics of cyber security incidents as potential crises issues. Students learn and practice public speaking and after that, the course ends with information security awareness and fundamental principles of threat communication.

9. Competences to be achieved:

Knowledge:
-

Capabilities:
-

Attitude:
Motivate and encourage people;
Collaborate with other team members and colleagues;

Autonomy and responsibility:
Communicate, present and report to relevant stakeholders;
(Communicate, coordinate and cooperate with internal and external stakeholders;

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. The competence of crisis communication, the theoretical background and principles;

11.2. Public opinion and the media on cyber incidents, communication culture and PR models;

11.3. The importance and possibilities of preventive communication (pre crisis communication);

11.4. Stakeholder analysis and risk assessment;

11.5. The crisis response team and the crisis management system;

11.6. Crisis Management Plan, Crisis Communication Plan (a decision-support framework);

11.7. Responding, rhetorical and incidents-disclosure strategies;

11.8. Communication on processes, losses and the results of the recovery;

11.9. Post Crises Care: Follow Up;

11.10. Case studies and simulations;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

Active participation in the sessions is a condition for signing the attendance sheet. The student must attend at least 75% of the sessions. Failure to sign for more than 25% will result in refusal to sign off from the teacher's side and the course will not be completed.

14. Term assignments, testing knowledge

Students will report on the knowledge they have acquired in a 10.000-11.000 character essay on one of the topics listed in point 11.
The assessment will be graded on a scale of five grades (60 % to satisfactory, 70 % to average, 80 % to good, 90 % to excellent).
In the case of an unsuccessful essay, a correction may be made by means of an oral exam at the end of the term.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

In order to obtain a signature from the teacher as completion of the course three requirements must be met:
1. Active participation in the sessions as described in point 13.
2. The preparation of the report as described in point 14, no later than 7 days

15.2. Evaluation:
The course will end with a practical grade which will be assessed in the same way as the mid-term grade.

15.3. The exact conditions of obtaining credits:
The prerequisite for the acquisition of credits is the obtaining of a signature and at least a satisfactory practical grade.

16. Bibliography:

16.1. Compulsory readings:

1. Kaschner, Holger: Cyber Crisis Management, Springer, Wiesbaden, Germany 2021. ISBN: 978-3-658-35488-6;

2. Agnes, Melissa: Crisis Ready. Building an INVINCIBLE Brand in an Uncertain World, Mascot Books, Herndon, U.S.A. 2018. ISBN: 978-1-68401-413-2;

3. Coleman, Amanda: Crisis Communication Strategies: How to Prepare in Advance, Respond Effectively and Recover in Full, Kogan Page, New York, U.S.A. 2020. ISBN: 9781789662900;

16.2. Recommended readings:

1. Coombs, Timothy W. : Ongoing Crisis Communication: Planning, Managing and Responding, SAGE. ISBN: 978-1-4129-8310-5, SAGE, 2012. ISBN: : 978-1-4129-8310-5;

2. Pursiainen, Christer : The Crisis Management Cycle, Routledge, London and New York 2018. ISBN: 978-1-138-64388-8;

Budapest, 2024

Edina KRISKÓ, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM017

2. Course title: Critical Information Infrastructure Protection

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Tamás SZÁDECZKY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

International and domestic evolution of definitions from the 2000's to present days. Interpretation, relationships, and differences between critical infrastructures and critical information infrastructures. Relevant EU regulatory environment (Directive (EU) 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of networks and information systems across the EU; about ENISA, and information and communications technology related cybersecurity certifications and repealing Regulation No 526/2013 (Cybersecurity Act), and related regulators). Legal environment in Hungary. Authorities and CSIRT's in Hungary. Cybersecurity requirements related to critical information infrastructures.

9. Competences to be achieved:

Knowledge:
The student is familiar with the Cyber threats

Capabilities:
The student is capable of
Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks,
Analyse and comply with cybersecurity-related laws, regulations and legislations,
Implement cybersecurity recommendations and best practices

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Basics of Critical Infrastructure Protection (CIP);

11.2. Basics of Critical Information Infrastructure Protection (CIIP);

11.3. The Critical Entities Resilience Directive (CER);

11.4. Network & Information Security Directive 2 (NIS2);

11.5. Digital Operational Resilience Act (DORA);

11.6. NIST 800-53;

11.7. Sector specific CIIP: Energy;

11.8. Sector specific CIIP: Water;

11.9. Sector specific CIIP: Healthcare;

11.10. Sector specific CIIP: Digital infrastructure;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the presence and synchron online sessions. Absences may be made up in justified cases (medical, official), by individual arrangement. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare independently.
In the case of individual study: attendance is not required, but the mid-semester requirements and the colloquium must be fulfilled.

14. Term assignments, testing knowledge

During the course of the semester, students will write two online term papers. The first exam will cover the topics 13.1-13.8, the second exam will cover the topics 13.9-13.14. The final examination is graded on a five-point scale, ranging from 51% satisfactory, 63% moderate, 75% good, 87% excellent. Unsuccessful papers may be retaken in the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and a grade of at least satisfactory in each of the final examination papers are required.

15.2. Evaluation:
The requirement for the written colloquium is based on the knowledge covered in class and the required literature. Based on the successful term papers, a grade is offered based on their average. The student may take the written colloquium instead.

For the written colloquium, the assessment is based on the marks obtained by the student as follows:
0-50% = unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits are awarded on the basis of a signature and at least a satisfactory colloquium.

16. Bibliography:

16.1. Compulsory readings:

1. Theron, Paula; Bologna, Sandroc: Critical information infrastructure protection and resilience in the ICT sector, IGI Global, USA 2013. ISBN: 978-146662964-6;

2. Hyslop, Maitland: Critical information infrastructures: Resilience and protection, Springer, 2007. ISBN: 978-038771861-3 DOI 10.1007/978-0-387-71862-0;

16.2. Recommended readings:

1. Pomerleau, P.-L., Lowery, D.L.: Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection, Springer, 2020. ISBN: 978-303054054-8, 978-303054053-1, DOI 10.1007/978-3-030-54054-8;

2. Leszczyna, Rafał: Cybersecurity in the Electricity Sector: Managing Critical Infrastructure, Springer, 2019. ISBN: 978-303019538-0, 978-303019537-3, DOI 10.1007/978-3-030-19538-0;

Budapest, 2024

Tamás SZÁDECZKY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF MILITARY SCIENCES AND OFFICER TRAINING

CURRICULUM

1. Course Code: HNBTTM63

2. Course title: Cyber Diplomacy

3. Credit value and course structure:

4.1. 4 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of International Security Studies

6. Name, position, academic degree of tutor responsible for the curriculum:

Dóra MOLNÁR, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 42 (42 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 3

7.3. Further special or unique methods applied throughout of the course:
- holding a small lecture/presentation on a given topic,
- writing a final examination paper,
- completing the Cyberdiplomacy online course at disarmamenteducation.org website (https://www.disarmamenteducation.org/index.php?go=education&do=training-cybe

8. The academic content of the subject:

The primary aim of the course is to provide a comprehensive overview of the main issues in international relations in cyberspace, giving insights into current trends and challenges. Students will learn the basic concepts and contexts of cyber diplomacy that will help them to understand this complex subject and lay the foundation for future professional development. In addition to general trends, the course will also focus on key issues such as the possibilities of legal regulation in the cyberspace, the threats of cyber warfare and cyber espionage, cyber deterrence, international aspects of internet governance, and the activities of various international organisations. Furthermore, the cyber strategy and cyber policy of leading nation states is also presented as a separate unit.

9. Competences to be achieved:

Knowledge:
- knowledge of cyber diplomacy channels, international fora, their work and achievements
- knowledge of the applicability of international law in cyberspace
- knowledge of the cybersecurity strategies of major nation states

Capabilities:
- the ability to understand the drivers of cyber diplomacy
- the ability to understand the current threats in cyberspace and the nation-state responses to them
- the ability to delineate the cyber diplomacy of individual states

Attitude:
- applies the cyber strategy process as part of their work
- independently processes new and complex information, problems and phenomena in a systematic and critical way
- proactively develops and presents alternative, original cyber-diplomatic solutions

Autonomy and responsibility:
- takes responsibility for developing professional proposals based on his/her contextual knowledge of cybersecurity and cyber diplomacy and their knowledge of the relevant legal and regulatory contexts
- takes responsibility for addressing cyber security

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Introduction;

11.2. Regulatory options for cyberspace;

11.3. Cyberspace, cyber diplomacy: basic concepts;

11.4. The dangers of cyber warfare and cyber espionage; cyber deterrence;

11.5. International aspects of internet governance;

11.6. Activities of international organisations in cyberspace;

11.7. Cyberspace in relation to other shared spaces;

11.8. Diplomatic activity of the European Union in cyberspace;

11.9. Cyberdiplomacy on national level I;

11.10. Cyberdiplomacy on national level II;

11.11. Cyberdiplomacy on national level III;

11.11. Cyberdiplomacy on national level IV;

11.13. End-term paper;

11.14. Correction, closing of the semester;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

If there are three onsite occasions during the semester, at least two must be attended. Absences cannot be made up.

14. Term assignments, testing knowledge

- holding a small lecture on a given topic,
- writing a final examination paper,

- completing the Cyberdiplomacy online course at disarmamenteducation.org website (https://www.disarmamenteducation.org/index.php?go=education&do=training-cyberdiplomacy

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

- attending at least two of the three onsite lectures,
- completing the Cyberdiplomacy online course
- holding presentation on the given topic

15.2. Evaluation:

The assessment is based on the result achieved in the term paper.

15.3. The exact conditions of obtaining credits:

Obtaining at least the evaluation/mark (2) pass in the exam.

16. Bibliography:

16.1. Compulsory readings:

1. Molnár Anna Mártonffy Balázs: Cyber Diplomacy from the European Perspective, Ludovika Egyetemi Kiadó, Budapest 2022. ISBN: 9789635318278;

2. Molnár Dóra: Great Power Cyber Diplomacy - China on the International Cyber Platform Accompanied by the Uni-ted States and Russia, Hadtudomány, Budapest 2022.

3. N Schmitt, Michael (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, London 2017. ISBN: 9781316822524;

16.2. Recommended readings:

1. Singer, P. W: Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, Oxford 2014. ISBN: 0199918112;

2. Jochen Rehrl: Handbook on Cyber Security. The Common Security and Defense Policy of the European Union., Federal Ministry of Defence of the Republic of Austria, Vienna 2019. ISBN: 978-3-902275-48-6;

3. EU: Cyber Diplomacy Toolbox, EU, Brussels 2023. ISBN: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf;

Budapest, 2024

Dóra MOLNÁR, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM020

2. Course title: Cyber Threat Intelligence

3. Credit value and course structure:

4.1. 2 credit

4.2. ratio of lectures and seminars: 100 % seminars, 0 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Sándor MAGYAR, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 14 (0 EA + 0 SZ + 14 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 1

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The course will provide students with an understanding of Cyber Threat Intelligence (CTI) and its contribution to strengthening resilience to threats that emerge from cyberspace. The life cycle of CTI will be introduced. Students will be familiarised in detail with the levels of CTI. Students will learn how data and information from different sources are collected and analysed during the activity. The main features of information sharing platforms will be introduced. The course also aims to provide students with the practical skills they need to be able to put their knowledge into practice effectively.

9. Competences to be achieved:

Knowledge:
He/she is familiar with cyber threats.
He/she is familiar with cybersecurity risks.

Capabilities:
He/she is capable of anticipate cybersecurity threats, needs and upcoming challenges.

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. General introduction to Cyber Threat Intelligence (CTI);

11.2. Practical course 1;

11.3. Levels of CTI;

11.4. Practical course 2;

11.5. Processes and cycles of CTI;

11.6. Practical course 3;

11.7. Sources of CTI;

11.8. Practical course 4;

11.9. Methodologies and models used to describe threats;

11.10. Practical course 5;

11.11. Commercial CTI platforms;

11.11. Practical course 6;

11.13. Open source CTI platforms;

11.14. Practical course 7;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

Students must be present for at least 70% of the lessons to be accepted. In case of absence, the student is obliged to obtain the lecture material and to prepare it independently.

14. Term assignments, testing knowledge

Studies are based on attending seminars and reading the required readings.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
A certain percentage of participation in the classes and completion of the mid-term assignments.

15.2. Evaluation:
Written colloquium, five-grade assessment. The colloquium is an evaluation of the theoretical and practical knowledge acquired during the semester.

15.3. The exact conditions of obtaining credits:
To obtain the credits, students must have obtained a signature and at least a satisfactory grade in a colloquium.

16. Bibliography:

16.1. Compulsory readings:

1. Michael Bazzell: OSINT Techniques: Resources for Uncovering Online Information, Independently published (January 1, 2023), 2023. ISBN: 979-8366259064;

2. Siri Bromander: Understanding Cyber Threat Intelligence - Towards Automation, University of Oslo, 2021.

16.2. Recommended readings:

1. Sean Barnum: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™), The MITRE Corporation, 2014.

2. Sagar Samtani: Developing Proactive Cyber Threat Intelligence from the Online Hacker Community: A Computational Design Science Approach, THE UNIVERSITY OF ARIZONA, https://repository.arizona.edu/bitstream/handle/10150/628454/azu_etd_16438_sip1_m.pdf?sequence=1&isAllowed=y 2018.

Budapest, 2024

Sándor MAGYAR, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF MILITARY SCIENCES AND OFFICER TRAINING

CURRICULUM

1. Course Code: HKEHVM69

2. Course title: Cyber Warfare

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Electronic Warfare

6. Name, position, academic degree of tutor responsible for the curriculum:

László KOVÁCS, DSc, professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

Students will learn about the components and possible impact of complex information attacks. This includes discussion of information infrastructures and their vulnerabilities; attack modes; relationships between offensive cyber abilities and cyber-deterrence; and the relationship between cyber warfare and international legal norms. The course also covers components of cyber warfare, which includes exploration and acquisition of information; the methodology of cyberattacks and the links between cyber defense and strategy. It will also highlight the relationships between cyber warfare and information operations; electronic warfare; media coverage and influence, as well as cyber terrorism.

9. Competences to be achieved:

Knowledge:
Familiar with cyber threats.
Familiar with cyber threats.

Capabilities:
-

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Components and possible impact of complex information attacks;

11.2. Information infrastructures and their vulnerabilities;

11.3. Attack modes;

11.4. Relationships between offensive cyber abilities and cyber-deterrence;

11.5. Relationship between cyber warfare and international legal norms;

11.6. Components of cyber warfare, exploration and acquisition of information;

11.7. Methodology of cyberattacks;

11.8. Links between cyber defense and strategy;

11.9. Relationships between cyber warfare and information operations;

11.10. Electronic warfare;

11.11. Media coverage and influence;

11.11. Cyber terrorism;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

Attendance is compulsory for 50% of the presentations, absence from lessons is limited to a maximum of 50%. Make up for absences from lessons by self studying the lesson material and literature and consulting the teacher if necessary.

14. Term assignments, testing knowledge

30-question multiple choice test. Must be reach 50% . Minimum 50% mark is required for a satisfactory grade and a semester assessment.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
At least 50% mark on test is required for a satisfactory grade and a semester assessment.

15.2. Evaluation:
0-50% insufficient (1)
51-60% sufficient (2)
61-70% medium (3)
71-80% good (4)
81-100% excellent (5)

15.3. The exact conditions of obtaining credits:
At least 50% mark on test is required for a satisfactory grade and a semester assessment.

16. Bibliography:

16.1. Compulsory readings:

1. Andress, Jason, Winterfeld, Steve : Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress, NY 2013. ISBN: 978-0124166721;

2. N Schmitt, Michael (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, London 2017. ISBN: 9781316822524;

3. Klimburg, Alexander : National Cyber Security Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2012. ISBN: 978-9949-9211-1-9;

16.2. Recommended readings:

1. Geers, Kenneth : Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015. ISBN: 978-9949-9544-4-5;

2. Kovács László: Cyber Security Policy and Strategy in the European Union and NATO, Revista Academiei Fortelor Terestre / Land Forces Academy Review, Sibiu 2018.

Budapest, 2024

László KOVÁCS, DSc, professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF LAW ENFORCEMENT

CURRICULUM

1. Course Code: RBGVM27

2. Course title: Cybercrime

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Crime, Economic Defence and Cybercrime

6. Name, position, academic degree of tutor responsible for the curriculum:

Réka Eszter GYARAKI, PhD, senior lecturer

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The course aims to provide a comprehensive overview of the characteristics, types and future trends of cybercrime, its material, procedural and international legal aspects. Students will also learn about the criminological aspects of cybercrime. The students will also gain a comprehensive understanding of national and international organisations involved in cybercrime and cybersecurity and their responsibilities. Theoretical knowledge will be acquired through lectures and interactive sessions. In particular, recent changes in legislation and organisations, as well as the possible links between universal (European) and Hungarian cybersecurity and the fight against cybercrime will be discussed during the lectures.

9. Competences to be achieved:

Knowledge:
Is familiar with cybersecurity related laws, regulations and legislations.
Is familiar with procedures in case of cyber attacks
Is familiar with cyber threats
Is familiar with legal, regulatory and legislative compliance requirements, recommendations and best practices
The tasks of investigative authorities in case of attacks against state organs, enterprises and institutions. The procedure of information sharing in case of a crime, and the procedures of covert information gathering.

Capabilities:
Is capable of understanding legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies
Is capable of explaining and communicating data protection and privacy topics to stakeholders and users
He/she is capable of interpreting legal requirements. Furthermore he/she is capable of cooperating with investigative authorities in investigations of cyber security incidents. He/she is capable of drawing complex conclusions in terms of the necessity of

Attitude:
Influence an organisation's cybersecurity culture.
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to support external parties by sharing information generated within the organisation.

Autonomy and responsibility:
Communicate, present and report to relevant stakeholders
Communicate, coordinate and cooperate with internal and external stakeholders
To take responsibility for making professional proposals based on comprehensive knowledge of cybersecurity and dominant legal, regulatory and economical processes and to handle cyber security threats

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Cyber security v. cybercrime: similarities and differences;

11.2. Cybercrime: phenomenology, epidemiology;

11.3. Criminal substantive law: cyber crimes and Budapest Convention;

11.4. Criminal procedural law: evidence and Budapest Convention;

11.5. International public law: Tallinn 2 Manual;

11.6. Analysis of selected issues: deep fakes, crypto assets, LLMs;

11.7. Crimes committed by publishing content (publishing defamatory, defamatory, racist, homophobic content);

11.8. Infringement of Intellectual Property Rights (Copyright Law, 3D printing etc.);

11.9. The appearance of extremist views and content promoting terrorism on the Internet;

11.10. Online crimes related to the sexual development of children (grooming, cyberbullying, cyber mobbing. "Revenge porn", child sexual exploitation materials);

11.11. Attacks against information systems and networks (DDos, Ransomware, malware-attack, defacing);

11.11. Darknet operation and role in committing crimes;

11.13. Online attacks on financial systems and fraud crimes on the Internet;

11.14. Money laundering related to cyberspace;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the sessions. Short/long-term absences can be compensated in justified cases (medical, service), which compensation is made according to individual discussion. Student must prove your absence at the first session following the absence. In case of absence, the student is obliged to obtain the material of the lecture and prepare from it independently.

14. Term assignments, testing knowledge

During the semester, students write two papers in private. The first indoor one checks the topics 13.1-13.7, the second the topics 13.8-13.14. The closed-room thesis is evaluated on a five-point scale as follows: from 51% to sufficient, from 63% to medium, from 75% to good, from 87% to excellent. Unsuccessful homework assignments can be made up in the last study week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
The condition for obtaining a signature is 70% attendance in classes and at least a satisfactory grade for each of the closed assignments.

15.2. Evaluation:
The requirement of the written colloquium is based on the knowledge imparted in the lessons and the compulsory literature. In the case of the written colloquium (exam), the assessment is based on the points achieved by the student in the following way:
0-50% = insufficient (1)
51%-62% = sufficient (2)
63%-74% = medium (3)
75%- 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The condition for obtaining credits is obtaining a signature and at least a sufficient colloquium (exam).

16. Bibliography:

16.1. Compulsory readings:

1. Alexandrou, Alex: Cybercrime and Information Technology: Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices, Taylor and Francis, 2021. ISBN: 978-100042686-1, 978-036725157-4 DOI 10.4324/9780429318726;

16.2. Recommended readings:

Budapest, 2024

Réka Eszter GYARAKI, PhD, senior lecturer

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM012

2. Course title: Cybersecurity Regulations and Standards

3. Credit value and course structure:

4.1. 4 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cybersecurity

6. Name, position, academic degree of tutor responsible for the curriculum:

Tamás SZÁDECZKY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 42 (42 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 3

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The aim of the course is to present the relevant international standards and legal requirements of the European Union along the development of cyber security regulations. The ISO/IEC 27001:2022 Information Security Management Systems Requirements, the Common Criteria for Information Technology Security Evaluation (CC), and the Common Methodology for Information Technology Security Evaluation (CEM) regulations will be detailed. From the legal regulation Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014

9. Competences to be achieved:

Knowledge:
The student is familiar with the Cybersecurity policies,
Cybersecurity standards, methodologies and frameworks,
Cybersecurity recommendations and best practices,
Cybersecurity related laws, regulations and legislations,
Cybersecurity-related certifications,
Legal, regulatory and legislative compliance requirements, recommendations and best practices.

Capabilities:
The student is capable of
Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks,
Analyse and comply with cybersecurity-related laws, regulations and legislations,
Implement cybersecurity recommendations and best practices,
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies.

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Cybersecurity regulation: global scene;

11.2. Cybersecurity regulation: Legal regulation in the USA;

11.3. Cybersecurity regulation: Authorities in the USA;

11.4. Cybersecurity regulation: Legal regulation in the EU (CSA, CRA);

11.5. Cybersecurity regulation: Authorities in the EU (ENISA and member states);

11.6. Cybersecurity standards: Requirements of ISO/IEC 27001;

11.7. Cybersecurity standards: Application of ISO/IEC 27001;

11.8. Cybersecurity standards: Requirements of Common Criteria ISO/IEC 15408;

11.9. Cybersecurity standards: Application of Common Criteria ISO/IEC 15408 ;

11.10. Cybersecurity standards: Requirements of PCI DSS ;

11.11. Cybersecurity standards: Application of PCI DSS ;

11.11. Cybersecurity standards: case study;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the presence and synchron online sessions. Absences may be made up in justified cases (medical, official), by individual arrangement. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare independently.
In the case of individual study: attendance is not required, but the mid-semester requirements and the colloquium must be fulfilled.

14. Term assignments, testing knowledge

During the course of the semester, students will write two online term papers. The first exam will cover the topics 13.1-13.8, the second exam will cover the topics 13.9-13.14. The final examination is graded on a five-point scale, ranging from 51% satisfactory, 63% moderate, 75% good, 87% excellent. Unsuccessful papers may be retaken in the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

To obtain the signature, attendance in class of 70 % and a grade of at least satisfactory in each of the final examination papers are required.

15.2. Evaluation:

The requirement for the written colloquium is based on the knowledge covered in class and the required literature. Based on the successful term papers, a grade is offered based on their average. The student may take the written colloquium instead.
For the written colloquium, the assessment is based on the marks obtained by the student as follows:

0-50% = unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:

The credits are awarded on the basis of a signature and at least a satisfactory colloquium mark.

16. Bibliography:

16.1. Compulsory readings:

1. Zubairi, Junaid Ahmed; Mahboob, Athar: Cyber security standards, practices and industrial applications: Systems and methodologies, IGI Global, 2011. ISBN: 978-160960851-4 DOI 10.4018/978-1-60960-851-4 ;

2. Douglas J. Landoll: Information Security Policies, Procedures, and Standards: A Practitioner's Reference, Auerbach Publications, 2016. ISBN: ISBN 978-1482245899 ;

16.2. Recommended readings:

1. Anne Kohnke, Ken Sigler : Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework, Auerbach Publications, 2017. ISBN: 9781498785143;

2. Schreider Tari: Cybersecurity Law, Standards and Regulations: 2nd Edition, Rothstein Publishing, 2020. ISBN: 978-1944480561;

Budapest, 2024

Tamás SZÁDECZKY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM018

2. Course title: Cybersecurity Strategy and Digital Transformation

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Tamás SZÁDECZKY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The course prepares students to develop an information security strategy, understand the relationship between business objectives, functions and information security. Students will learn about strategic cost planning and reporting procedures required to develop strategic plans, and how to manage costs of security investments. With regard to information security management, and through practical examples they will learn about the roles and responsibilities of information security managers. In terms of control, students will learn the procedures of selecting and implementing key metrics (KPIs), and about the methods to control them.

9. Competences to be achieved:

Knowledge:
The student is familiar with the
Resource management,
Management practices

Capabilities:
The student is capable to
Manage cybersecurity resources,
Develop, champion and lead the execution of a cybersecurity strategy,

Anticipate required changes to the organisation’s information security strategy and formulate new plans,
Define and apply maturity models for cybersecurity management,
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards’ requirements,

Attitude:
Influence an organisation’s cybersecurity culture

Autonomy and responsibility:
Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Concept of leadership. The difference between leadership and management;

11.2. Leadership theories;

11.3. Organizational theory and design;

11.4. People in the organization;

11.5. Project management;

11.6. Information Security Management System;

11.7. Defining an information security strategy;

11.8. Governance of information security, strategy implementation;

11.9. Strategic planning;

11.10. Cost planning and reporting;

11.11. Organizational Structures;

11.11. Metrics and measurement;

11.13. Audit;

11.14. Digital transformation;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the presence and synchron online sessions. Absences may be made up in justified cases (medical, official), by individual arrangement. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare independently.
In the case of individual study: attendance is not required, but the mid-semester requirements and the colloquium must be fulfilled.

14. Term assignments, testing knowledge

During the course of the semester, students will write two online term papers. The first exam will cover the topics 13.1-13.8, the second exam will cover the topics 13.9-13.14. The final examination is graded on a five-point scale, ranging from 51% satisfactory, 63% moderate, 75% good, 87% excellent. Unsuccessful papers may be retaken in the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and a grade of at least satisfactory in each of the final examination papers are required.

15.2. Evaluation:
The requirement for the written colloquium is based on the knowledge covered in class and the required literature. Based on the successful term papers, a grade is offered based on their average. The student may take the written colloquium instead.
For the written colloquium, the assessment is based on the marks obtained by the student as follows:
0-50% = unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits are awarded on the basis of a signature and at least a satisfactory colloquium.

16. Bibliography:

16.1. Compulsory readings:

1. Karolin Frankenberger, Hannah Mayer, Andreas Reiter, Markus Schmidt: The Digital Transformer's Dilemma: How to Energize Your Core Business While Building Disruptive Products and Services, Wiley, 2020. ISBN: 978-1119701309;

2. Falco, Gregory; Rosenbach, Eric: Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity, Oxford University Press, 2021. ISBN: 978-019752654-5 DOI 10.1093/oso/9780197526545.001.0001;

16.2. Recommended readings:

1. Yigal Behar: Digital War: The One Cybersecurity Strategy You Need to Implement Now to Secure Your Business, CreateSpace Independent Publishing Platform, 2017. ISBN: 1548459712;

2. Laudon, Kenneth C; Laudon, Jane: Management Information Systems: Managing the Digital Firm, Pearson, 16th Edition 2020. ISBN: 978-0135191798;

Budapest, 2024

Tamás SZÁDECZKY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF LAW ENFORCEMENT

CURRICULUM

1. Course Code: NPNBM53

2. Course title: Human Factors of Cybersecurity

3. Credit value and course structure:

4.1. 4 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Civil National Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Imre DOBÁK, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 42 (42 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 3

7.3. Further special or unique methods applied throughout of the course:
Preparation of project tasks (Individual and team work). Working on sub-themes through independent work. Drawing conclusions from the analysis of statistical data. This subject is a part of a blended learning program, thus a major part of the lectures is

8. The academic content of the subject:

Using a social science approach, the course examines the significance of human factor in cyber security and introduces students to the idea of "human-based" vulnerability, as well as influence and deception related to cyberspace. It deals with the growing role of awareness, its methods and options. In the context of "social engineering" (SE), types of attacks based on the exploitation of the human factor, it examines the significance of human risks, the human-based methods, techniques, goals of attacks, and the possibilities of defense as a separate topic. In the area of human factors of information security, it strengthens the development of security-conscious professional thinking through case studies and examples. Related to the psychological issues, it discusses the elements of deception and influence in cyberspace, the observable processes, the psychological operations, the collection and dissemination of information, the specifics of fake news and disinformation, their presence, possible effects, and the possible aspects of treatments. It covers the phenomenon through examples and case studies, with particular attention to the role of social media.

9. Competences to be achieved:

Knowledge:
- He/She is familiar with the importance of human factors in cybersecurity
- He/She is familiar with the role of the human factor in the execution of cyber attacks

Capabilities:
- He/she is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans.
- He/she is capable of assessing cybersecurity risks posed by internal employees.
- He/she is capable of creating regulations to handle threats posed by internal employees.

Attitude:
- He/She is motivated to take effective measures to prevent cyber-attacks, which means reducing the organisation's exposure.
- He/She is able to treat internal staff as high risk and design information security processes accordingly.

Autonomy and responsibility:
- He/She integrates and applies the results of ongoing research in the field of cybersecurity.
- He is open to handle responsibly the cyber security threats.
- He/She is ready to incorporate and apply the results of ongoing research in the field of cybers

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. The human side of cybersecurity, the role of human factor;

11.2. Players and attackers in the cyberspace;

11.3. Information gathering in cyberspace ;

11.4. Attacking techniques and forms based on human factors, Social Engineering, Case Studies (Interpreting and processing examples) ;

11.5. Social networking sites, online space, platforms - possibilities of influencing personality;

11.6. Internet, social media, phone, game addiction ;

11.7. Understanding and Significance of Psychological Operations in Cyberspace;

11.8. Objectives and actors of psychological operations with a view to (national) security ;

11.9. Phenomenon of influence, its possible aims and peculiarities ;

11.10. Possibilities, techniques, international examples of deception, characteristics, goals, and effects of fake news, fight against fake news;

11.11. Case Studies (Interpreting and processing examples);

11.11. Importance of awareness, role of education ;

11.13. Framework for security awareness programmes;

11.14. Security awareness program - implementation of a practical project task;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the sessions.

14. Term assignments, testing knowledge

During the semester, students should
- produce a short presentation (video) on topics 1-4 (individual project assignment) (20% of the total grade, 1-5 marks)
- prepare a research outline based on individual research on topics 5-6, aiming at exploring deeper contexts, formulating hypotheses, identifying possible research methods (20% of the total mark) (20% of the total mark, 1-5 marks)
- in topics 7 to 11, work individually on a case study, interpret it and draw conclusions (20% of total assessment) (20% of total assessment, 1-5 marks)
- preparation of an awareness programme, incorporation of the learning material for topics 1-11 (50% of the total mark (1 to 5 marks)

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

To obtain the signature, the student must attend at least 70% of the lessons and complete at least 80% of the requirements with a mark of 2 or better.

15.2. Evaluation:

The requirements for the exam are based on the knowledge taught in class, individual research and the required literature.
In the case of a written examination, the exam mark is based on the following:
0-50% = fail (1)
51%-62% = pass (2)
63%-74% = satisfactory (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:

Obtaining a signature and passing at least a "pass" exam.

16. Bibliography:

16.1. Compulsory readings:

1. Rashid A., Chivers H., Danezis G., Lupu E., Martin A.: The Cyber Security Body of Knowledge (CyBOK Version 1.0), The National Cyber Security Centre , UK 2019.

2. Wilson, M. and Hash, J.: Building an Information Technology Security Awareness and Training Program, Computer Security, Computersecurity NIST Special Publication 800-50, 2003.

3. Christopher Hadnagy: Social Engineering: The Science of Human Hacking, Wiley, 2018. ISBN: 978-1-119-43373-6 (ebk);

16.2. Recommended readings:

1. Young, Heather - Vliet, Tony - Ven, Josine - Jol, Steven - Broekman, Carlijn: Understanding Human Factors in Cyber Security as a Dynamic System (In: D. Nicholson (ed.), Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing 593, DOI 10.1007/978-3-319-605)85-2_23, Springer, 2018.

2. Raef Meeuwisse: How to Hack a Human: Cybersecurity for the Mind, Cyber Simplicity Limited, 2019. ISBN: 9781911452232;

3. Rantos, K., Fysarakis, K., and Manifavas, C.: How effective is your security awareness program? An evaluation methodology, Information Security Journal 21(6), 2012. ISBN: https://doi.org/10.1080/19393555.2012.747234;

Budapest, 2024

Imre DOBÁK, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM019

2. Course title: Incident Management

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Csaba KRASZNAY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (14 EA + 0 SZ + 14 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The goal of this course is to introduce the basics and procedures of incident management for the students. In details, it discusses the qualification of incidents, components of incident response, the setup and role of the organization responsible for incident management. It introduces the national and international CERT/CSIRT network. It also includes the design questions of business continuity. The lecture highlights incident information sharing with official and private actors. On the practice lessons, technical tools of incident management are presented, that are used by the students to solve case studies.

9. Competences to be achieved:

Knowledge:
- Cybersecurity risks
- Monitoring, testing and evaluating cybersecurity controls' effectiveness

Capabilities:
-

Attitude:
- Collaborate with other team members and colleagues

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Theory of incident management;

11.2. Legal background of incident management;

11.3. Organizational background of incident management in Hungary and internationally, CERT/CSIRT;

11.4. Security Operation Centers;

11.5. Technical tools of incident management, log sources;

11.6. Log analysis, SIEM systems;

11.7. EDR, XDR, MDR;

11.8. Incident information sharing, CTI;

11.9. Artificial Intelligence in incident management;

11.10. Business continuity planning;

11.11. Definition of security event, problem and incident, practical examples;

11.11. Incident related case studies;

11.13. Setup of an incident management team;

11.14. Incident management in practice, TTX;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the lectures. Short/lasting absences may be made up in justified cases (medical, official), which will be discussed individually. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare it individually.

14. Term assignments, testing knowledge

Students will be given individual study material for each lecture, which will be checked at the beginning of the next lecture: 5 test questions per day, each of which must be passed with a minimum of 60%.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

To obtain the signature, attendance in class of 70 % and, in the case of the examinations under point 16, the minimum results specified must be achieved.

15.2. Evaluation:

The written examination is based on the knowledge acquired in the lessons and the compulsory literature. For the written examination, the assessment is based on the marks obtained by the student as follows:
0-50%= unsatisfactory (1)
51%-62% = satisfactory (2)

63%-74% = moderate (3)
75%- 86%= good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits can be obtained by obtaining a signature and at least a satisfactory colloquium (K).

16. Bibliography:

16.1. Compulsory readings:

1. Arun E. Thomas: Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence, CreateSpace Independent Publishing Platform, 2018. ISBN: 978-1986862011;

2. Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, 2014. ISBN: 978-0071798686;

16.2. Recommended readings:

1. Thompson, Eric C.: Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents, Apress, 2018. ISBN: 978-1484238691;

2. Whitman, Michael E., Mattord, Herbert J., Green, Andrew: Principles of Incident Response and Disaster Recovery, Cengage Learning, 2013. ISBN: 978-1111138059;

Budapest, 2024

Csaba KRASZNAY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM013

2. Course title: Introduction to Cybersecurity

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 0 % seminars, 100 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cybersecurity

6. Name, position, academic degree of tutor responsible for the curriculum:

Csaba KRASZNAY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The aim of the course is to provide an insight into the basics of cybersecurity. Throughout the semester, students will learn about the evolution of the cyberspace threat environment and the development of the information security and cybersecurity profession from the prehistory of computing. They will learn the basic conceptual and mathematical principles that are frequently encountered in the field. In doing so, the lecture will also cover the most important information security protection models. Finally, the main information security standards will be discussed, with a description of their basic conceptual framework, to lay the foundations for further subjects.

9. Competences to be achieved:

Knowledge:
- Ethical cybersecurity organisation requirements
- Cybersecurity maturity models
- Cybersecurity procedures

Capabilities:
- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
- Review and enhance security documents, reports, SLAs and ensure the security objectives

- Identify and solve cybersecurity-related issues
- Establish a cybersecurity plan

Attitude:
- Understand, practice and adhere to ethical requirements and standards

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. General Security Concepts;

11.2. Threat actors, motivations and attack vectors;

11.3. Vulnerabilities and exploits;

11.4. Mitigation techniques;

11.5. Security architectures and infrastructures;

11.6. Data security and infrastructure resilience;

11.7. Security techniques and secure lifecycle in operations;

11.8. Vulnerability and incident management;

11.9. Tools of enterprise network and endpoint protection, identity and access management;

11.10. Security orchestration, automation and response;

11.11. Security governance and risk management;

11.11. Compliance and supply chain security;

11.13. Security audits and awareness trainings;

11.14. Summary, the actual trends of cyberattacks and cyberdefense;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the lectures. Short/lasting absences may be made up in justified cases (medical, official), which will be discussed individually. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare it individually.

14. Term assignments, testing knowledge

Students will be given individual study material for each lecture, which will be checked at the beginning of the next lecture: 5 test questions per day, each of which must be passed with a minimum of 60%.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and, in the case of the examinations under point 16, the minimum results specified must be achieved.

15.2. Evaluation:
The written examination is based on the knowledge acquired in the lessons and the compulsory literature. For the written examination, the assessment is based on the marks obtained by the student as follows:
0-50%= unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75%- 86%= good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits can be obtained by obtaining a signature and at least a satisfactory colloquium (K).

16. Bibliography:

16.1. Compulsory readings:

1. William Stallings, Lawrie Brown: Computer Security: Principles and Practice, Pearson, 2017. ISBN: 978-0134794105;

2. Joe Shelley, Darril Gibson : CompTIA Security+ Get Certified Get Ahead: SY0-701 Study Guide, Certification Experts, LLC, 2023. ISBN: 979-8988984801;

16.2. Recommended readings:

1. Schneier, Bruce: We Have Root, Wiley, 2019. ISBN: 978-1-119-64301-2;

2. Howard, Rick: Cybersecurity First Principles: A Reboot of Strategy and Tactics, Wiley, 2023. ISBN: 978-1-394-17309-9;

Budapest, 2024
Csaba KRASZNAY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF MILITARY SCIENCES AND OFFICER TRAINING

CURRICULUM

1. Course Code: HKHIRA100

2. Course title: IT System and Network Security

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 50 % seminars, 50 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Intelligence

6. Name, position, academic degree of tutor responsible for the curriculum:

András TÓTH, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (28 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The aim of this course is to provide a comprehensive knowledge of the structure and operation of computer networks. In this course, students will learn about network infrastructure, network protocols and communication, network connectivity, the OSI model, the TCP/IP model, the Ethernet standard, network, transport and application layer functions, IPv4 and IPv6 addressing, IP subnet design and construction. The curriculum includes introduction to switched networks, switching basics and configuration, routing basics, static traffic management, dynamic traffic management, DHCP, IPv4 network address translation (NAT). It covers VLAN design and traffic management options, configuration and implementation of IPv4 and IPv6 access control lists, characteristics of different WAN technologies, their advantages, description of virtual private network (VPN) operation. It provides a comprehensive theoretical and practical understanding of the configuration and troubleshooting of network connections, in particular network diagnostics, the basics of authentication and encryption protocols, and the use of proxies and firewalls. It includes an introduction to the network services and configuration of Windows and Linux operating systems. Students will cover active and passive methods of network traffic analysis, wireless network performance testing, comparative measurement of Ethernet standards, protocol analyzer testing of network devices (HUB, switch, router, firewall, proxy), network device load testing, and functional testing of network devices. In addition, IP traffic encryption options (network, transport, application layer options) will be covered, including a practical examination of firewall types and functions.

9. Competences to be achieved:

Knowledge:
Defence solutions against cyber attacks. Familiar with the procedures applicable in case of a cyber attack.

Capabilities:
He/she is capable of taking defensive measures that ensure the reduction of risk resulting from threat against humans. Moreover he/she is capable of taking technological defensive measures related to elements of the cyber kill chain. Furthermore has the capability and understanding of the current threats of cyberspace. He/she is capable of supporting his/her organisation and external parties in handling a cyber attack.

Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

Autonomy and responsibility:
To implement advanced knowledge characterising cybersecurity on a national and international level. To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of profess

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Introduction to networks: Introduce students to network infrastructure, OSI model, TCP/IP model, Ethernet standard, network protocols and communication, network layer functions, transport layer functions, IPv4 addressing, IP subnet design and construction);

11.2. Fundamentals of traffic management and switching: Introduction to switched networks, switching basics and configuration, basics of traffic routing, static traffic routing, dynamic traffic routing, DHCP, IPv4 network address translation (NAT);

11.3. Interconnecting networks: VLAN design and traffic routing options, configuring and implementing IPv4 access control lists, introducing the features of different WAN technologies, defining their benefits, and describing how virtual private networks (VPNs);

11.4. Security solutions: To provide students with a comprehensive theoretical and practical knowledge of the configuration and troubleshooting options for network connections, particularly network diagnostics, the basics of authentication and encryption protoc;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the sessions. Short/lasting absences may be made up in justified cases (medical, official), which will be discussed individually. The absence must be certified at the first session following the absence. In the case of a student's absence, it is deemed necessary that they familiarize themselves with the lecture material uploaded on Moodle and complete the practical task independently. However, in case of any queries or clarifications needed for the practical task, students may schedule a pre-arranged consultation with their instructor.

14. Term assignments, testing knowledge

During the semester, students write two exams. The first exam will cover the first two topics, the second exam will cover the second two topics. The exam is graded on a five-point scale, ranging from 51% satisfactory, 63% average, 75% good, 87% excellent. Unsuccessful exams can be re-submitted during the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain a signature, students must have 70% attendance in class and at least a satisfactory grade in each of the exams.

15.2. Evaluation:
The exam is graded on a five-point scale, ranging from 51% satisfactory, 63% average, 75% good, 87% excellent.

15.3. The exact conditions of obtaining credits:
To obtain credits, you must obtain the signature.

16. Bibliography:

16.1. Compulsory readings:

1. Andrew Tanenbaum, Nick Feamster, David Wetherall : Computer Networks,. ISBN: 9781292374062;

2. Mike Meyers : CompTIA Network+ Certification All-in-One Exam Guide,. ISBN: 9781260122381;

3. James Kurose, Keith Ross : Computer Networking: A Top-Down Approach, A Top-Down Approach, 2016. ISBN: 9780133594140;

16.2. Recommended readings:

1. Gary A. Donahue : Network Warrior,. ISBN: 9781449387860;

2. Jason Edelman , Scott Lowe , Matt Oswalt : Network Programmability and Automation,. ISBN: 9781491931257;

3. Jill West, Tamara Dean, Jean Andrews : Network+ Guide to Networks (Comptia Network+),. ISBN: 9781337569330;

Budapest, 2024

András TÓTH, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM015

2. Course title: Personal Data Protection

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 100 % seminars, 0 % lectures

4.3. grading: term mark

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Tamás SZÁDECZKY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (0 EA + 0 SZ + 28 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The students will acquire comprehensive and in-depth knowledge of data protection, the data processing in the public and private sectors, and will learn about national and international laws legal practices. The approach of the subject is to address different data protection systems of some countries in Europe, America and Asia. Relevant legal cases will be presented and discussed.

9. Competences to be achieved:

Knowledge:
Privacy impact assessment standards, methodologies and frameworks

Capabilities:
- Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy,
- Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties,
- Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools,
- Explain and communicate data protection and privacy topics to stakeholders and users,

Attitude:
-

Autonomy and responsibility:
-

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Data Protection as a fundamental right;

11.2. Purpose of Personal Data Protection;

11.3. The European General Data Protection Regulation (GDPR);

11.4. Material Scope of Application and Territorial Scope of Application of GDPR;

11.5. Basic Principles of GDPR;

11.6. Compliance and Consequences of Non-compliance;

11.7. In-depth: The Role of the Data Protection Autority and the Data Protection Officer;

11.8. In-depth: Privacy Impact Assessment;

11.9. In-depth: Data Breaches and Data Breach Notifications;

11.10. Case studies;

11.11. Comparing European and American / Asian Data Protection Concepts;

11.11. USA: The California Consumer Privacy Act (and other US Data Protection Laws);

11.13. India: The Indian Digital Personal Data Protection Act (2023);

11.14. Current Issues in Data Protection (e.g. Data Protection and AI, Whistleblowing, Cross Border Data Transfer);

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the presence and synchron online sessions. Absences may be made up in justified cases (medical, official), by individual arrangement. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare independently.
In the case of individual study: attendance is not required, but the mid-semester requirements and the colloquium must be fulfilled.

14. Term assignments, testing knowledge

During the course of the semester, students will write two online term papers. The first exam will cover the topics 13.1-13.8, the second exam will cover the topics 13.9-13.14. The final examination is graded on a five-point scale, ranging from 51% satisfactory, 63% moderate, 75% good, 87% excellent. Unsuccessful papers may be retaken in the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and a grade of at least satisfactory in each of the final examination papers are required.

15.2. Evaluation:
The requirement for the term mark is the two passing term papaers.
The assessment is based on the marks obtained by the student as follows:
0-50% = unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75% - 86% = good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits are awarded on the basis of a signature and the passing term mark.

16. Bibliography:

16.1. Compulsory readings:

1. Lothar Determann: Determann's field guide to data privacy law : international corporate compliance, Edward Elgar, Cheltenham 2022. ISBN: 9781802202922;

2. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler, Luca Tosoni: The EU General Data Protection Regulation: A Commentary/Update of Selected Articles, SSRN, 2021. ISBN: http://dx.doi.org/10.2139/ssrn.3839645;

16.2. Recommended readings:

1. Walters, Robert; Novak, Marko: Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer Nature, 2021. ISBN: https://doi.org/10.1007/978-981-16-1665-5;

2. Gloria González, Rosamunde Van Brakel, and Paul De Hert: Research Handbook on Privacy and Data Protection Law, Edward Elgar, Gloucestershire 2022. ISBN: https://doi.org/10.4337/9781786438515;

Budapest, 2024

Tamás SZÁDECZKY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES

CURRICULUM

1. Course Code: ÁKIBTM016

2. Course title: Risk Assessment, Risk Management

3. Credit value and course structure:

4.1. 4 credit

4.2. ratio of lectures and seminars: 33 % seminars, 67 % lectures

4.3. grading: exam

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of Cyber Security

6. Name, position, academic degree of tutor responsible for the curriculum:

Csaba KRASZNAY, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 42 (42 EA + 0 SZ + 0 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 3

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The goal of the course is to introduce information security risk analysis and risk management. In this context, the student will become familiar with the conceptual toolkit used in the standards, in particular ISO 31000 and 27005, which are general and information security risk management standards. Students will acquire quantitative, qualitative and semi-quantitative solutions to risk assessment. The risk assessment options and algorithms are reviewed. The lecture introduces risk management frameworks such as COBIT5 - RiskIT, ITILv3, Octave, ISO 73, ISO / IEC 31000, ISO 13335, NIST 800-53 and detailed analysis of the Act L of 2013 and CISM-based risk management. As practice, risk assessment case studies are developed, students prepare risk scenarios and prepare risk management plans, including asset inventories and vulnerability analysis.

9. Competences to be achieved:

Knowledge:
- Risk management standards, methodologies and frameworks
- Risk management tools
- Risk management recommendations and best practices

Capabilities:
- Assess and enhance an organisation’s cybersecurity posture

- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
- Analyse and consolidate organisation's quality and risk management practices
- Build a cybersecurity risk-aware environment

Attitude:
-

Autonomy and responsibility:
- Propose and manage risk-sharing options

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Organizational governance;

11.2. Risk governance I.;

11.3. Risk governance II.;

11.4. Risk identification;

11.5. Risk analysis;

11.6. Risk evaluation;

11.7. Risk response;

11.8. Control design;

11.9. Control implementation;

11.10. Risk monitoring;

11.11. Risk reporting;

11.11. Risk management standards;

11.13. Role of risk management in the ISMS;

11.14. Summary;

12.the subject/its position in the curriculum of the term:

1. semester/autumn;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the lectures. Short/lasting absences may be made up in justified cases (medical, official), which will be discussed individually. The absence must be certified at the first session following the absence. In the case of absence, the student is obliged to obtain the lecture material and to prepare it individually.

14. Term assignments, testing knowledge

Students will be given individual study material for each lecture, which will be checked at the beginning of the next lecture: 5 test questions per day, each of which must be passed with a minimum of 60%.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:
To obtain the signature, attendance in class of 70 % and, in the case of the examinations under point 16, the minimum results specified must be achieved.

15.2. Evaluation:
The written examination is based on the knowledge acquired in the lessons and the compulsory literature. For the written examination, the assessment is based on the marks obtained by the student as follows:
0-50%= unsatisfactory (1)
51%-62% = satisfactory (2)
63%-74% = moderate (3)
75%- 86%= good (4)
87%-100% = excellent (5)

15.3. The exact conditions of obtaining credits:
The credits can be obtained by obtaining a signature and at least a satisfactory colloquium (K).

16. Bibliography:

16.1. Compulsory readings:

1. ISACA: CRISC Official Review Manual, 7th Edition Revised, ISACA, 2023. ISBN: 978-1604209778;

2. Evan Wheeler: Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngress, 2011. ISBN: 978-1597496155;

16.2. Recommended readings:

1. Mark Talabis: Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress, 2012. ISBN: 978-1597497350;

2. Hubbard, Douglas W., Seiersen, Richard: How to Measure Anything in Cybersecurity Risk, Wiley, 2023. ISBN: 9781119085294;

Budapest, 2024

Csaba KRASZNAY, PhD, associate professor

LUDOVIKA UNIVERSITY OF PUBLIC SERVICE
FACULTY OF MILITARY SCIENCES AND OFFICER
TRAINING

CURRICULUM

1. Course Code: HKHIRA101

2. Course title: Security Testing and Forensics

3. Credit value and course structure:

4.1. 3 credit

4.2. ratio of lectures and seminars: 100 % seminars, 0 % lectures

4.3. grading: term mark

4. Name of major(s), specializations (where it is taught):

5.1. International Cyber Security Studies MA;

5. Name of organizational unit responsible for its education:

Department of News

6. Name, position, academic degree of tutor responsible for the curriculum:

András TÓTH, PhD, associate professor

7. Number and types of classes

7.1. full number of classes/semester:

7.1.1. full time course: 28 (0 EA + 0 SZ + 28 GY)

7.1.2. part time course: 0 (0 EA + 0 SZ + 0 GY)

7.2. weekly number of classes - full time course: 2

7.3. Further special or unique methods applied throughout of the course:
This subject is a part of a blended learning program, thus a major part of the lectures is in an online format. The exact schedule is in the Neptun system.

8. The academic content of the subject:

The objective of the course is to introduce students to the planning, execution and documentation of security testing of information systems. During laboratory exercises, students will learn the steps of designing and setting up a security test lab, different methodologies for security testing of IT systems, types of vulnerability scans and the steps of their implementation. They will learn about the main types of security testing methodologies that can be used in the development, integration and operational verification of IT systems. They will gain practical knowledge of the possibilities of security device testing, the "classic" life cycle of network attacks, local and remote vulnerability scanning and exploitation methods. They will learn about the role, advantages and disadvantages of automated vulnerability scanning, steps to interpret and validate results, options for testing applications and services on Windows and Linux operating systems, security testing of web services and databases, user security awareness testing, wireless systems testing methodology, embedded systems testing options, mobile devices (smart devices) testing options, and security testing team communication and test documentation options, as well as individual and group training and self-training options. The course will also cover the legal and professional recording of electronic evidence, which is essential for the detection of security-related crimes and incidents, and the criminological and forensic knowledge of this.

9. Competences to be achieved:

Knowledge:
Defence solutions against cyber attacks, and the concept and mode of action of malware codes.

Capabilities:
He/she is capable of taking technological defensive measures related to elements of the cyber kill chain. Moreover he/she is capable of understanding the current threats of cyberspace. Therefore he/she is capable of supporting his/her organisation in developing cyber security skills.

Attitude:
An effort to take effective measures in order to prevent cyber attacks, by this means reducing the exposure of his/her organisation. An ability to cooperate in preventing his/her organisation and him/herself from becoming a victim of a cyber attack.

Autonomy and responsibility:
To obtain, evaluate and utilize theoretical, scientific and practical information necessary for the improvement of the field and the methodology of professional practice. Furthermore to take the initiative in converting technical and operational tasks int

10. Required previous studies:

-

11. Description of the subject, curriculum:

11.1. Steps to design and build a security test lab;

11.2. Different methodologies for security testing of IT systems;

11.3. Functional safety testing, Vulnerability testing, Penetration testing;

11.4. Local and remote vulnerability discovery and exploitation;

11.5. Opportunities for testing applications, services, web services and databases;

11.6. User safety awareness tests;

11.7. Methodology for testing wireless systems, opportunities for testing mobile devices (smart devices);

11.8. Possibilities of testing embedded systems;

11.9. Individual and group opportunities for further education and self-education;

11.10. The concept of evidence and means of proof, concept of electronic data and digital data in law;

11.11. Sources of evidence in cyberspace;

11.11. Knowledge of digital devices;

11.13. Legal Provisions of research and seizure in computer and cyberspace;

11.14. Issues of digital forensic and criminal methodology of digital tracking;

12.the subject/its position in the curriculum of the term:

2. semester/spring;

13. Requirements of attendance, acceptable absence, opportunity for making up missed classes:

The student must attend at least 70% of the sessions. Short/lasting absences may be made up in justified cases (medical, official), which will be discussed individually. The absence must be certified at the first session following the absence. In the case of a student's absence, it is deemed necessary that they familiarize themselves with the lecture material uploaded on Moodle and complete the practical task independently. However, in case of any queries or clarifications needed for the practical task, students may schedule a pre-arranged consultation with their instructor.

14. Term assignments, testing knowledge

During the semester, students write two exams. The first exam will cover the first two topics, the second exam will cover the second two topics. The exam is graded on a five-point scale, ranging from 51% satisfactory, 63% average, 75% good, 87% excellent. Unsuccessful exams can be re-submitted during the last week of the semester.

15. The exact conditions of testing knowledge, obtaining signature or credits:

15.1. The exact conditions of obtaining signature:

To obtain a signature, students must have 70% attendance in class and at least a satisfactory grade in each of the exams.

15.2. Evaluation:

The exam is graded on a five-point scale, ranging from 51% satisfactory, 63% average, 75% good, 87% excellent.

15.3. The exact conditions of obtaining credits:

To obtain credits, you must obtain the signature.

16. Bibliography:

16.1. Compulsory readings:

1. Hertzog, Raphael, O'Gorman, Jim : Kali Linux Revealed: Mastering the Penetration Testing Distribution,. ISBN: 9780997615609;

2. Kim, Peter : The Hacker Playbook 3: Practical Guide To Penetration Testing,. ISBN: 9781980901754;

3. Gus Khawaja : Kali Linux Penetration Testing, 2021. ISBN: 978-1119719083;

4. Radhi Shatob: Penetration Testing: Step By Step Guide, 2020. ISBN: 978-1999541248;

16.2. Recommended readings:

1. OWASP recommendations,.

2. RTFM - Red Team Field Manual,.

3. PCI Data Security Standard (PCI DSS) - Information Supplement:Penetration Testing Guidance,.

4. Open Source Security Testing Methodology Manual – OSSTMM,.

5. CISA: Known Exploited Vulnerabilities Catalog,.

Budapest, 2024

András TÓTH, PhD, associate professor

Annex 1. The class-, credits- and exams-plans

CURRICULUM PLAN
INTERNATIONAL CYBERSECURITY STUDIES MA
from Academic Year 2024/2025.
Full Time Training

Course unit type	Course type	Course title	Semester												Total						RESPONSIBLE ORGANIZATIONAL UNIT	RESPONSIBLE INSTRUCTOR
			1.						2.													
			Lecture		Seminar				Lecture		Seminar				Lecture		Seminar					
			classes/week	classes/semester	classes/week	classes/semester	credit	evaluation	classes/week	classes/semester	classes/week	classes/semester	credit	evaluation	classes/week	classes/semester	classes/week	classes/semester	credit	lectures + seminars total / week		
		General course units																				
ÁKIBTM012	O	Cybersecurity Regulations and Standards	3	42			4	K							3	42			4	3	ÁNTK KBT	Szádeczky Tamás
ÁKIBTM013	O	Introduction to Cybersecurity	2	28			3	K							2	28			3	2	ÁNTK KBT	Krasznay Csaba
HKEHVM69	O	Cyber Warfare	2	28			3	K							2	28			3	2	HHK EHT	Kovács László
ÁKIBTM014	O	Applied Cybersecurity Technologies	2	28			3	K							2	28			3	2	ÁNTK KBT	Szádeczky Tamás
ÁKIBTM015	O	Personal Data Protection			2	28	3	GYJ									2	28	3	2	ÁNTK KBT	Péterfalvi Attila
ÁKIBTM016	O	Risk Assessment, Risk Management	3	42			4	K							3	42			4	3	ÁNTK KBT	Krasznay Csaba
ÁKIBTM017	O	Critical Information Infrastructure Protection	2	28			3	K							2	28			3	2	ÁNTK KBT	Szádeczky Tamás
RBGVM27	O	Cybercrime	2	28			3	K							2	28			3	2	RTK BGKET	Gyaraki Réka
HKHIRA100	O	IT System and Network Security	2	28			3	K							2	28			3	2	HHK HT	Tóth András
HNBTTM63	O	Cyber Diplomacy							3	42			4	K	3	42			4	3	HHK NBTT	Molnár Dóra
ÁKIBTM018	O	Cybersecurity Strategy and Digital Transformation							2	28			3	K	2	28			3	2	ÁNTK KBT	Szádeczky Tamás
ÁTKTM90	O	Crisis Management and Communications									2	28	3	GYJ			2	28	3	2	ÁNTK TKT	Kriskó Edina
NPNBM53	O	Human Factors of Cybersecurity							3	42			4	K	3	42			4	3	RTK PNBT	Dobák Imre
ÁKIBTM019	O	Incident Management							1	14	1	14	3	K	1	14	1	14	3	2	ÁNTK KBT	Krasznay Csaba
ÁKIBTM020	O	Cyber Threat Intelligence									1	14	2	K			1	14	2	1	ÁNTK KBT	Magyar Sándor
HKHIRA101	O	Security Testing and Forensics									2	28	3	GYJ			2	28	3	2	HHK HT	Tóth András
	E	Optional course-unit 1.									2	28	2	GYJ			2	28	2	2		
	E	Optional course-unit 2.									2	28	2	GYJ			2	28	2	2		
		General course units total	18	252	2	28	29	x	9	126	10	140	26	x	27	378	12	168	55	39		
		Couse units without credits:																				
		Couse units without credits:	0	0	0	0	x	x	0	0	0	0	x	x	0	0	0	0	x	0		
		Degree thesis course unit																				
ÁKIBTM021	O	Degree Thesis									6	84	5	GYJ			6	84	5	10	ÁNTK KBT	Szádeczky Tamás
		Degree thesis course units total	0	0	0	0	0	x	0	0	6	84	5	x	0	0	6	84	5	10		
		TOTAL COURSE UNITS IN CURRICULUM	18	252	2	28	29	x	9	126	16	224	31	x	27	378	18	252	60	49		
		EVALUATION SUMMARY																				
		Practical mark (GYJ)						1						5						6		
		Exam (K)						8						5						13		
		TOTAL EVALUATIONS / SEMESTER						9						10						19		

Annex 2. - Previous study requirements

INTERNATIONAL PUBLIC SERVICE RELATIONS MA
ORDER OF PREVIOUS STUDIES

Course unit code	Course	Required previous studies		Paralel registering (YES/NO)
		Course unit code	Course	