Implementation of Active Learning in the Master’s Program on Cybersecurity

Volodymyr Buriachok
Volodymyr Sokolov

Borys Grinchenko Kyiv University, Ukraine
Design of Learning Outcomes

Central Level

National Qualifications Framework

Area

Industry Qualifications Framework

Specialty

Higher Education Standards

Educational Program

Curriculum and Curriculum Programs

“Security of Information and Communication Systems”

125.00.01 First (bachelor) level

125.00.02 Second (master) level

ICCSEEA2019
International Experience in Active Learning

• Conceiving
• Designing
• Implementing
• Operating

Translation into Ukrainian*:


* Original see http://www.cdio.org/content/cdio-standard-21
Main Approaches to Active Learning

Individuality of the task:
- Due to a different set of skills and competencies of applicants
- Characterized by the need to select a topic according to the student’s prior knowledge, skills and abilities

Focus on the result:
- Due to student interest in master’s work
- Characterized by the need to develop experimental layouts, stands and systems
- The need to ensure transparency of the results of master’s work
Master Skills and Curriculum Formation Scheme

Employer
- Technical Tasks
- Staff Requirements
- Number of Specialists

Active Learning
- Hard Skills
  - Syllabus and Courses
- Soft Skills
  - Competencies and Skills

Employment

ICCSEEA2019
Block Diagram of the Master’s Program in “Cybersecurity”

Bachelor’s degree
- Preknowledge
  - Basic wireless technologies
  - Principles of channel formation & encoding
  - Protocols
  - Principles of access organization
  - OSI protocol stack
  - Principles of network construction
  - Basics of cryptography
  - Concept of building cloud systems
- Web Security
  - Architecture of web resources
  - Programming languages, protocols & techs (PHP, SQL, HTML, HTTP, IP, TCP, UDP, IP, Java, JavaScript, REST, etc.)
- Network and Cloud Security
  - Architecture of operating systems
  - Programming languages (compiler, C/C++, Java)

Master’s diploma
- Knowledge
  - Vulnerabilities in wireless & mobile networks
  - Threats of penetration
  - Specialized network equipment
  - Design of protected wireless networks
  - Vulnerabilities of telecommunication techs
  - Specialized equipment for secure networks
  - Design of protected wired ITS
  - Methods of secure data transfer
  - Vulnerabilities of web resources (SQL injection, bufferovers, XSS, etc.)
  - Development & process of exploitation
  - Design patterns of secure web development
  - Methods for testing network resources
  - Ways to eliminate vulnerabilities
  - Semantic analysis of malware & files
  - Recovery of damaged information
  - Simulation of vulnerabilities
  - Design patterns to protect software
  - Methods of developing and testing software
  - Detection and elimination of activity threatening system security (antivirus, firewalls, sniffer, port scanners)

Additional courses
- Construction and Analysis of Cryptosystems
- Mathematical Methods of Cryptography

Internship
- Scientific Research Internship
- Industrial (Technological) Internship
Continuity of Competencies for “Wireless and Mobile Security”

Bachelor Courses

- Circles and Signals
  - PC:2
  - LO:2
  - LO:3

- Security in Telecommunications
  - PC:5
  - LO:2
  - LO:3
  - LO:4
  - LO:8

- Protection of Information and Communication Systems
  - PC:1
  - LO:2
  - LO:4
  - PC:5
  - LO:3
  - LO:12

- Basics of Physical Security
  - PC:1
  - LO:2
  - LO:11

Master Courses

- Wireless and Mobile Security
  - PC:1
  - LO:2
  - PC:5
  - LO:3
  - LO:7
  - LO:9

- Digital Forensic
  - PC:2
  - LO:3
  - PC:5
  - LO:9

- Penetration Testing and Ethical Hacking
  - PC:4
  - LO:4
  - PC:5
  - LO:5
  - LO:9

- Secure Software Development
  - PC:2
  - LO:2
  - LO:4

PC — Professional Competencies
LO — Learning Outcomes

ICCSEE2019
Active Learning in Wireless and Mobile Security Course

Research of load of a wireless network

DoS attacks on the Wi-Fi network

ICCSEEA2019
Active Learning in Wireless and Mobile Security Course

Radio frequency resource
Wi-Fi 2.4–2.5 GHz

125 kHz RFID sniffing

ICCSEEA2019
Evaluation of the Course

Blekinge Institute of Technology (Sweden)
Wroclaw University of Science and Technology (Poland)
Training and Research Center of the Federal Criminal Police Office (Germany)
Bonch-Bruevich Saint-Petersburg State University of Telecommunications (Russian Federation)
Kharkiv National University of Radioelectronics
Lviv Polytechnic National University
State University of Telecommunications
Borys Grinchenko Kyiv University
1. Before implementation — the Laplace distribution.

2. After — the \( \chi^2 \)-distribution with 4 freedom degrees.

The average score increased by 4 points (from 76.3 to 79.3).
Examples of Master’s Work

1. Hardware implementation
   - Analysis of integrity of data transmission in 2.4–2.5 GHz wireless communication channels using the hardware spectrum analyzer
   - Investigating wireless botnets and making recommendations on their use for implementing denial-of-service attacks

2. Software implementation
   - Software complex for comparative analysis of integrity of data transmission in 2.4-2.5 GHz wireless channels
   - Methodology of counteraction to social engineering at objects of information activity

3. Hardware and software implementation
   - Research on the security of low-power wireless technologies
   - Investigation of ways and recommendations on safety of monitoring systems of wireless ad hoc networks in conditions of third-party influence

ICCSEEA2019
Analysis of Integrity of Data Transmission in 2.4–2.5 GHz Wireless Communication Channels using the Hardware Spectrum Analyzer

Student
Rossykhin Oleksandr Volodymyrovych

Results of Work:
- Detailed design process
- Production of printed circuit boards
- Collection of devices
- Testing and making improvements

Scientific Publication
Investigating Wireless Botnets and Making Recommendations on Their Use for Implementing DoS Attacks

Student
Braslavskiy Myktya Serhiyovych

Results of Work:
• Design process
• Manufacturing of wireless bots
• Conduct an experiment
• Testing and making improvements

Scientific Publication

ICCSEEA2019
Software Complex for Comparative Analysis of Integrity of Data Transmission in 2.4–2.5 GHz Wireless Channels

Student
Grebenyuk Oleksandr Volodymyrovych

Results of Work:

- Overview of technical characteristics
- Development of protocols
- Unification of work with modules
- Software implementation of interfaces

Scientific Publication
Methodology of Counteraction to Social Engineering at Objects of Information Activity

Student
Kurbanmuradov Davyd Mykolayovych

Results of Work:
- Development of a fake access point
- Fishing page design
- Collecting statistics
- Implementation of the stand

Scientific Publication
Research on the Security of Low-Power Wireless Technologies

Student
Taj Dini Makhiar Madzhyd

Results of Work:
- Type of human attack in the middle
- Collection of IEEE 802.15.4/802.16 data
- Analysis of received packages
- Implementation of the stand

Scientific Publication

TajDini M, Sokolov VY (2018) Penetration tests for Bluetooth low energy and Zigbee using the software-defined radio. Mod Inf Prot 1:82–89. DOI: 10.5281/zenodo.2528810
Investigation of Ways and Recommendations on Safety of Monitoring Systems of Wireless Ad Hock Networks in Conditions of Third-Party Influence

Student
Bogachuk Ivan Artemovych

Results of Work:
- Review of technical characteristics
- Spectrum research
- Programming services
- Implementation of the interface

Scientific Publication
November 15
Sokolov VY, Implementation of the world-wide methods of active training in the Master’s program in specialty 125 “Cybersecurity”
Round Table “Cybersecurity: Educational Aspect”
Kiev Boris Grinchenko University, Kyiv

November 29
Buryachok VL, Introduction of Active Learning Technologies into the Educational Process in Borys Grinchenko Kyiv University
Cybersecurity & Intelligent Manufacturing Conference — 2018
Changsha, China

December 1
Babich AN, Active learning: implementation and popularization
Competition for projects among Student Action participants: Leadership competency development program for students
The British Council, Ramada Encore Kiev

December 8
Buryachok VL, Introduction of technologies of practice-oriented training in specialty 125 “Cybersecurity”
Kiev Boris Grinchenko University, Kyiv
Future Work

According to the results of this international project and educational programs, it is planned to create a project of the **national master’s standard** for the training of specialists in the field of cybersecurity.
Conclusions

The usage of active learning will allow:

- To harmonize international standards of the cybersecurity educational programs
- To prepare the translation of the current version of the CDIO standard (2.1)
- To improve the student’s level in cybersecurity
- To increase the competence of specialists in cybersecurity and information security
Implementation of Active Learning in the Master’s Program on Cybersecurity