

Faculty of Computer Technology and Cybersecurity
Department of Cybersecurity



APPROVED BY
Vice-rector for academic affairs,
International Information
Technology University JSC
Mustafina A.K.
03 2023

6B06302

Hardware Security

CATALOGUE OF ELECTIVE DISCIPLINES

2023 entry year

The catalogue of elective disciplines for the specialty/AP 6B06302 - Hardware Security is developed on the basis of the working curriculum of the specialty/AP.

The catalogue of elective disciplines was discussed at a meeting of the Cybersecurity department

minutes No. 2 from « 03 » 11 2023

Head of Department

CED compilers



S.T. Amanzholova

S.T. Amanzholova

A.O. Sagymbekova

N.Y. Askarbekova

The catalogue of elective disciplines was approved at a meeting of the Academic Council of JSC IITU

minutes No. 2 from « 03 » 11 2023

1 TERMS AND ABBREVIATIONS

1.1 Academic program is a single set of basic characteristics of education, including goals, results and content of training, the organization of educational process, ways and methods for their implementation and criteria for assessing learning outcomes. The content of academic program of higher education consists of three cycles of disciplines - general education disciplines (hereinafter - GED), basic disciplines (hereinafter - BD) and core disciplines (hereinafter - CD). The cycle of GED includes disciplines of the compulsory component (hereinafter - CC), the university component (hereinafter - UC) and (or) the component of choice (hereinafter - COC). BD and CD include disciplines of UC and COC.

1.2 Catalogue of elective disciplines (CED) is a systematic annotated list of all COC disciplines, for the entire training period, containing a brief description indicating the purpose of study, a summary of main sections and expected learning outcomes. CED reflects the prerequisites and postrequisites of each academic discipline. It should provide the students with the possibility of an alternative choice of elective disciplines for the formation of an individual educational trajectory.

On the basis of academic program and CED, the students develop individual curricula with the help of advisers.

1.3 Individual curriculum (IC) is a curriculum formed by the students independently with the help of an adviser for each academic year on the basis of the academic program, the catalogue of elective disciplines or modules;

IC defines an individual educational trajectory of each student separately. It includes disciplines and types of educational activities (internship, experimental research, forms of final certification) of the compulsory component (CC), the university component (UC) and the component of choice (COC).

1.4 Advisor is a teacher who performs the functions of an academic mentor of a student (according to the appropriate academic program), and assists in choosing a learning path (creating an individual curriculum) and mastering the academic program during the training period.

1.5 The university component is a list of compulsory educational disciplines determined by the university independently for the mastering of the academic program.

1.6 The component of choice is a list of academic disciplines and the corresponding minimum amounts of academic credits offered by the university and independently chosen by students in any academic period, taking into account their prerequisites and postrequisites.

1.7 Elective disciplines are educational disciplines that are a part of the university component and the component of choice in the framework of established academic credits, introduced by organizations of education reflecting the individual preparation of students and taking into account the specifics of socio-economic development, the needs of a particular region and established scientific schools.

1.8 Postrequisites are the disciplines and (or) modules and other types of academic work, the study of which requires knowledge, skills and competencies acquired at the end of the study of this discipline and (or) modules;

1.9 Prerequisites are the disciplines and (or) modules and other types of educational work containing knowledge, abilities, skills and competencies necessary for the mastering of the studied discipline and (or) modules;

1.10 Competencies are the ability of the practical use of acquired knowledge and skills in professional activities.

2 ELECTIVE DISCIPLINES

№	Cycle of discipline	Code of discipline	Name of discipline	Semester	Number of credits	Prerequisites
3 year						
1	BD	SEC6233	Introduction to Intelligent Cybersecurity	6	4	MAT6018 Mathematical foundations of information security
2	BD	HRD6205	Architecture of computer systems	6	4	NET 6201 Fundamentals of Computer Networks
3	ПД	MIN601	Minor 1	5	5	
4	ПД	MIN602	Minor 2	6	5	
4 year						
5	OOD	ECO6004	Economics and organization of production	8	5	SPS6002 Sociology
6	OOD	MGT6706	Startups and entrepreneurship	8	5	SPS6002 Sociology
7	OOD	JUR 6470	Fundamentals of law and anti-corruption culture	8	5	SPS6002 Sociology
8	OOD	JUR 6507	Fundamentals of ecology and life safety	8	5	SPS6002 Sociology
9	PD	SEC6205	Mobile technology security	7	4	SFT6207 Object-oriented Programming (Java)
10	PD	SEC6252	Smart technologies	7	4	SEC6204 Project Management in Information Security
11	PD	SEC6211	Protection of database management systems	7	4	SFT6211 Organization of database management systems
12	PD	SEC6239	Hardware Security Integration	7	4	SEC6201 Computer Information Protection Technologies
13	PD	SEC6208	Practical pentesting	7	6	SEC6202 Operating System Security
14	PD	SEC6240	Development of applications for hardware devices in Python	7	6	SFT6202 Object-oriented Programming (Java)
15	PD	MIN603	Minor 3	7	5	
16	PD	SEC6241	Hardware Security encryption Technologies	8	5	EGR6202 Information Theory
17	PD	SEC6238	Blockchain Technologies	8	5	MAT6018 Mathematical

						foundations of information security
18	PD	NET6207	DevNet	8	5	NET 6201
19	PD	SEC6242	Security management of reconfigurable embedded systems	8	4	Fundamentals of Computer Networks
20	PD	SEC6235	Biometric access control systems	8	4	NET 6202 Basics of Switching, Routing and Wireless Networks
						EEC6003 Design and modeling of electronic devices

3 DESCRIPTION OF ELECTIVE DISCIPLINES

Discipline description	
Code of discipline	ECO6004
Name of discipline	Economics and organization of production
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	SPS6002 Sociology
Postrequisites	Graduation project
Brief course description	<p>Enterprise economics is a system of knowledge related to the process of developing and making business decisions in the course of the company's activities. Therefore, the economy of an enterprise, as a system of knowledge and methods of managing the economic activity of an enterprise, occupies an important place in the organization of production and distribution of goods in any economic system.</p> <p>The course introduces the production structure of the enterprise, in relation to the type of production, the organization of the production cycle, issues of technical preparation of production and the creation of the necessary production infrastructure, innovative activity of the enterprise, product quality, investment policy of the enterprise, environmental issues, foreign economic activity of the enterprise and the organization of the enterprise management process as a whole.</p>
Expected learning outcomes	<p>To form fixed and circulating funds, to use capital, to receive and distribute the income (profits) of the enterprise.</p> <p>Develop strategies for the economic activity of the enterprise, plan production and sales of products.</p> <p>To know the financial resources of the enterprise, the efficiency of economic activity, to assess the risk in entrepreneurship.</p> <p>To solve the issues of material and technical support of production: supply of raw materials, materials, formation of stocks and their rational use.</p>

Discipline description	
Code of discipline	MGT6706
Name of discipline	Startups and entrepreneurship
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	SPS6002 Sociology
Postrequisites	Graduation project
Brief course description	<p>A startup is a commercial project based on an idea and requires financing for development related to entrepreneurship.</p> <p>The course introduces the formation of a business idea that solves a real consumer problem, the launch of a minimum viable product (MVP) to test a hypothesis, the achievement of product-market fit - acceptance of the product by the market, scaling of the project through investments in advertising, attracting partners and achieving maturity — a stable position in the market.</p>

Expected learning outcomes	<p>"Consumer identification", during which a startup builds hypotheses about how its product solves the problems of potential customers.</p> <p>"Consumer verification", the stage of hypothesis testing and preparation of a sales plan, marketing strategy, search for early followers of the company. In case of failure at this stage, the startup returns to identifying its consumers.</p> <p>"Attracting consumers" after confirming the usefulness of the company's product. The startup is moving to product sales and marketing investments.</p> <p>"Creating a company" is the ultimate goal of a startup, creating a formal company structure and business processes for further development.</p>
----------------------------	---

Discipline description	
Code of discipline	JUR 6470
Name of discipline	Fundamentals of law and anti-corruption culture
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	SPS6002 Sociology
Postrequisites	Graduation project
Brief course description	The aim of the course is to understand the basics of anti-corruption culture, to develop the ability to describe the essence and causes of corruption in society. The course forms the acquisition of skills to work with legislation in the field of anti-corruption, and develops a civic attitude to this phenomenon. This course is aimed at improving the anti-corruption culture and the formation of moral and legal responsibility for corruption offenses.
Expected learning outcomes	Develops knowledge, skills and anti-corruption skills. Knows the basics of law

Discipline description	
Code of discipline	JUR 6507
Name of discipline	Fundamentals of ecology and life safety
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	SPS6002 Sociology
Postrequisites	Graduation project
Brief course description	<p>The purpose of the course is to study the basics of life safety and environmental protection, teaching the goals and objectives of the methodology, methods used in the process of planning and conducting classes, and ways to use modern new technologies in the classroom.</p> <p>The course introduces the issues of theoretical and practical foundations of safety, harmlessness and facilitation of working conditions at its maximum productivity, on the legislative and regulatory framework in the field of labor protection. Legislative acts. Organizational and theoretical foundations of life safety. Concepts and definitions.</p>
Expected learning outcomes	Be able to be guided by ethical and legal norms of relations to a person, society, and the environment.

	<p>Possess knowledge about the factors affecting the technical and economic efficiency of production.</p> <p>Be able to identify hazards and assess risks in the field of occupational safety at work.</p> <p>Be able to apply professional knowledge to minimize negative technogenic consequences, ensure safety and improve working conditions in the field of their professional activities.</p>
--	--

Discipline description	
Code of discipline	SEC6233
Name of discipline	Introduction to Intelligent Cybersecurity
Number of credits (ECTS)	4
Course, semester	3,6
Department	CYBERSECURITY
Prerequisites	MAT6018 Mathematical foundations of information security
Postrequisites	SEC6206 Cryptographic methods of information protection
Brief course description	<p>The Intelligent Cybersecurity Intelligence System (CIS) protects against APT attacks using technologies such as big data analytics and machine learning. To protect key information resources, CIS accurately identifies APT threats and prevents attacks. The system allows you to restore the "killer chain" in APT attacks by extracting key information from a large array of data, assessing risks in several directions and comparing isolated suspicious areas based on the results of big data analysis.</p> <p>The purpose of the course is to gain theoretical knowledge, skills and practical skills on intellectual security issues. The acquired knowledge, skills and abilities will allow students to navigate the issues of intellectual cybersecurity and continue their cybersecurity studies in more advanced courses.</p> <p>This course develops the ability to analyze possible security threats, the ability to choose and apply various methods of protection with the help of AI.</p>
Expected learning outcomes	To develop the skills of safe use of the Internet, selection and application of various ways to protect your personal data, analysis of possible security threats based on the AI system.

Discipline description	
Code of discipline	NET6207
Name of discipline	DevNet
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	NET 6201 Fundamentals of Computer Networks
Postrequisites	Graduation project
Brief course description	<p>This course introduces the methodologies and tools of modern software development used in OT and network operations. It covers a complete overview of the subject area, including microservices, testing, containers and DevOps, as well as secure infrastructure automation using application programming interfaces (APIs).</p>

Expected learning outcomes	Get hands-on, up-to-date hands-on laboratory experience, including Python programming, using GIT and common data formats (JSON, XML and YAML), deploying applications as containers, using continuous integration/continuous deployment pipelines (CI/CD) and automating infrastructure using code. Developing skills for entry-level software development and infrastructure automation
----------------------------	---

Discipline description	
Code of discipline	SEC6208
Name of discipline	Practical pentesting
Number of credits (ECTS)	6
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SEC6202 Operating System Security
Postrequisites	Graduation project
Brief course description	This course is closely integrated with a laboratory component that introduces students to various aspects of practical software and networking exploit techniques in Windows, Linux and Android operating systems. The course also teaches students various important practical attacks on OSI levels and ways to eliminate them.
Expected learning outcomes	Have basic knowledge of shell coding and exploit development. Have practical knowledge about conducting systematic penetration testing against the target Search, analysis and execution of a specific exploit Have basic knowledge in the field of software error detection Practical knowledge of the Metasploit Framework

Discipline description	
Code of discipline	HRD6205
Name of discipline	Architecture of computer systems
Number of credits (ECTS)	4
Course, semester	3,6
Department	CYBERSECURITY
Prerequisites	NET6201 Fundamentals of computer networks
Postrequisites	SEC6201 Computer Information Protection Technologies
Brief course description	Computer architecture is the science and art of selecting and connecting hardware components to create a computer that meets the requirements for functionality, performance and cost. The course introduces the basic structure of a modern programmable computer, including the basic laws underlying the evaluation of equipment performance. It discusses the basics of classical and modern processor design: performance and cost issues, instruction sets, pipelining, caches, physical memory, virtual memory, I/O superscalar and an introduction to multiprocessors with shared memory.
Expected learning outcomes	Analysis of the structure of the main components of the computer, including CPU, ALU and control unit, memory, I/O and storage. Explain the execution of the program in a high-level language at the instruction level.

	<p>Optimize the operation of the cache memory.</p> <p>Apply a wide range of memory technologies, both internal and external.</p> <p>Create a program code in the C language that controls the processes in the processor.</p>
--	---

Discipline description	
Code of discipline	SEC6235
Name of discipline	Biometric access control systems
Number of credits (ECTS)	4
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	EEC6003 Design and modeling of electronic devices
Postrequisites	Graduation project
Brief course description	This course describes methods for obtaining biometric data; The main methods of digital signal and image processing used for biometric identification are studied.
Expected learning outcomes	<p>After successful completion of the course, students will:</p> <ul style="list-style-type: none"> - apply methods of recognition of control samples; - use technical means to obtain initial biometric data; - be able to design devices, devices and systems.

Discipline description	
Code of discipline	SEC6238
Name of discipline	Blockchain Technologies
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	MAT6018 Mathematical foundations of information security
Postrequisites	Graduation project
Brief course description	<p>Blockchain is a technology for encrypting and storing data distributed across multiple computers connected to a common network.</p> <p>This course describes a digital database of information that reflects all transactions made, records in the blockchain, presented in the form of blocks interconnected by special keys.</p>
Expected learning outcomes	<p>After successful completion of the course, students will:</p> <ul style="list-style-type: none"> -know the principles of blockchain, -use blockchain for storing and transmitting digital data.

Discipline description	
Code of discipline	SEC6205
Name of discipline	Mobile technology security
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SFT6207 Object-oriented Programming (Java)
Postrequisites	Graduation project

Brief course description	The discipline provides knowledge on the use of tools for programming and designing mobile applications, on the development of user interfaces for mobile applications, on the use of software functions that support telephony, sending /receiving SMS, connection management via Wi-Fi, Bluetooth, programming background services, notification and alarm mechanisms, interaction of applications with geolocation and mapping services.
Expected learning outcomes	After successful completion of the course, students will: -know the basics of mobile technology security -apply the knowledge gained in practice.

Discipline description	
Code of discipline	SEC6211
Name of discipline	Protection of database management systems
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SFT6211 Organization of database management systems
Postrequisites	Graduation project
Brief course description	Protection of database systems is a set of methods, software tools, processes, programs and technologies, the use of which ensures the security of stored information and prevents it from unauthorized electronic access, modifications, accidental disclosure, violation, destruction, copying. The course introduces concepts such as basic database protection tools, regular database audit, automated database protection systems.
Expected learning outcomes	Is able, knows and conducts: <ul style="list-style-type: none"> – Regular audit and monitoring – Backup – Encryption – VPN and two-factor authentication – Automated protection systems (Database Activity Monitoring)

Discipline description	
Code of discipline	SEC6239
Name of discipline	Hardware Security Integration
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SEC6201 Computer Information Protection Technologies
Postrequisites	SEC6215 IoT Security
Brief course description	The discipline provides fundamental knowledge about hardware security integration, including basic components such as network infrastructure devices, low-power network solutions and middleware solutions, as well as relevant security and privacy issues related to these components.
Expected learning outcomes	After successful completion of the subject, students should be able to: - demonstrate an understanding of the basics and solutions of hardware security integration

	<ul style="list-style-type: none"> - analyze algorithms, architecture, and hardware security integration approaches - check hardware security protections, including software-defined security for networks and the cloud.
--	--

Discipline description	
Code of discipline	SEC6240
Name of discipline	Development of applications for hardware devices in Python
Number of credits (ECTS)	6
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SFT6202 Object-oriented Programming (Java)
Postrequisites	Graduation project
Brief course description	Python is a multi—paradigm programming language. Django is a full-featured server-side web framework written in Python. The Django framework copes with a large number of tasks and increased loads. It is used to create: CRM systems, CMS, Communication platforms, room booking services, document management platforms. The course studies the creation of modern web applications on this framework.
Expected learning outcomes	<ul style="list-style-type: none"> -design and build Django web applications -testing Django web applications -using the built-in tools of the framework to ensure the security of the web application

Discipline description	
Code of discipline	SEC6252
Name of discipline	Smart technologies
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SEC6204 Project Management in Information Security
Postrequisites	Graduation project
Brief course description	The subject of the discipline is information technology infrastructure, the use of software, communication systems, information centers, networks and databases. The purpose of this course is to study rapidly developing and changing technologies in the field of embedded systems, sensors, wireless networks, Internet-of-Things (IoT). The course includes obtaining solid skills in programming in various modern programming languages, including C++, Java, Python, including applications to IoT, cybersecurity, data processing and analysis.
Expected learning outcomes	<p>Knows technologies in the field of embedded systems, sensors, wireless networks, Internet-of-Things (IoT)</p> <p>Is able to program in various modern programming languages, including C++, Java, Python, including applications to IoT, cybersecurity, data processing and analysis</p>

Discipline description	
Code of discipline	SEC6241
Name of discipline	Hardware Security encryption Technologies

Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	EGR6202 Information Theory
Postrequisites	Graduation project
Brief course description	This course will discuss in detail the goals, methods and ways of implementing various encryption technologies for hardware security of devices. Hardware encryption methods will be studied to ensure a high level of security.
Expected learning outcomes	Uses various encryption technologies for hardware security of devices Knows hardware encryption methods to ensure a high level of security

Discipline description	
Code of discipline	SEC6242
Name of discipline	Security management of reconfigurable embedded systems
Number of credits (ECTS)	4
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	NET 6202 Basics of Switching, Routing and Wireless Networks
Postrequisites	Graduation project
Brief course description	The course is designed to teach students security techniques in reconfigurable embedded systems. As part of the course, students study the principles of security management, including methods of risk analysis, identification of threats and risks, as well as assessment of the effectiveness of security measures.
Expected learning outcomes	Uses security methods in reconfigurable embedded systems Knows the principles of security management, including methods of risk analysis, identification of threats and risks Assesses the effectiveness of security measures