

Faculty of Computer Technology and Cybersecurity  
Department of Cybersecurity

APPROVED BY

Vice-rector for academic affairs,  
International Information  
Technology University JSC

Mustafina A.K.

2023



6B06303

Network Security

## CATALOGUE OF ELECTIVE DISCIPLINES

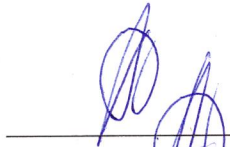
2023 entry year

The catalogue of elective disciplines for the specialty/AP 6B06303 - Network 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

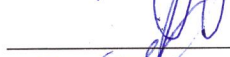
minutes No. 2 from «03» 11 2023

Head of Department



S.T. Amanzholova

CED compilers



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
<b>3 year</b>						
1	BD	SEC6233	Introduction to Intelligent Cybersecurity	6	4	MAT6018 Mathematical Foundations of Information Security
2	BD	SEC6247	Network Infrastructure Security	6	4	SEC6201 Computer Information Protection Technologies
3	PD	MIN601	Minor 1	5	5	
4	PD	MIN602	Minor 2	6	5	
<b>4 year</b>						
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	SEC6248	Intrusion detection and prevention systems	7	6	SEC6217 Legal basis of information security
10	PD	SFT6206	Development of corporate applications on the Django framework	7	6	SFT6202 Object-oriented Programming (Java)
11	PD	SEC6205	Mobile technology security	7	4	SFT6207 Object-oriented programming (Java)
12	PD	SEC6249	Digital forensics of network infrastructure	7	4	SEC6201 Computer Information Security Technologies
13	PD	SEC6211	Protection of database management systems	7	4	SFT6211 Organization of database management systems
14	PD	SEC6234	Introduction to Cloud technologies	7	4	EGR6202 Information Theory
15	PD	MIN603	Minor 3	7	5	
16	PD	NET6207	DevNet	8	5	NET 6201 Fundamentals of Computer Networks

17	PD	SEC6250	Managing network infrastructure vulnerabilities	8	5	EGR6202 Information Theory
18	PD	SEC6238	Blockchain Technologies	8	4	MAT6018 Mathematical Foundations of Information Security
19	PD	SEC6251	Networking	8	4	NET 6202 Fundamentals of Switching, Routing and Wireless Networks
20	PD	SEC6237	Analytics of the Information Security Center	8	4	SEC6201 Computer Information Protection Technologies

### 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	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.
Expected learning outcomes	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.

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	A startup is a commercial project based on an idea and requires financing for development related to entrepreneurship. 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.
Expected learning outcomes	"Consumer identification", during which a startup builds hypotheses about how its product solves the problems of potential customers. "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. "Attracting consumers" after confirming the usefulness of the company's product. The startup is moving to product sales and marketing investments. "Creating a company" is the ultimate goal of a startup, creating a formal company structure and business processes for further development.

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.

### 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	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. 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.
Expected learning outcomes	Be able to be guided by ethical and legal norms of relations to a person, society, and the environment. Possess knowledge about the factors affecting the technical and economic efficiency of production. Be able to identify hazards and assess risks in the field of occupational safety at work. Be able to apply professional knowledge to minimize negative technogenic consequences, ensure safety and improve working conditions in the field of their professional activities.

### 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	The Intelligent Cybersecurity Intelligence System (CIS) protects against APT attacks using technologies such as big data analytics and machine learning. To



	<p>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	NET6201 Fundamentals of computer networks
Postrequisites	Graduation project
Brief course description	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).
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.

Discipline description	
Code of discipline	SFT6206
Name of discipline	Development of corporate applications on the Django framework
Number of credits (ECTS)	6
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SFT6202 Object-oriented Programming (Java)
Postrequisites	Graduation project
Brief course description	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	-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	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	SEC6249
Name of discipline	Digital forensics of network infrastructure
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SEC6201 Computer information protection technologies
Postrequisites	Graduation project
Brief course description	Purpose of the course: • Present the field of digital forensics, including its tools and applications. Goals: • Explain how the use of electronic evidence has evolved. • Disseminate knowledge and the importance of digital forensics in everyday life. • Prepare students to become the next cyberspace researchers. • Raise awareness about digital crimes, how to deal with them, collect evidence and report them.
Expected learning outcomes	Explain the requirements for workstations and data recovery software. Describe the components to build a business case for the development of a forensic laboratory. Explain how to determine the best data collection method. Explain the instructions for removing digital evidence at the scene. Describe the available software tools of digital forensics.

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"> <li>- Regular audit and monitoring</li> <li>- Backup</li> <li>- Encryption</li> <li>- VPN and two-factor authentication</li> <li>- Automated protection systems (Database Activity Monitoring)</li> </ul>

<b>Discipline description</b>	
Code of discipline	SEC6247
Name of discipline	Network infrastructure security
Number of credits (ECTS)	4
Course, semester	3,6
Department	CYBERSECURITY
Prerequisites	SEC6201 Computer Information Protection Technologies
Postrequisites	NET6203 Security and automation of corporate networks
Brief course description	The discipline provides fundamental knowledge about the security of network infrastructure, 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: <ul style="list-style-type: none"> <li>- demonstrate an understanding of the basics and solutions of network infrastructure security</li> <li>- analyze algorithms, architecture and security approaches of the network infrastructure</li> <li>- check the security measures of the network infrastructure, including software-defined security for networks and the cloud.</li> </ul>

<b>Discipline description</b>	
Code of discipline	SEC6248
Name of discipline	Intrusion detection and prevention systems
Number of credits (ECTS)	6
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	SEC6217 Legal basis of information security
Postrequisites	Graduation project
Brief course description	The discipline provides fundamental knowledge about the intrusion detection and prevention system, including a set of software or hardware tools that identify facts and prevent unauthorized access attempts to the corporate system and IDS architecture and technology
Expected learning outcomes	After successful completion of the subject, students should be able to: <ul style="list-style-type: none"> <li>- demonstrate an understanding of the basics of intrusion detection and prevention systems</li> <li>- analyze algorithms, architecture, and infrastructure security approaches</li> <li>- check security protection measures, including software-defined security to prevent intrusions.</li> </ul>

<b>Discipline description</b>	
Code of discipline	SEC6234

Name of discipline	Introduction to Cloud Technologies
Number of credits (ECTS)	4
Course, semester	4,7
Department	CYBERSECURITY
Prerequisites	EGR6202 Information Theory
Postrequisites	Graduation project
Brief course description	The course contains basic information about the emergence, development and use of cloud computing technologies. The course examines the main models of providing cloud computing services. The solutions of the leading vendors – Microsoft, Amazon, Google - are reviewed. The main advantages and disadvantages of cloud computing models and solutions based on them are analyzed.
Expected learning outcomes	After successful completion of the subject, students should know: <ul style="list-style-type: none"> <li>- Fundamentals of Cloud Computing</li> <li>- Examples of Microsoft cloud services</li> <li>- Web services in the Cloud</li> <li>- Virtualization technologies</li> </ul>

#### 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	Blockchain is a technology for encrypting and storing data distributed across multiple computers connected to a common network. 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.
Expected learning outcomes	After successful completion of the course, students will: <ul style="list-style-type: none"> <li>-know the principles of blockchain,</li> <li>-use blockchain for storing and transmitting digital data.</li> </ul>

#### Discipline description

Code of discipline	SEC6237
Name of discipline	Analytics of the Information Security Center
Number of credits (ECTS)	4
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	SEC6201 Computer Information Protection Technologies
Postrequisites	Graduation project
Brief course description	This course describes security concepts, attack techniques, and security monitoring. The course allows students to understand security concepts and begin to learn the basic security techniques used in the Security Management Center to search for threats on the network using various popular security tools of the real network infrastructure.
Expected learning outcomes	Explain how to investigate vulnerabilities and attacks of enterprise endpoints.

	<p>Identify network security warnings.</p> <p>Analyze data about an intrusion into the enterprise network to check for possible exploits.</p> <p>Apply incident response models to manage network security incidents.</p>
--	---

Discipline description	
Code of discipline	SEC6250
Name of discipline	Managing network infrastructure vulnerabilities
Number of credits (ECTS)	5
Course, semester	4,8
Department	CYBERSECURITY
Prerequisites	EGR6202 Information Theory
Postrequisites	Graduation project
Brief course description	<p>Vulnerability Management is a process aimed at reducing the damage from the implementation of threats caused by infrastructure vulnerability.</p> <p>This course describes the concepts of identifying devices on the network, their systematization by groups for further work, a list of vulnerabilities, recommendations for eliminating vulnerabilities or minimizing risks.</p>
Expected learning outcomes	<p>Skills of building a vulnerability management process:</p> <ul style="list-style-type: none"> <li>Inventory</li> <li>Scanning and analysis</li> <li>Working with vulnerabilities</li> <li>Control</li> </ul>

Discipline description	
Code of discipline	SEC6251
Name of discipline	Networking
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	<p>Modern corporate information systems by their nature are always distributed systems. User workstations, application servers, database servers and other network nodes are distributed over a large area. In a large company, offices and sites are connected by various types of communications using various technologies and network devices.</p>
Expected learning outcomes	<p>Knows the components of the network infrastructure, such as:</p> <ul style="list-style-type: none"> <li>cable system and means of communication;</li> <li>active network equipment;</li> <li>network protocols;</li> <li>network services;</li> <li>network applications.</li> </ul>