Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Basics of Information Security in Financial Organizations/Основы информационной безопасности в финансовых организациях

Purpose of the course:

To provide students with basic concepts of information security activity organization in financial institutions.

Tasks of the course:

- the study of approaches, methods of information security risk management;

- the acquisition of practical skills of information assets inventory, analysis of business processes of information processing, threats and risks definition;

- the acquisition of the ability to develop compensating measures for information security risks.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

- procedure of organization of information security activity in financial organizations;

- typical information infrastructures of financial organizations;

- processed in financial organizations data types and typical business processes.

be able to:

- conduct an inventory of information assets;

- to analyze the business processes of information processing;

- identify threats to information security;

- determine the level of information security risk;

- develop effective compensating measures for information security risks.

master:

- skills of mastering a large amount of information;

- the skills of presenting the results of the activities of the information security unit;

- incident investigation skills.

Content of the course (training module), structured by topics (sections):

1. Basics of information security and description of the infrastructure of financial institutions.

Information. Properties of information. Information security legislation. Financial institutions, their processes and infrastructure.

2. Analysis of business processes of financial organizations and identification of threats. Determination of the level of risks. Development of compensatory measures

Definition of business processes and their analysis, identification of threats and calculation of the level of risk. Determination of the most effective compensatory measures and creation of measures implementation program.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Basics of Network Technologies/Основы сетевых технологий

Purpose of the course:

studying fundamental principles of data network construction, description of the role of computer networks in the telecommunications world, types and types of networks, methods of multiplexing, switching packets and channels, open systems and model OSI.

Tasks of the course:

 To provide students with an in-depth knowledge and understanding of the basics of network technology in relation to cyber security applications;

 To develop engineering skills in the implementation of network technologies in practice.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

 Main concepts of building local and global networks;

 Field of applicability of traditional and modern network technologies;

 Diversity of network protocols and standards;

 Principles of operation of various types of communication equipment;

 Fundamentals of TCP/IP protocol, routing and IP-addressing, CIDR (Classless Inter-Domain Routing) method;

 Understanding of the range of problems associated with data protection in networks.

be able to:

 use advantage of the advantages and disadvantages of various network technologies to address a variety of applications;

 explain the differences between different types of network architectures;

 describe the typical equipment components used for data transmission in the network;

 describe the principles and protocols of remote communication.

master:

 get skills in building local area network and network structures, including global connectivity;

 usage communication models used in the communication network;

 skills in the application of the network technologies studied to solve applied tasks of data processing in the field of cyber security.

Content of the course (training module), structured by topics (sections):

1. Introduction to network technology

Theoretical fundamentals, principles and systematic introduction to network issues that provide the basic knowledge needed to solve applied data processing tasks in the field of cyber security.

2. The basic foundation of network technology

Studding principles of network operation as a whole considers the basic concepts and the most important characteristics of software and hardware components that make up the network: computers, communication equipment and operating systems.

3. Decision Trees Algorithms

Typical structures of computer networks are given. The functional purpose of the main elements of the network operating system - the server, the redirector and communication drivers - is explained. The characteristic of the most known network operating systems is given. The principles of gateway interaction are considered. The basic concepts from the field of network security are resulted.

4. The most popular communication protocol stacks

The most popular communication protocol stacks are reviewed and their conformity to the seven-level ISO/OSI model is considered. The principles of operation of various types of communication equipment are studied: repeaters, bridges, switches, routers, multiplexers.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Critical Infrastructure Security and Management System Security/Безопасность критически важной инфраструктуры и системы управления

Purpose of the course:

Studying the theoretical and practical foundations of cybersecurity of critical information infrastructures, as well as preparing students for further independent work in the field of protection of critical information infrastructures.

Tasks of the course:

1. To provide students with in-depth knowledge and understanding of approaches and methods of protecting CII facilities for solving the problems of cybersecurity infrastructure;

2. Explore best practices for protection critical information infrastructures;

3. To develop practical skills in the application of technology for protecting objects of CII from computer attacks.

4. To teach methods of monitoring information security events and the ability to conduct incident assessments.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

- Theoretical and regulatory framework for the protection of CII;

- Basic concepts of building local and global networks;

- Applicability of traditional and modern network technologies;

- The content and purpose of the main network protocols and standards;

- How different types work communication equipment;

- Application of the TCP / IP protocol, routing and IP addressing;

- An understanding of the range of problems associated with data protection in networks;

- Basic requirements for the protection of CII;

- Methods and approaches to creating a protection system for CII facilities;

- Information security event response technologies and rules for responding to computer security incidents;

- Intelligent information security technologies based on data flow processing;

- Trusted device mesh technologies and secure system architecture;

- Technologies of software-defined networks and virtualization of network functions;

- Fundamentals of Cryptographic Modules Technology;

- Fundamentals of the functioning of trusted "cloud" computing;

- Fundamentals of creating secure mobile technologies of 4G + and 5G generations;

- Fundamentals of program analysis and analytical verification;

- Fundamentals of quantum data transmission technology.

be able to:

- Use various network technologies to solve various applied problems;

- Use the differences between different types of network architectures;

- Describe the typical pieces of equipment used to transmit data over a network;

- Apply principles and protocols of remote communication;

- Plan work to create an open segment of the early detection system for computer attacks on critical infrastructure.

master:

- Skills of building structural diagrams of local networks and networks, including global connections;

- Skills in the use of various models of data exchange in a communication network;

- Skills in the use of network technologies for solving applied problems of data processing in the field of cybersecurity;

- Skills of working with the data used in the systems for detecting and preventing computer attacks of the CII.

Content of the course (training module), structured by topics (sections):

1. National critical infrastructures

CII of Great Britain, European Community, Germany and Russian Federation. The main objects of KII.

Basic national technical standards for information infrastructure. Survey of research and development of cybersecurity technologies of the US DARPA agency. Development of functional safety standards of the RF CII.

2. Typical compositions of information objects of critical information infrastructures

The standard open systems interoperability model is the OSI model. TCP / IP protocol stack model. Basic network protocols. Data transmission medium and digital coding. Characteristics of the physical environment of network technologies. Basics of digital coding. Hierarchical structure of LAN. LAN cable system. Switching technology in SCS. LAN access protocols. Ethernet protocols. Network addressing. Virtual LANs. Wireless networks. Detection of errors and faults at the link level.

Basics of IPv4 and IPv6 protocols. Statistical routes. Routing tables. Internet Control Message Protocols. External inter-gateway routing protocol.

3. Organization and management of network services at the facilities of critical information infrastructures in ensuring national and international security

Basic Internet Network Services and Application Protocols. Service classification. Transport layer protocols. Domain Name System. Protocols: remote procedure call, terminal, hypertext data transfer, file transfer. Email service. Organization of network file systems. Control systems architecture. Analysis of data streams. Analysis of the content of data traffic in the network.

4. National approaches to the protection of critical information infrastructures

Cyberspace as a potential source of threats to critical infrastructure and state infrastructure.

The main types of threats to CII facilities.

5. Security of critical information infrastructures

Strategic goals and main directions of ensuring information security. Techniques for conducting computer attacks on TCP networks of CII facilities: Listening to the network. Scanning the network.

Packet generation. Interception of data. False ARP replies. Imposing a false router. Open loop impersonation of TCP connections. Desynchronization of TCP connections. Unauthorized connection to the network. Unauthorized data exchange. Tunneling. Forcing to accelerate data transfer.

Denial of service.

6. Methods and measures to ensure the security of critical information infrastructures

Filtering data on the router. Host Protection. Router Security Proactive Scan. Encryption protection potential. Encryption schemes. Vulnerability in wireless LAN encryption schemes.

7. Objects of protection of critical information infrastructures

Protection of speech information in digital telephone networks. Threats to violate the confidentiality of information in IP telephony. Threats to the security of IP traffic on the network.

8. Vulnerabilities of critical information infrastructures

Vulnerability classification. Assessment of threats of computer attacks on information resources.

9. CII defense model

Potential violators of the security of critical information infrastructures. Threat model. Intruder model. A categorization scheme for CII objects. The task for meeting the requirements of information security of the CII. Measures to protect CII.

10. Certification of CII facilities for compliance with information security requirements

The procedure for attestation of CII objects. Accredited laboratories. Requirements for attestation of CII objects.

11. Threats to the security of critical information infrastructures

CII security events and incidents.

Assessment of threats of computer attacks on information resources of the CII. Sources of computer attack threats. Methodology for probabilistic assessment of actual threats to information security.

12. Monitoring the security of critical information infrastructures

Problems of detecting and preventing computer attacks. Systems for monitoring information security messages and detecting incidents at CII facilities. Overview of detection methods. IPS, IDS systems. Classification of intrusion detection systems. SIEM systems. Comparative analysis of SIEM systems. Monitoring security threats.

13. System of detection and prevention and prevention of computer attacks of the CII object

Models and Methods of Preemptive Computer Attack on CII

Modification of the "von Neumann architecture" to select the hardware platform. Network information security tools for ACS.

14. Principles of security of critical information infrastructures

Stability of CII objects. Method for assessing the resistance of CII objects to IS threats.

15. Security management of critical information infrastructure

Approaches to creating an information security management system for CII facilities. Risk-based approach to assessing the quality indicators of CII management.

16. Technologies for ensuring the safety of software and equipment of information systems of objects of critical information infrastructure

CII safety assessment models. Basic approaches to the CII model. Weylet analysis method. Condition for the stability of the forecasting model.

17. Organization of national systems for the protection of critical information infrastructures

Detection of computer attacks using neural networks. Practical tasks of detecting attacks.

18. Technical methods and technologies for protecting critical information infrastructures

Recommendations and requirements of regulators. Methodology for categorizing CII objects. Measures for the protection of CII facilities. Firewall. VPN. Perimeter protection. Segmentation of the system. Protection of communication lines and communications. System monitoring with intrusion detection tools. Separation of protection. Identification and Authentication. Antivirus

protection. Trusted download. Updating protection tools. Trusted configuration. Organization of a demilitarized network zone. Network flow control. Hiding addresses and network architecture. Anti-spoofing. NAT. Separate filtering of open IP traffic and encrypted traffic.

19. Organizational methods of protecting critical information infrastructures

Creation of a categorization commission. Categorization of CII objects. Collecting data for categorizing CII objects. Assessment of the criticality of processes. Formation of a list of CII objects. Assessment of the magnitude of the consequences and correlation with the values of indicators of the CII categories. A method for assessing the category of significance of an object of CII. Determination of CII objects associated with critical processes. The act of categorizing objects of CII. Making changes to the results of categorizing objects.

20. Responsibility for violation of security requirements of critical information infrastructures

Rights and obligations of CII subjects. Responsibility of officials of the subject of CII in accordance with 187-FZ and the Code of Administrative Offenses of the Russian Federation.

21. Advanced technologies for the development of critical information infrastructures

Operation security of trusted "cloud" and "fog" computing, virtual environments;

Problems of creating secure mobile technologies of 4G + and 5G generations;

Possible approaches in the technology of automated simulation of the situation. Predictive analytics. Systemic look of the security BI platform.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Cyber Defense/Киберзащита

Purpose of the course:

1. To teach students the skills of developing methods for the synthesis of secure distributed computer networks (DCN), which are the basis for building departmental and corporate networks.

2. Acquisition of skills in analyzing the applicability of DCN security technologies in the face of destructive impacts from both internal and external penetrations, with the complex use of cryptographic algorithms and multi-level and layered information protection.

Tasks of the course:

Formation of students ' practical skills in applying the studied methods and schemes in the conditions of a complex of destructive influences.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

The students mastering approaches, methods and models for the analysis of the dynamics of the processes of information warfare different nature.

be able to:

The acquisition of practical skills of application of risk models and methods of the multidimensionality of the data for identifying the parameters of web-based attacks, and retrieval of knowledge in information warfare.

master:

The acquisition of the ability to interpret the results obtained to build scenarios, forecasts, decision making with the aim of countering web injection attacks and explain the nature of arising in information and communication systems information security incidents.

Content of the course (training module), structured by topics (sections):

1. Methodology for system analysis of the risk of an attack on DCN objects. The concept of separation of information security solutions.

Option of forming a multi-zonal system for the protection of computer networks. The use of firewalls (FW) systems, intrusion detection and protocols that provide authentication, encryption, and establishing a session for secure information exchange in the upper levels of OSI.

Examples of programming authentication protocols in the Matlab environment.

2. Fundamentals of building a public key management infrastructure.

Tasks and procedures for managing public keys. The life cycle of a cryptographic key. Examples of programming stages and phases of the cryptographic key lifecycle in Matlab.

3. General provisions on certification and certificates.

Key certificate. End-user certificates. Publisher certificates.

4. Complex application of cryptographic algorithms and systems in computer networks. Cryptographic interface (CryptoaAPI).

Windows cryptographic subsystem architecture, electronic signature algorithm, symmetric encryption session key exchange algorithm, session key generation scheme from hash value, public key module.

Examples of programming encryption algorithms in the Matlab environment.

5. Sources of information about the attacks.

Operating system log (system event, application, and security logs). Log of communication equipment registration. The log of the firewall. Examples of log event analysis programs in Matlab.

6. Hiding the source and fact of the attack.

Spoofing the address of the attack source. The creation of false packets. Using other people's computers to attack. Fragmentation of the attack. Examples of programming fake packages in Matlab.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Fundamentals of Intelligent Cyber Security Management/Основы систем управления информационной безопасностью

Purpose of the course:

1.To develop the students to assess the current security landscape, including the general status of common vulnerabilities, and the likely consequences of security failures;

2.To develop the students critique and asses the strengths and weaknesses of general cyber security models, including CIA triad..

Tasks of the course:

1.To develop the students appraise the interrelationships among elements security system, including hardware, software, policies, and people.

2. To develop the students to understand how the organizations are managing cyber security concern, Designing and the Cyber security solution for Organization, Component .of devices, forming integrating technology for cyber security issues. The existing methods used for effective Cyber security solutions.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

1.The students will be able to understand in depth the cyber security overview and principles behind theory of risks.

2.The students will be able to understand the concept of implementing the cyber security solutions in the organization.

be able to:

the students would be able to assessment the risk posed by the threat landscape of cyber space.

master:

1.The students would be able to learn the anatomy of cyber-attack and this will help them in future to design new solutions.

2.The students would be able to learn the defense technology for cyber threat and will try to understand how it works.

Content of the course (training module), structured by topics (sections):

1. The concept of risk cyber-attacks

Setting the task of assessing the risk of an attack. Risk structure. Invariants, functions of security. Examples of programming security functions using neural networks in Matlab.

2. Logical-probabilistic approach to risk assessment

LP-polynomials. Comparative analysis of the security of the risk object. Examples of programming LP-polynomials in Matlab.

3. Destabilizing factors and security functions

Completeness and content nature of the system of security functions for any attack. Cause-and-effect diagram of security functions. Examples of programming a cause-and-effect diagram of risk object security functions in Matlab.

4. Criteria for the security of the cyber-attack object. Risk Assessment

Condition for the security of the risk object. Assessment of the security of the risk object. Examples of programming the algorithm for assessing the security of a risk object in Matlab.

5. Risks evaluation

Updated security condition for the risk object. New gradations of security functions. Examples of programming new gradations of risk object security functions in Matlab.

6. Enterprise Role and Structure

Platform as a service: current state, opportunities. Tools for tracking cyber-attacks. Examples of programming tools for tracking cyber-attacks in Matlab.

7. Security Metrics and Measurements

Risk assessment of a DDoS attack. Assessment of the risk of spam. Examples of programming the risk assessment of a specific cyber-attack in Matlab.

8. Cyber Security Anatomy

Secure private and public cloud models. Requirements for secure Hypervisors in cloud technologies. Examples of programming sensors for detecting malicious traffic in public clouds in Matlab.

9. Cyber Security Controls

Models for secure management of cloud systems. Examples of programming algorithms for event analysis in control procedures of cloud systems in Matlab.

10. Testing and Validation of Security Devices

Repelling cyber attacks. Providing guaranteed quality of service (QoS) in cloud infrastructures. Information security as a quality of service. Examples of programming algorithms for repelling cyber attacks in cloud infrastructures in Matlab.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

History, Philosophy and Methodology of Natural Science/История, философия и методология естествознания

Purpose of the course:

To familiarize students with the historical experience of world philosophical thought, give a clear idea of the main stages, directions and problems of the history and philosophy of science, contribute to the formation of skills to work with extreme issues related to the boundaries and foundations of various sciences and scientific rationality, and mastery of the principles of a rational philosophical approach to processes and trends in the development of modern science.

Tasks of the course:

- systematic study of the philosophical and methodological problems of natural science, taking into account the historical and philosophical context and the current state of science;

- the acquisition by students of theoretical ideas about the diversity of forms of human experience and knowledge, the nature of thinking, the ratio of truth and error;

- understanding the role of science in the development of civilization, the relationship between science and technology and related modern social and ethical problems, the ability to distinguish between historical types of scientific rationality, to know the structure, forms and methods of scientific knowledge in their historical genesis, modern philosophical models of scientific knowledge;

- acquaintance with the main scientific schools, directions, concepts, with the role of the latest information technologies in the world of modern culture and in the field of humanities and natural sciences;

- understanding the meaning of the correlation of biological and social in man, man's attitude to nature, discussions about the nature of changes taking place with man and humanity at the turn of the third millennium;

- knowledge and understanding of the dialectic of personality formation, its freedom and responsibility, the uniqueness of the intellectual, moral and aesthetic experience of different historical eras.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

 - the structure of the natural and socio-humanitarian sciences, the specifics of their methodological appa-ratus;

 - the ratio of principles and hypotheses in the construc-tion of scientific systems and theories;

 - the foundations of a modern scientific picture of the world, the basic principles of scientific knowledge and key areas of interdisciplinary research;

 - concepts of the development of science and different approaches to the problem of the cognitive status of scientific knowledge;

 - the problem of matter and motion;

 - concepts of energy and entropy;

 - problems of space-time;

 - modern problems of physics, chemistry, mathematics, biology, ecology;

 - great scientific discoveries of the XX and XXI centu-ries;

 - key events in the history of the development of science from ancient times to the present day;

 - the relationship of worldview and science;

 - the problem of forming a worldview;

 - a system of interdisciplinary relations in science, the problem of reductionism in science;

 - theoretical models of fundamental processes and phenomena in physics and its applications to the natural sciences;

- about the Universe as a whole as a physical object and its evolution;

- about the relationship between order and disorder in nature, about the problems of non-linear processes and self-organizing systems;

- dynamic and statistical patterns in nature;

- of the role of probabilistic descriptions in the scientific picture of the world;

- principles of symmetry and conservation laws;

- The latest discoveries of natural science for the creation of technical devices;

- Features of the biological form of organization of mat-ter, principles of reproduction and development of living systems;

- About the biosphere and the direction of its evolution.

be able to:

 - effectively use in practice the theoretical components of science: concepts, judgments, conclusions, hypotheses, evidence, laws;

 - apply the methodology of science in the organization of specific research;

- - give a panorama of the most universal methods and laws of modern science.

master:

- - scientific methodology as the initial principle of cognition of the objective world;
- - the principles of choosing an adequate methodology for the study of specific scientific problems;
- - system analysis;
- - knowledge of the scientific picture of the world;
- - the conceptual and methodological apparatus of interdisciplinary approaches in science.

Content of the course (training module), structured by topics (sections):

1. The formation of science and philosophy in the West and in the East.

The problem of the emergence of science in antiquity. Prescription and applied nature of knowledge in the Ancient East. The birth of philosophy. Scientific programs of Plato, Aristotle and Democritus. The origin of ancient science: mathematics, physics, astronomy and biology. The problem of the social organization of ancient science. "Musical" cult and scientific and philosophical schools. The Alexandrian Museyon and the further development of Hellenistic science. The science of ancient Rome. Arab medieval science.

Science in Europe in the Middle Ages. Christianity and science The dispute of faith and reason. Rethinking Antique Heritage. Medieval empiricism. Nikolay Kuzansky and the concept of infinity. The ideological turn of the Renaissance.

2. The main periods and basic forms of the development of science

The emergence of modern science: basic concepts and key personalities. Key research programs in modern European science. The triumph of Newtonian physics and the formation of mathematical science. Central theoretical postulates and methods of classical science.

3. Rationalistic and empiricist traditions in the philosophy of the Modern Times

The dispute of rationalism and empiricism Rationalistic direction: the method of deduction and the concept of intellectual intuition in the philosophy of Descartes and Spinoza. Cartesian probabilism. The theory of innate ideas. Leibniz’s teaching on the “truths of fact” and “truths of the mind”, on the types of knowledge, on analysis and synthesis. Rationalist interpretation of the thesis of the correspondence of being and thinking.

The tradition of English empiricism: Bacon's doctrine of experience, the role of induction, the “idols” of knowledge. Locke's model of scientific knowledge. Berkeley thesis: to be means to be perceived. Humeian skepticism and psychologism, criticism of the concept of causality.

4. Kant’s solution of the problem of knowledge

Kant's solution to the problem of knowledge. The question of the possibility of knowledge. Space and time as forms of sensuality. The construction of objectivity in the process of cognition. Reason as a legislator. The specifics of Kant's understanding of thinking. Critique of the possibility of supersensory knowledge The concept of "things in themselves." Antinomies of the mind.

5. The approach to knowledge in neokantian philosophy

Interpretation of knowledge in neo-Kantianism. Marburg and Baden schools of neo-Kantianism. Neo-Kantian development of the theory of knowledge. Division of sciences into nomothetic and idiographic. The problem of values in the Baden school.

6. Positivism

Positivism and postpositivism. The first and second positivism of the XIX century. Analytical philosophy of B. Russell and L. Wittgenstein. Logical positivism and the “linguistic turn”. Postpositivism of K. Popper, T. Kuhn and I. Lakatos.

7. Critique of positivism from the point of view of logic. Critical rationalism of Karl Popper

Logical criticism of positivism by K. Popper: problems of induction and demarcation; falsification principle; attitude to the truth. K. Popper's concept of science growth: fallibilism and likelihood theory. The development of modern cosmology and elementary particle physics.

8. Historical criticism of positivism. Historical approach in the philosophy of science.

Historical criticism of positivism. Are there “crucial experiments”? The thesis of the "incommensurability of theories." The Kuhn’s model of the development of science: the scientific community and the scientific paradigm, “normal” and “abnormal” phases in the history of science. The model of research programs by I. Lakatos: “hard core” and “protective belt of hypotheses”; “Progressive problem shift” as a criterion for rejecting research programs. Historical Relativism of P. Feyerabend.

The dispute between realism and antirealism in modern philosophy of science. Sociologization of modern philosophy of science. The debate about the model of the "external" and "internal" history of Lakatos. Laboratory place in science. The relationship of science and technology in the second half of the XX - beginning of the XXI century.

9. The structure of scientific knowledge

The structure of science. Place of mathematics and measurements. Place of foundations and theories of phenomena. Place of methodological principles.

10. Philosophical problems of natural sciences

The concept of dynamic and statistical laws and probability as an objective characteristic of natural objects. Place of principles of symmetry and conservation laws.

Synergetics, selforganization and the ratio of order and disorder. Model of global evolutionism.

Specific features of life sciences. Question of the reduction of biology and chemistry to physics. Contradictions between nature and man today. Global problems of modern civilization, the

possibility of environmental disaster. Biosphere, noosphere, ecology and the problem of sustainable development.

Interdisciplinary approaches in modern science.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Information Security in the Cloud/Информационная безопасность в облаке

Purpose of the course:

To provide students with knowledge and understanding of cloud cybersecurity.

Explore and learn how to apply classic security techniques to today's cloud security problems.

Tasks of the course:

- mastering by students of approaches, methods of searching for cloud security vulnerabilities using standard systematic methods.

- acquiring practical skills in creating your own implementations of cloud infrastructure and web services, developing security solutions for them.

- the acquisition of the ability to use classical security concepts such as least privilege and separation of duties, as well as more technical methods of cryptography and access control.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

- how to secure network, infrastructure, data and applications in cloud

- how to create and secure private network in cloud

- ways of monitoring, logging and auditing in cloud

- identify the risks based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs).

- how to detect and respond to security incidents in the cloud and take appropriate steps.

be able to:

- create accounts and use the services on any one the leading CSPs

- secure access to the consoles used to access the CSP environments.

- evaluate the logging services of various CSPs and use those logs to provide the necessary accountability for events that occur in the cloud environment.

- implement, configure, and secure certificate-based SSH authentication to virtual machines launched in the cloud.

- configure the CLI and properly protect the access keys to minimize the risk of compromised credentials.

- use basic Bash and Python scripts to automate tasks in the cloud.

- implement network security controls that are native to both AWS and Azure.

- employ an architectural pattern to automatically create and provision patched and hardened virtual machine images to multiple AWS accounts.

- use AWS and Azure best practices for security.

- deploy a complete "infrastructure as code" environment to multiple cloud providers.

master:

- tools of monitoring and audit Cloud resources for continuous security in cloud

- methods to use AWS managed security services to automate security,

- use application security tools and threat modeling to assess the security of cloud-based web applications.

- automatically create and provision patched and hardened virtual machine images.

Content of the course (training module), structured by topics (sections):

1. Accessing the web management consoles of cloud infrastructure.

Accessing the web consoles AWS, Azure, GCP, and launching virtual machines in select environment. Web Consoles.

Practical launch Virtual Machines in AWS and Azure. VPCs. Hardened Image Provisioning.

2. AWS Security Center and Azure

Security of a Software-as-a-Service offering. Platform-as-a-Service AWS and Azure.

3. Hardening and securing cloud environments and applications.

Using security tools and services. Securing Console Access. Hardening, patching, and securing virtual machine images, including SSH.

4. Command line interface (CLI)

Using simple scripts to automate work.

5. Logs and security services to detect malware on a cloud virtual machine.

Secrets leakage in code deployed to the cloud. Cloud Log Retrieval & Parsing. Open-Source Tool to Audit an AWS Account.

6. Government Clouds.

Transport-level encryption with HTTPS. Advanced Threat Protection. Control network access. Azure Security Center. Key Vault.

7. Implementation enterprise governance strategies

Role-based access control, Azure policies, and resource locks.

8. Azure AD infrastructure, users, groups, and multi-factor authentication.

Azure AD Identity Protection, risk policies, conditional access, and access reviews. Azure AD Privileged Identity Management, Azure AD roles and Azure resources. Azure AD Connect including authentication methods and on-premises directory synchronization.

9. Perimeter security strategies,

Azure Firewall. Network security strategies, Network Security Groups and Application Security Groups.

Host security strategies, endpoint protection, remote access management, update management, and disk encryption.

10. Container security strategies

Azure Container Instances, Azure Container Registry, and Azure Kubernetes. Azure Key Vault including certificates, keys, and secretes. Application security strategies, app registration, managed identities, and service endpoints.

11. Storage security strategies.

Shared access signatures, blob retention policies, and Azure Files authentication. Database security strategies, authentication, data classification, dynamic data masking, and always encrypted.

12. Azure Security Center.

Policies, recommendations, and just in time virtual machine access.Azure Monitor, connected sources, log analytics, and alerts.

13. Azure Data Lake enterprise-class security features.

Transport-level encryption with HTTPS. Advanced Threat Protection. Control network access. Azure Security Center. Key Vault.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Intelligent Technology for Information Security/Интеллектуальные технологии в информационной безопасности

Purpose of the course:

1. To provide students skills of development of methods for the generation of hypotheses about risk-models web-attacks in a highly dynamic web systems.

2. Acquisition of skills of analyzing the applicability of neuro-fuzzy and Bayesian approaches (combining a priori and observed data) to the synthesis of intellectual systems of decision making on information security incidents and development of mechanisms for web programming in Hadoop.

Tasks of the course:

The formation of practical skills of application of the studied methods and schemes of reasoning when making decisions on combating web-based attacks in conditions of multiple choice.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

The students mastering approaches, methods and models for the analysis of the dynamics of the processes of information warfare different nature.

be able to:

The acquisition of practical skills of application of risk models and methods of the multidimensionality of the data for identifying the parameters of web-based attacks, and retrieval of knowledge in information warfare.

master:

The acquisition of the ability to interpret the results obtained to build scenarios, forecasts, decision making with the aim of countering web injection attacks and explain the nature of arising in information and communication systems information security incidents.

Content of the course (training module), structured by topics (sections):

1. The methodology of a systematic risk analysis of Infocommunications.

Historical information about formation of scientific discipline – a systematic analysis of risks of Infocommunications. Basic Concepts of information warfare on the Internet.

Examples of programming information warfare in Matlab.

2. Examples of information warfare. The formal statement of the research problem.

Characteristics features of complex systems: uniqueness, weak structuring of theoretical and factual knowledge about the systems, the composite character

(multi protocols), the heterogeneity of subsystems and elements, randomness and uncertainty factors operating in the systems, the multicriteriality assessment processes (games with conflicting interests), large dimension, continuity of variables and non-monotonicity in the dynamics, the subjectivity in the description of complex systems. Integral characteristics. General property.

Examples of programming infocommunications in Matlab.

3. Overviev: globalism and the case of Azia and Africa blocs.

The limits of applicability of probabilistic risk assessment approaches attacks. Completeness, invariance of casual diagram risk attack. Examples of programming a value at risk of object of risk in Matlab.

4. Criteria for the security of the cyber-attack object. Risk Assessment.

Condition for the security of the risk object. Assessment of the security of the risk object. Examples of programming the algorithm for assessing the security of a risk object in Matlab.

5. Risks evaluation.

Updated security condition for the risk object. New gradations of security functions. Examples of programming new gradations of risk object security functions in Matlab.

6. Risks analysis methods and mathematical techniques used in intelligent systems information security.

Extreme risk assessment. Metrics for risk assessment. Maximization, extremal problems, multi extremal problems. Examples of programming tools for risk assessmant in Matlab.

7. Modeling web-based attacks

Class of models. The process of identification in a system-oriented modeling in the cloud. Examples of programming bot-attacks in Matlab, Hadoop.

8. Premodernity analysis: goal setting.

Modeling steps, setting goals, building an information structural-functional environment, the construction of the logical DBMS environment. verification. Examples of programming logical DBMS environment in Matlab, Hadoop.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Machine Learning Techniques for Cybersecurity/Методы машинного обучения применительно к кибербезопасности

Purpose of the course:

To study of machine learning methods in the application for solving cybersecurity tasks, as well as preparing students for further independent work, using practical skills of machine learning algorithms.

Tasks of the course:

1. To provide students with in depth knowledge and understanding of the machine learning techniques in respect of applications for cybersecurity tasks solutions;

2. To develop practical skills in using machine learning algorithms.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

theoretical foundations and principles of machine learning;

classes of models and quality metrics;

approaches to the preparation and preprocessing of data;

basic approaches to the generation and selection of features;

basic concepts used in the description of learning algorithms;

basic concepts for describing decision trees; operations with trees;

multilayer perceptron, convolutional, recurrent, and generative adversarial networks;

dataset augmentation methods;

features of the pre-trained models using (transfer learning);

algorithms with adaptive learning rates;

distance measures, hierarchical and flat, clear and fuzzy clustering algorithms.

be able to:

use machine learning algorithms for solving classification tasks;

use machine learning algorithms to solve clustering tasks;

use machine learning algorithms to predict time series;

use neural network algorithms for intrusion detection;

use decision trees;

use anomaly detection algorithms

master:

skills to handle data used in intrusion detection systems.

skills to apply the studied machine learning algorithms for solving applied data processing tasks in the field of cybersecurity

Content of the course (training module), structured by topics (sections):

1. Introduction to Learning Systems.

Theoretical foundations and principles of machine learning, classes of models (linear, logical, neural network), quality metrics, approaches to data preparation, data preprocessing, generation and selection of signs, exploratory data analysis, data and model interpretation methods.

2. Machine Learning Theory

Learning Algorithms (Task, Performance Measure, unsupervised upervised Experience), Capacity, Overfitting and Underfitting, Regularization, Hyperparameters and Validation Sets, Optimization, Cross-Validation, Estimators, Bias and Variance, Maximum Likelihood Estimation, Bayesian Statistics, Supervised Learning Algorithms, Unsupervised Learning Algorithms, Stochastic Gradient Descent.

3. Decision Trees Algorithms

Sample Complexity, Classification and Regression Trees, Gini Index, Iterative Dichotomiser 3, Entropy function and Information gain, Chi-square automatic interaction detection, Implementations of the Gain Measure, Pruning, Threshold-Based Splitting Rules, Gradient tree boosting, AdaBoost, Random Forests

4. Deep Learning (Practice, Programming).

Multilayer perceptron. Convolutional neural networks. Recurrent neural networks. Generative-competitive networks. Activation functions. Optimization functional. Loss function. The problem of retraining and the generalizing ability of a neural network. Back propagation error. Computational graph. The problem of vanishing gradients and normalization. Regularization. Dataset augmentation. Transfer learning (pre-trained model). Noise resistance. Stochastic Gradient Descent. Parameter initialization strategies. Algorithms with adaptive learning rates AdaGrad, RMSProp, Adam. Algorithms for automatic optimization of hyperparameters. Grid Search and Random Search.

5. Machine Learning for Classification Tasks.

Practical classification tasks in the field of cyber security. E-mail Spam Classification. Internet Resources Classification. Malicious Programs Classification. Network Attacks Classification.

6. Machine Learning for Clustering Tasks

Practical clustering tasks, Clustering concept, Distance measures, Hierarchical and flat algorithms, Clear and Fuzzy Algorithms, Clusters Combining, DBSCAN algorithm

7. Machine Learning for Time Series Prediction.

Exponential Smoothing Models, Moving Average Models, Trend Models, Bootstrapping, Autoregressive Models, ARMA, ARIMA, GARCH, Adaptive Autoregression, Prediction of Distribution Density.

8. Intrusion Detection Using Neural Networks.

Practical intrusion detection tasks.

9. Anomaly Detection

Practical Anomaly Detection Tasks, Outlier Detection, Novelty Detection, Extreme-Value Analysis, Statistical tests, Iterative methods, Metric methods, Task substitution methods, Isolating forest, Algorithm ensembles

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Neural Network Based Intrusion Detection System/Нейросетевые системы обнаружения компьютерных атак

Purpose of the course:

To provide students development skills of methods for the generation of hypotheses about risk-models web-attacks in a highly dynamic web systems.

Tasks of the course:

1. The formation of practical skills of application of the studied methods and schemes of reasoning when making decisions on combating web-based attacks in conditions of multiple choice.

2. Acquisition of skills of analyzing the applicability of neuro-fuzzy and Bayesian approaches (combining a priori and observed data) to the synthesis of intellectual systems of decision making on information security incidents and development of mechanisms for web programming in Hadoop.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

- Students mastering approaches, methods and models for the analysis of the dynamics of the processes of information warfare different nature.

be able to:

1. The acquisition of practical skills of application of risk models and methods of system analysis in terms of the multidimensionality of the data for identifying the parameters of web-based attacks, and retrieval of knowledge in information warfare;

2. Optimize the code using the features and methods of system analysis in terms of the multidimensionality of the data for identifying the parameters of web-based attacks.

master:

- The acquisition of the ability to interpret the results obtained to build scenarios, forecasts, decision making with the aim of countering web injection attacks and explain the nature of arising in information and communication systems information security incidents.

Content of the course (training module), structured by topics (sections):

1. Own risk analysis methods and mathematical techniques used in intelligent systems information security

Extreme risk assessment. Metrics for risk assessment.Traditional methods of system analysis of complex systems: a matrix, systematisations, graph, stochastic models.

Maximization, extremal problems, multiextremal problems. Search methods of local and global extrema of functions.

Linear programming - formulation of the problem. The algorithm of the simplex method. The concept of the method of ellipsoids. The algorithm is an internal point. Linearization of mathematical programming problems.

Other methods of system analysis:

1) cluster analysis;

2) minimax, multi-objective optimization;

3) operations research;

4) decision-making and decision-making processes, decision support (dss), the comparison and selection criteria, comparison of alternatives;

5) the mathematical theory of experiment planning;

6) the task network planning and analysis of graphic designs.

2. Practical examples of the applicability of the models.

Practical examples of the applicability of the models.

3. Modeling web-based attacks

Main tasks and methods. System modeling botnet attacks. Components of system modeling: mathematical modeling, computer modeling, information modeling, modeling of decision making, simulation, optimization models, probabilistic (stochastic) simulation. System-integrated modeling. Principles. Class of models. The process of identification in a system-integrated modeling in the cloud. Environment of web programming, Hadoop.

4. The use of ITU experience.

The use of ITU experience.

5. Premodernity analysis: goal setting.

Modeling steps: setting goals, building an information structural-functional environment, the construction of the logical DBMS environment, verification.

Goals and objectives depending on the purpose of the model: a generic model of problem-based model, global and local model. Accuracy, time horizon, objects, functional connectivity, species descriptions (logical and probabilistic equations, neuro-fuzzy design of decision-making on security incidents).

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Russian as a Foreign Language/Русский язык как иностранный

Purpose of the course:

The Russian as a foreign language (A2) course is aimed at the formation of intercultural professionally oriented communicative competence from the zero level to the elementary level (according to the European scale of foreign language proficiency levels) for solving social and communicative tasks in various areas of everyday, cultural, professional and scientific activities in the Russian language, as well as for further self-education.

Tasks of the course:

The tasks of the formation of intercultural, professionally oriented communicative competence consist of the gradual mastery by students of a set of competences, the main of which are:

– linguistic competence, i.e. the ability to adequately perceive and correctly use language units based on knowledge of phonological, grammatical, lexical, stylistic features of the studied language;

– sociolinguistic competence, i.e. the ability to adequately use realities, background knowledge, situationally conditioned forms of communication;

– sociocultural competence, i.e. the ability to consider during the communication speech and behavioral models adopted in the relevant culture;

– social competence, i.e. the ability to interact with communication partners, to make contact and maintain it, owning the necessary strategies;

– strategic competence, i.e. the ability to apply different strategies to maintain successful interaction in oral/written communication;

– discursive competence, i.e. the ability to understand and generate foreign language discourse considering cultural differences;

– general competence, including, along with knowledge about the country and the world, about the features of the language system, also the ability to expand and improve their own picture of the world, to be guided by the media sources of information;

– intercultural competence, i.e. the ability to achieve mutual understanding in intercultural contacts, using the entire set of skills to realize the communicative intention;

– compensatory competence, i.e. the ability to avoid misunderstandings, to overcome the communication barrier through the use of well-known speech and metalanguage means.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

– The main facts, realities, names, attractions, traditions of Russia;

– some achievements, discoveries, events in the field of Russian science, culture, politics, social life;

– basic phonetic, lexical-grammatical, stylistic features of the Russian language and its difference from the native language;

– the main differences in writing and speaking.

be able to:

– Generate adequate oral and written texts in a specific communication situation;

– to realize the communicative intention with the purpose of influencing the communication partner;

– adequately understand and interpret the meaning and intention of the author in the perception of oral and written authentic texts;

– identify similarities and differences in the systems of native and foreign languages;

– show tolerance, empathy, openness and friendliness when communicating with representatives of another culture.

master:

– Intercultural professionally oriented communicative competence in different types of speech activity at the level of A2;

– social and cultural competences for successful mutual understanding in terms of communication with representatives of another culture;

– various communication strategies;

– learning strategies for organizing the learning activities;

– strategies of reflection and self-evaluation for self-improvement of personal qualities and achievements;

– different methods of memorization and structuring digestible material;

– Internet technologies to select the optimal mode of obtaining information.

Content of the course (training module), structured by topics (sections):

1. My World

Communicative tasks. To talk about your everyday activity. To tell the time. To make an appointment. To talk about your family. To fill the registration form.

Vocabulary. Verbs describing everyday activity. Time. Parts of the day. Numbers 10-100. Events. Family. Registration form.

Grammar. 1st conjugation of verbs. 1 час, 2-4 часа, 5-20 часов. Consolidate conjugation of verbs. Possessive adjectives: мой/моя, твой/твоя.

Phonetics. Pronunciation of sounds: т, ть. Pronunciation of [ц], unstressed «я», «е». Pronunciation of [ж], [ш]. Devocalization of sound «ж» at the end of words.

2. Our Lesson

Communicative tasks. To understand your teacher's instructions in Russian. To ask people if they have something. To indicate something. To set a meeting. To talk about your plans for a week.

Vocabulary. Verbs describing activities at the lesson. Personal things. Numbers 100-1000. Days of week. Events.

Grammar. Imperative form of verbs - читайте, слушайте etc. Construction "у меня есть". Gender of nouns. Construction "У меня + событие". Nouns in plural. Days of week.

Phonetics. Pronunciation of "o" in unstressed position. [ж], [ш]. Devocalization of sound «ж» at the end of words. Pronunciation of у, г.

3. In the City

Communicative tasks. To talk about your city. To ask where to go. To understand signs of a city. To buy a ticket for metro. To order in a restaurant. To refuse an offer. To say where you were yesterday.

Vocabulary. Places in town (parks, restaurants, museums etc.). Words for ordering in a café or buying a ticket for metro. Russian way to say "last/next week".

Grammar. Endings of adjectives. Possessive pronouns. The prepositional case for locations. The past tense of the verb "to be".

Phonetics. Devocalization "д" at the end of words and in front of voiced consonants. Practicing the phrase "к сожалению". Words where "ч" is pronounced as [ш].

4. My Home

Communicative tasks. To describe your house. To call for a master to fix broken things at home. To explain location of things in the house. To talk about your free time and ways to rest at home.

Vocabulary. Furniture. Rooms. Verbs (to sleep, to want, to see, to watch, to hate). Parts of a house (wall, floor etc.). Outside the house (garden, forest). Verbs describing activities at home.

Grammar. Neuter gender nouns in plural. Masculine gender nouns in plural. Exceptions. The prepositional case, exceptions. The past tense. The accusative case for objects.

Phonetics. Pronunciation of the names of the rooms. Pronunciation of words with a change of stress in the prepositional case (в лесу, на полу, etc.). Pronunciation of [х]. Being surprised by the word "ух ты!"

5. Tasty Food

Communicative tasks. To explain what you need to buy. To talk about food preferences. To order and pay in a restaurant. To talk about recipes. To invite friends for dinner. To express admiration or criticism.

Vocabulary. Phrases for shopping. Phrases for restaurants. Phrases for inviting and accepting invitations.

Grammar. Personal pronouns with “нужно”, “надо”, “нравится”. The instrumental case after the preposition “с”. The future tense.

Phonetics. Pronunciation [ы], [и]. Devocalization of the voiced consonants at the end of words (б, д, в, з, ж, г). Intonation of admiration: “Как хорошо!”

6. Health

Communicative tasks. To talk to a doctor. To talk about health. To give recommendations. To talk about mood (I am sad, happy etc.). To agree/disagree.

Vocabulary. Parts of body. Health. Можно/нельзя. Emotions. Mood.

Grammar. Construction “у меня был”. Personal pronouns of with age, “можно”, “нельзя”. Short forms of adjectives.

Phonetics. Intonation of the interjection "ай!" when expressing pain. Pronunciation of ь, ъ.

7. People

Communicative tasks. To talk about people’s character. To describe appearance. To compare things. To buy clothes. To agree to do something.

Vocabulary. Adjectives. Describing a person. Adjectives. Appearance. Clothes. Colors. Size.

Grammar. Endings of adjectives. The comparative and superlative degree. The genitive case in possessive constructions. Endings of adjectives.

Phonetics. Pronunciation of [ш], [щ]. Combination «дж». Intonation of admiration urprise using the word “так”. Pronunciation of “ё” after the hushing sounds.

8. Transport

Communicative tasks. To talk with a taxi driver (price, address, etc.). To order a taxi. To cancel, reschedule or confirm a meeting. To talk about your trip. To describe cities.

Vocabulary. Transport. Dates. Verbs: перенести, отменить, подтвердить, прийти/приехать, уйти/уехать. The compass. Words for travelling.

Grammar. The prepositional case for transport. Ordinal numbers. The accusative case for directions with prepositions “в”, “на”.

Phonetics. Practicing the difference of pronunciation between "е" and "ё" in the conjugation of the verbs "идти", "ехать". Words where the letter "г" is pronounced as "в" (его, сегодня). Devocalization "з" in the preposition "из".

9. My Family

Communicative tasks. To talk about family. To accept the invitation. To talk about hobbies. To refuse the invitation. To ask and tell about biography.

Vocabulary. Family. Relatives. Activities during the holidays. Verb “уметь”. Verbs: пожениться, родиться, случиться, познакомиться.

Grammar. The genitive case. Possession. Reflexive verbs (the present tense). Заниматься + the instrumental case. Reflexive verbs (the past tense).

Phonetics. Devocalization of sound “ж” at the end of words. Pronunciation of тс, тьс = [ц]. Pronunciation of и = [ы] after ш, ж, ц.

10. Holidays

Communicative tasks. To congratulate with holidays. To tell about traditions. To sign postcards. To say wishes. To suggest the idea of gifts. To express surprise.

Vocabulary. Name of the holidays. Verbs: праздновать, поздравлять, прощаться, гулять. Wishes (happiness, love, luck, etc.). Gifts.

Grammar. Поздравлять + the instrumental case. The genitive case with the verb желать. The genitive case after prepositions.

Phonetics. Words with an unpronounceable "д". Words where г = [в]. Intonation of the phrase "Да ладно?!"

11. Shopping

Communicative tasks. To understand the information on the labels of cosmetic products. To buy groceries. To communicate in the store. To buy clothes.

Vocabulary. Body parts. Cosmetic. Stores. Numbers and time. Fruits and vegetables. Clothes, shoes, accessories. In the store.

Grammar. The genitive case. Plural. The genitive case with numbers. The genitive case.

Phonetics. Devocalization of "в" at the end of words. Devocalization of paired voiced consonants before voiceless consonants. The difference in pronunciation between "большой" and "больше".

12. Countries and Nationalities

Communicative tasks. To ask a person where he he is from. To talk about countries. To talk about the weather. To talk about the season. To talk about traditions and nationalities.

Vocabulary. Countries. Months. Weather. Season. Verbs (to love, to call, to speak). Traditions and nationalities.

Grammar. Months in the prepositional case (when?). 2nd conjugation of verbs. Nationalities.

Phonetics. Pronunciation of р, рь, ю. Pronunciation of the names of nationalities.

Annotation

Major: 03.04.01 Прикладные математика и физика

specialization: Cyber Security/Кибер-безопасность

Vulnerabilities and Attacks/Уязвимости и атаки

Purpose of the course:

Studying the relevance of the problem of information technology protection in modern conditions and creating a coherent and consistent security system in the field of accumulation, use and protection of information .

Tasks of the course:

1. Provide students with in-depth knowledge and understanding of building and administering infrastructure from a cyber defense perspective.

2. Develop students ' engineering skills to protect against cyber- attacks using information and network technologies in practice.

List of the planned results of the course (training module)

As a result of studying the course the student should

know:

- basic concepts of building secure local and global networks,

- scope of application of traditional and modern network technologies,

- variety of network protocols and standards,

- principles of operation of various types of communication and information security equipment,

- basics of the TCP/IP Protocol, routing and IP addressing, CIDR method (Classless Inter-Domain Routing - classless inter-domain routing). Methods for the detection of vulnerabilities and identification of cyber-attacks,

- understanding the range of issues related to data protection in networks,

be able to:

- use the advantages and disadvantages of various network technologies to solve a variety of security applications,

- explain the differences between different types of network architectures and their impact on information security,

- describe typical hardware components used for data transmission in the network. Approaches to the synthesis of new safe technologies,

- describe the principles and protocols of remote communication with the solution of information security problems " from end to end»,

master:

skills in building structural schemes of secure local networks and networks that include global communications,

using various models of secure data exchange in the communication network,

skills in applying the studied information network technologies to solve applied problems of ensuring information security of various risk objects.

Content of the course (training module), structured by topics (sections):

1. Model of the offender information safety of computer networks and systems.

Model of threats to information security of software and hardware and software of various risk objects.

Method of forming a profile of protection of risk objects for various purposes.

Examples of programming the selected security profile in the Matlab environment.

2. Checking the functionality of protected fragments of Infocommunications.

Structure of the hardware and software complex for conducting research on the characteristics of secure Infocommunications.

Cloud-based security monitoring cluster.

Examples of programming fragments of a system security monitoring cluster in the Matlab environment.

3. General provisions for the organization of network protection.

Formation of inter-network interaction policy.

Basic wiring diagrams for firewalls.

Examples of programming the firewall connection scheme for a risk object in Matlab.

4. Criteria for the security of the cyber attack object.

Condition for the security of the risk object. Assessment of the security of the risk object. Examples of programming the algorithm for assessing the security of a risk object in Matlab.

Examples of programming new gradations of risk object protection functions in Matlab.

5. Risk analysis methods and mathematical techniques used in intelligent systems for information security.

Extreme risk assessment. Metrics for risk assessment. Maximization, extremal problems, multi extremal problems.

Examples of programming tools for risk assessmant in Matlab.

6. Modeling web-based attacks.

Class of models. The process of identification in a system-oriented modeling in the cloud. Examples of programming bot-attacks in Matlab, Hadoop.

7. Premodernity analyses: goal settings.

Modeling steps, setting goals, building an information structural-functional environment, the construction of the logical DBMS environment. verification.

Examples of programming logical DBMS environment in Matlab, Hadoop.