KHMELNYTSKYI NATIONAL UNIVERSITY

APPROVED
Dean of IT Faculty
_____ Tetiana HOVORUSHCHENKO
"29" August 2025

WORKING PROGRAMME OF THE EDUCATIONAL COMPONENT

Computer Networks Protection and Monitoring

Field of study F – Information technology

Major F5 – Cyber Security and Information Protection

Educational program – Cyber Security and Information Protection

Course status: optional, professional training course

Faculty – Information Technologies

Department – Cyber Security

Study mode	Total load		Number of hours						Semester control form
			Contact Hours					Independent Work (incl. Individual tasks)	
	ECTS credits	Hours	Total	Lectures	Laboratory works	Practical classes	Seminar classes		pass/ fail test
F	8	240	66	32	34			174	+

The working program is based on the Educational and Professional Program "Cybersecurity and information protection" within the specialty F5 "Cybersecurity and information protection".

Program's author _____ Natalia PETLIAK

Approved at the meeting of the Department of Cybersecurity
Minutes No. 1 dated August 29, 2025

Head of the Department _____ Yurii KLOTS

Khmelnytskyi 2025

COMPUTER NETWORKS PROTECTION AND MONITORING

Course type	Optional
Education level	Second (master's)
Language of instruction	English
Semester	–
Number of ECTS credits	8
Course study mode	Full-time

Learning outcomes. A student who has successfully completed the course is required to: *know* the basic concepts of computer systems and their components; *protect* edge traffic and establish access control for additional protocols and tools; *examine* and analyze the architecture of the fence, which supports advanced security features; *expand* the security policy based on models of attacks on the target object (business); *analyze* computer measurements using additional tools for auditing and monitoring.

Course content. Basic concepts of computer network protection. Firewalls and their functions in network protection tasks. Firewalls. Remote access security. Network administration. Concepts of network protocols and services. Basics of TCP/IP protocol functioning. DNS service. Architecture of protected computer networks. Design and installation of protected computer networks. Information security policy of an enterprise network. Methodology of attacks on computer networks. Classification of attacks on computer networks. Analysis and modeling of network security threats. Analysis of computer network security. Technologies for detecting attacks in computer networks. Methods of managing network security tools. Security audit of computer networks.

Planned academic activity: at least 1/3 of the planned volume of the discipline.

Teaching methods: verbal and visual (lectures); practical and search (laboratory works), explanation and illustration, research (independent work).

Assessment forms and methods: defense of laboratory works, written control.

Type of semester control: test.

Навчальні ресурси:

1. Tekhnolohii zabezpechennia bezpeky merezhevoi infrastruktury/ V. L. Buriachok, A. O. Anosov, V. V. Semko, V. Yu. Sokolov, P. M. Skladannyi. K.: KUBH, 2019. 218 s.
2. Informatsiina bezpeka v kompiuternykh merezhakh: navch. posib./ [O.A. Smirnov, O.K. Konoplitska-Slobodeniuk, S.A. Smirnov, K.O. Buravchenko ta in.] – Kropyvnytskyi: Vydavets Lysenko V.F., 2020. 295 s.
3. Informatsiina bezpeka: navchalnyi posibnyk/ [Iu. Ya. Bobalo, I. V. Horbatyi, M. D. Kiselychnyk, A. P. Bondariev ta in.]; za zah. red. d-ra tekhn. nauk, prof. Yu. Ya. Bobala ta d-ra tekhn. nauk, dots. I. V. Horbatoho. Lviv: Vydavnytstvo Lvivskoi politekhniky, 2019. 580 s.
4. Modulne seredovyshche dlia navchannia. Dostup do resursu: https://msn.khnu.km.ua.
5. Elektronna biblioteka universytetu. Dostup do resursu: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php

Викладачі: PhD N. Petliak

INTRODUCTION

The course «Computer Networks Protection and Monitoring» – is an optional component of the professional training of masters in the specialty "F5 - Cybersecurity and Information Protection".

The purpose of teaching the discipline is to form in future specialists the skills and competencies necessary for the development and design of secure computer networks, their administration and maintenance; to provide deep and solid knowledge on the methodology of attacks on computer networks, analysis of computer network security and management of their security.

The subject of the discipline is firewalls and their connection schemes, security protocols and their configuration, construction of secure computer networks, remote access security, development of internetwork policy, vulnerability scanners, monitoring of events and incidents in networks, analysis of threats to information security in networks, examination of network security.

The task of the discipline is to ensure the acquisition of the following competencies and achievement of the following program learning outcomes**:**

Competencies:

- Understand the tasks of protecting network traffic and controlling access using existing protocols and tools.
- Understand the methodology of attacks on computer networks and apply this understanding in practice.
- Apply security policies for a specific object (enterprise) to prevent unauthorized access to computer networks
- Use tools and utilities for administering and maintaining computer networks in accordance with existing security policies.
- Use modern tools, IDS and SIEM systems for auditing, monitoring processes and detecting intrusions in computer networks.

learning outcomes:

- Know the basic concepts of computer networks and their components
- Protect network traffic and implement access control using existing protocols and tools
- Develop and analyze a network architecture that meets increased security requirements
- Develop a security policy based on attack models for a specific object (enterprise)
- Analyze computer networks using tools for auditing and monitoring.

A student who has successfully completed the course must: know the basic concepts of computer networks and their components; protect network traffic and implement access control using existing protocols and tools; develop and analyze a network architecture that meets increased security requirements; develop a security policy based on attack models for a specific object (enterprise); analyze computer networks using tools for auditing and monitoring.

COURSE CREDIT STRUCTURE

Topic title	Number of hours for:		
	lectures	**laboratory works**	**independent work**
Topic 1. Introduction to Computer Networks	2	4	10
Topic 2. Network Administration	6	4	32
Topic 3. Methods and Tools for Protecting Computer Networks	6	4	31
Topic 4. Development and Design of Secure Computer Networks	6	4	32
Topic 5. Methodology of Attacks on Computer Networks	4	4	21
Topic 6. Monitoring Computer Network Security	4	8	21
Topic 7. Managing Computer Network Security	4	6	27
Total:	**32**	**34**	**174**

COURSE PROGRAM

Content of lectures

Lecture number	Lecture topics and abstracts	Number of hours
Topic 1. Introduction to Computer Networks		**2**
1	**Fundamentals of Computer Networks** Concept of Computer Networks. Hardware and Software Components of Computer Networks. Network Topologies. Lit.: [1] c. 8-69; [12] c. 356-371	2
Topic 2. Network Administration		**6**
2	**Concept of network protocols and services. Network models** Tasks and goals of network administration. Models of internetwork interaction (OSI model, TCP/IP model). Lit.: [1] c. 132-181; [12] c. 407-461	2
3	**Basics of TCP/IP Protocol Operation** Addressing Hosts in IP Networks. Subnetting Networks Using a Subnet Mask. Introduction to IP Routing. DNS Service (Namespace, Domains, Zones, Dynamic Server Registration). TCP/IP and DNS Diagnostic Utilities. Lit.: [2] c. 88-108; Lit.: [3] c. 7-56; [7] c. 10-48; [11] c. 14-60	2
4	**Other Network Protocols** SSH Secure Remote Management Protocol. SNMP Network Equipment Interconnection Protocol. Telnet Text Interface Access Network Protocol. FTP File Transfer Protocol. Mail Protocols (POP3, IMAP, SMTP). Hypertext Transfer Protocols HTTP/HTTPS. Internet Control Message Protocol ICMP. Transport Layer Security Protocols TLS/SSL. Lit.: [7] c. 9-56	2
Topic 3. Methods and Tools for Protecting Computer Networks		**6**
5	**Firewalls and their functions in network protection tasks** Advantages of using a firewall in network protection tasks. Types of firewalls Lit.: [2] c. 20-39; [10] c. 180-197	2
6	**Firewalls and Internetwork** Firewall as a means of protection against intrusion from the Internet. Functional requirements and components of firewalls. Filtering routers. Types of gateways. Basic schemes of network protection based on firewalls. Lit.: [2] c. 20-39; [8] c. 434-439	2
7	**Remote Access Security** Identity and Access Management. Organization of Secure Remote Access. Access Management Models (Credential, Discretionary, Role-Based). Access Management Using Single Sign-On with Authorization. Single Sign-On (SSO) Kerberos Protocol Lit.: [10] c. 115-167; [12] c. 272-325; [15] c. 315-371	2
Topic 4. Development and Design of Secure Computer Networks		**6**
8	**Architecture of secure computer networks** Parameters (services, metrics, levels) of network security. Physical protection of networks (cable system, power supply systems, protection against natural disasters). Counteraction to traffic eavesdropping. Network segmentation [1] c. 183-213; [2] c. 10-34, c. 109-117; [7] c. 56-67	2
9	**Network Backup and Recovery** Network equipment and communication channel backup. Information archiving and duplication systems. Recovery of computer networks after cyberattacks, failures and failures of various classes and origins [1] c. 183-213; [2] c. 10-34, c. 109-117; [5] c. 22-134	2

10	**Information security policy of the enterprise network** Structure of the enterprise security policy. Classification of network components from the point of view of information security. Access control matrix and distribution of information flows and roles Lit.: [8] c. 177-240	2
Topic 5. Methodology of Attacks on Computer Networks		**4**
11	**Classification of attacks on computer networks** Access attacks (Sniffing, Hijacking, Session Hijacking). Modification attacks (changing, adding, deleting data). Denial of service attacks. Combined attacks (trusted entity impersonation, Man-in-theMiddle, exploits, password attacks, application-level attacks, network traffic analysis, Phishing, Pharming, botnets, theft of confidential data) Lit.: [4] c. 5-18; [10] c. 206-227; [12] c. 373-381	2
12	**Analysis and modeling of network security threats** Threats, their sources and vulnerabilities. Threats and their classification as an object of modeling. A generalized approach to building threat models in computer networks Lit.: [8] c. 116-177; [12] c. 27-38; [14] c. 46-109	2
Topic 6. Monitoring Computer Network Security		**4**
13	**Network information security problems** Manifestations of network security threats. Hacker and intruder strategies. Overview of the main hacking tools Lit.: [4] c. 154-203	2
14	**Technologies for detecting attacks in computer networks** Classification of attack detection systems IDS (Intrusion Detection System). IDS components and architecture. SIEM systems. Methods of responding to attacks Lit.: [1] c. 71-131; [10] c. 197-206	2
Topic 7. Managing Computer Network Security		**8**
15	**Computer Network Security Audit (Part 1)** Audit Goals and Objectives. Audit Phases Lit.: [4] c. 205-231; [8] c. 348-357; [18] c. 7-103	2
16	**Computer Network Security Audit (Part 2)** Network Compliance. Risk Management. Making Recommendations Lit.: [8] c. 348-357; [18] c. 7-103	2
	Total for the semester:	**32**

Number	Topics of laboratory works	Number of hours
1	Designing a company's computer network	**4**
2	IP addressing and IP routing in computer networks. Administration of computer networks using TCP/IP utilities, TCP/IP services and domain group policy tools	**4**
3	Research on firewalls and firewalls as a means of protecting the network from attacks	**4**
4	Configuring and managing remote access using Windows OS tools	**4**
5	Research on computer network hacking technologies, collecting technical and sensitive information, analyzing network traffic	**4**
6	Research on computer network vulnerabilities, scanning network protocols	**4**
7	Monitoring of incidents and events in computer networks	**4**
8	Managing network information security risks using software tools	**4**
9	Control measures based on the theoretical material passed (testing)	**6**
	Total for the semester:	**34**

Content of independent (individual) work

The volume of independent work is 174 hours. It includes study of lecture material and literary sources, preparation for written control, preparation for defense of laboratory work. The teacher supervises independent work according to the consultation schedule.

Week number	Type of independent work	Number of hours
1	Elaboration of theoretical material. Preparation for laboratory work №1.	10
2	Elaboration of theoretical material. Preparation for defense of laboratory work №1.	11
3	Elaboration of theoretical material. Preparation for laboratory work №2.	10
4	Elaboration of theoretical material. Preparation for defense of laboratory work №2.	11
5	Elaboration of theoretical material. Preparation for laboratory work №3.	10
6	Elaboration of theoretical material. Preparation for defense of laboratory work №3.	11
7	Elaboration of theoretical material. Preparation for laboratory work №4.	10
8	Elaboration of theoretical material. Preparation for defense of laboratory work №4.	11
9	Elaboration of theoretical material. Preparation for laboratory work №5.	10
10	Elaboration of theoretical material. Preparation for defense of laboratory work №5.	11
11	Elaboration of theoretical material. Preparation for laboratory work №6.	10
12	Elaboration of theoretical material. Preparation for defense of laboratory work №6.	11
13	Elaboration of theoretical material. Preparation for laboratory work №7.	10
14	Elaboration of theoretical material. Preparation for defense of laboratory work №7.	11
15	Elaboration of theoretical material. Preparation for laboratory work №8.	10
16	Elaboration of theoretical material. Preparation for defense of laboratory work №8.	11
17	Elaboration of theoretical material. Preparation for written control.	6
	Total for the semester:	**174**

TEACHING METHODS

Lectures are conducted mainly with the use of verbal and visual methods; laboratory works are conducted by practical and search methods; independent work involves the performance of individual tasks using explanation and illustration and research methods.

ASSESSMENT FORMS AND METHODS

Current control is carried out during lectures, laboratory works as well as on testing days indicated in the working plan of the course. Semester control is conducted in the form of the course project defense and examination. The results of the current control are taken into account when making the final assessment.

Each type of work in the course is assessed by a four-point scale. The semester final grade is defined as the weighed average of all types of academic work performed and passed with positive grades taking into account the weighing coefficient. Weights vary depending on the structure of the course and the importance of its individual types of work. A student who scored a positive weighed average score for current work and did not pass the final test (exam) is considered to have failed.

When assessing students' knowledge various means of control are used, in particular: oral quiz before admission to laboratory and practical work is carried out before them; knowledge of theoretical material on the topic is checked by a test control; the quality of performance, mastering theoretical knowledge and practical skills is checked by defending each laboratory and practical work, course project and individual task in accordance with the course program and the curriculum.

When assessing students' knowledge the teacher is guided by the following criteria.

The students receive an "excellent" grade, A according to ECTS scale, for deep and complete mastery of the content of educational material in which they are fluent, knowledge of the nomenclature, for the ability to relate theory to practice, solve practical problems, express and justify their own judgments. Excellent grade means a competent, logical presentation of the answer (both orally and in writing), high-quality design. The student should not hesitate when answering modified questions, should make detailed and generalized conclusions.

The student receives a "good" grade, B according to ECTS scale, for full mastery of the material, knowledge of the nomenclature, fluency in the studied material, conscious use of knowledge to solve practical problems, competent presentation of the answer, but there may be some inaccuracies in the content and form of the answer (errors), unprecise wording of regularities, etc. The student's answer should be based on independent thinking.

The grade "good", C according to ECTS scale, is given to the student for the correct answer with one or two significant errors.

"Satisfactory" grade, D according to ECTS scale, is awarded to students who have shown basic knowledge of the material which is necessary for further study and practical activities in the profession, the students cope with practical tasks required by the program. As a rule, the student's answer is based on the level of reproductive thinking, the student knows little about the structure of the course, makes mistakes in the answer, has mastered and acquired practical skills but has inaccuracies in tasks or replies. The student hesitates when answering a modified question, however, the student can eliminate inaccuracies in the answer with the teacher's help.

"Satisfactory" grade, E according to ECTS scale, is given to the student who demonstrated incomplete mastery of the program material, but has acquired some knowledge and mastered practical skills.

The students receive "unsatisfactory", FX according to ECTS scale, if they have fragmented, unsystematic knowledge, can not distinguish between primary and secondary issues, makes mistakes in defining concepts, distorts their content, chaotically and uncertainly presents the material, can not apply knowledge in solving practical tasks.

As a rule, the grade "unsatisfactory", F according to ECTS scale, is given to a student who cannot continue studies without additional knowledge in the course.

The final semester grade is based on the results of the current control and the final control. Taking into account the analysis of knowledge control the teacher improves the lecture course paying special attention to those sections or topics that had most inaccurate answers which indicates methodological or other shortcomings in the coverage of these topics or sections.

Similarly, adjustments are made to the manuals for laboratory works, fundamental issues are paid more attention when doing laboratory works and in the process of their defense.

Structuring the course by types of work and assessing learning outcomes

Classwork								**Independent, individual work**	**Semester control**
Laboratory works №:								Test control:	Test
1	2	3	4	5	6	7	8	T 1-7	
Кількість балів за вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100***

Correspondence of the national and ECTS grading scales

ECTS grade	**Institutional score scale**	**Assessment criteria**
A	90-100	***Excellent*** **–** deep and complete mastery of educational material and demonstrating relevant skills and abilities.
B	83-89	***Good*** **–** complete knowledge of the material with a few minor errors.
C	73-82	***Good*** **–** correct answer in general with two to three significant errors.
D	66-72	***Satisfactory*** **–** incomplete mastery of the program material but sufficient for practical activities in the professional field.
E	60-65	***Satisfactory*** **–** incomplete mastery of the program material that meets the minimum assessment criteria.
FX	40-59	***Unsatisfactory*** **–** unsystematic knowledge and inability to continue studies without additional knowledge of the course.
F	0-39	***Unsatisfactory*** **–** serious further work is needed and the course is to be retaken.

QUESTIONS FOR STUDENTS' SELF-CONTROL

1. Tasks of computer network protection
2. Physical network protection (cable system, power supply systems, protection against natural disasters)
3. Overview of software and hardware methods of network protection (protection against network viruses, protection against unauthorized access)
4. Administrative measures
5. Using a firewall in network protection tasks
6. Types of firewalls
7. Firewall as a means of protection from the Internet
8. Functional requirements and components of firewalls
9. Filtering routers
10. Types of gateways
11. Basic network protection schemes based on firewalls
12. Identity and access management
13. Organization of secure remote access
14. Access control models (mandatory, discretionary, role-based)
15. Access control using the Single Sign-On (SSO) authorization scheme
16. Kerberos protocol
17. Public Key Infrastructure (PKI)
18. Network protocols and services
19. Tasks and goals of network administration
20. Models of internetwork interaction (OSI model, TCP/IP model)
21. Addressing nodes in IP networks
22. Public and private IP addresses
23. Mapping IP addresses to physical addresses
24. Subnetting networks using a subnet mask
25. Introduction to IP routing
26. TCP/IP and DNS diagnostic utilities
27. Namespace, domains and zones
28. Algorithms of iterative and recursive DNS queries
29. Configuring nodes to perform dynamic registration on a DNS server
30. Architecture of secure computer networks
31. Parameters (services, metrics, levels) of network security
32. Countermeasures traffic listening
33. Network segmentation
34. Network equipment and communication channel redundancy
35. Network archiving and duplication systems
36. Restoring computer networks after cyberattacks, failures and failures of various classes and origins
37. Design and installation of secure computer networks: general requirements and project input data
38. Design and installation of secure computer networks: design documentation for creating a network.
39. Design and installation of secure computer networks: choosing the architecture and structure of the network.
40. Enterprise security policy structure
41. Classification of network components from the point of view of information security
42. Access control matrix and distribution of information flows and roles
43. Problems of information security of networks
44. Manifestations of threats to network security
45. Strategies of hackers and violators
46. Overview of the main hacking tools

47. Classification of attacks on computer networks
48. Threats, their sources and vulnerabilities of wired and wireless networks
50. Generalized approach to building threat models in computer networks
51. The concept of adaptive security management
52. Security analysis technology
53. Tools for analyzing the security of networks, network protocols and services (vulnerability scanners, sniffers, SIEM systems)
54. Technologies for detecting attacks in computer networks
55. Methods for analyzing network information
56. Classification of attack detection systems IDS (Intrusion Detection System)
57. IDS components and architecture
58. Methods of responding to attacks, keeping logs
59. Tasks of network security system management
60. Network security management architecture
61. Functioning of network security management system
62. Computer network security audit
63. Risk management in computer networks

TEACHING AND LEARNING MATERIALS

The educational process of the course is provided with all necessary educational materials and guidelines that are placed at MOODLE Learning Platform.

RECOMMENDED LITERATURE

1. Tekhnolohii zabezpechennia bezpeky merezhevoi infrastruktury/ V. L. Buriachok, A. O. Anosov, V. V. Semko, V. Yu. Sokolov, P. M. Skladannyi. – K.: KUBH, 2019. – 218 s.
2. Orhanizatsiia kompiuternykh merezh: pidruchnyk/ Yu.A. Tarnavskyi, I.M. Kuzmenko. – Kyiv: KPI im. I. Sikorskoho, 2018. – 259 s.
3. Administruvannia kompiuternykh merezh ta operatsiinykh system [Elektronnyi resurs]/ V.V. Polishchuk. – Uzhhorod: 2019. – rezhym dostupu: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/24567/1/Metodychne%20vydannia%20administruvannia%20KM%20i%20OS.pdf
4. Informatsiina bezpeka v kompiuternykh merezhakh: navch. posib./ O.A. Smirnov, O.K. Konoplitska-Slobodeniuk, S.A. Smirnov, K.O. Buravchenko, T.V. Smirnova, L.I. Polishchuk. – Kropyvnytskyi: Vydavets Lysenko V.F., 2020. – 295 s. http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf
5. Proektuvannia ta montazh lokalnykh kompiuternykh merezh/ I. M. Zhuravska. – Mykolaiv: Vydavnytstvo ChDU im. Petra Mohyly, 2016. – 396 s.
6. Kompiuterni merezhi: navch. posib./ B.Iu. Zhurakovskyi, I.O. Zeniv. – Kyiv : KPI im. Ihoria Sikorskoho, 2020. – 213 s. https://ela.kpi.ua/bitstream/123456789/36689/1/Zhurakovkyi_Zeniv_Kompiuterni_merezhi_lab.pdf
7. Tekhnolohii ta protokoly infokomunikatsiinykh merezh. Chastyna 1[Elektronnyi resurs]/ O.L. Nedashkivskyi. – Kyiv, 2017. – rezhym dostupu: http://www.dut.edu.ua/uploads/l_1799_76743031.pdf
8. Modeliuvannia system zakhystu informatsii/ A.O. Antoniuk. - Irpin: Natsionalnyi universytet DPS Ukrainy, 2015. - 273 s.
9. Modelyrovanye systemы zashchytы ynformatsyy. Praktykum: Ucheb. posobye./ E.K. Baranova, A.V. Babash. - M.: RYOR: YNFRA-M, 2015. - 120 s.
10. Kompleksna bezpeka informatsiinykh merezhevykh system. Navchalnyi posibnyk/ A.H. Mykytyshyn, M.M. Mytnyk, P.D. Stukhliak. – Lviv, «Mahnoliia 2006», 2016. – 256 s
11. Kompiuterni merezhi ta Internet. Navchalnyi posibnyk/ V.M. Franchuk. – K.: NPU imeni M.P. Drahomanova, 2015 r. – 141 s.
12. Informatsiina bezpeka: navchalnyi posibnyk/ Yu. Ya. Bobalo, I. V. Horbatyi, M. D. Kiselychnyk, A. P. Bondariev, S. S. Voitusik, A. Ya. Horpeniuk, O. A. Niemkova, I. M. Zhuravel, B. M. Bereziuk, Ye. I. Yakovenko, V. I. Otenko, I. Ya. Tyshyk; za zah. red. d-ra tekhn. nauk, prof. Yu. Ya. Bobala ta d-ra tekhn. nauk, dots. I. V. Horbatoho. – Lviv : Vydavnytstvo Lvivskoi politekhniky, 2019. – 580 s.
13. Informatsiina bezpeka derzhavy: metodychni vkazivky do vykonannia laboratornykh robit/ uklad. O.A. Smirnov, O.K. Konoplitska-Slobodeniuk, V.D. Khokh, S.A. Smirnov/ – Kropyvnytskyi: TsNTU – 2017. – 90 s.
14. Zakhyst informatsii v kompiuternykh systemakh ta merezhakh: navch. posib./ S.H.Semenov, A.O.Podorozhniak, O.I.Balenko, S.Iu.Havrylenko – Kh.: NTU «KhPI», 2014.– 251 s. http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_BKM%20Pos_bnyk.pdf
15. Tekhnolohii zakhystu informatsii: navchalnyi posibnyk/ S. E. Ostapov, S. P. Yevseiev, O. H. Korol. – Kh. : Vyd. KhNEU, 2013. – 476 s. http://kist.ntu.edu.ua/textPhD/tzi.pdf
16. Aparatno-prohramni zasoby zakhystu informatsii u korporatsiiakh: navchalno-metodychnyi posibnyk [Elektronnyi resurs]/ V.H. Kryzhanovskyi, S.P. Serhiienko. – Vinnytsia : DonNU imeni Vasylia Stusa, 2019. – rezhym dostupu: https://r.donnu.edu.ua/bitstream/123456789/111/1/Metodychka%20Zasoby%20zakhystu%20informatsii%20u%20korporatsiiakh.pdf

17. IBM QRadar. Installation Guide [Elektronnyi resurs]. – IBM Corp., 2019. – rezhym dostupu: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_inst.pdf
18. Audyt ta upravlinnia intsydentamy informatsiinoi bezpeky: navchalnyi posibnyk/ O.H. Korchenko, S.O. Hnatiuk S.O, S.V. Kazmirchuk ta in. – K.: Tsentr navch.-nauk. ta nauk.-pr. vydan NA SB Ukrainy, 2014. – 190 s.
19. The Practice of System and Network Administration. Volume 1. Third Edition/ Th. A. Limoncelli, Ch. J. Hogan, S. R. Chalup. – Virtual.NET Inc., Lumeta Corporation, 2017. – 1426 p.
20. Linux Command Line. A Beginners Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.
21. Mastering Windows Server 2019. Second Edition/ J. Krause. – Packt Publishing Ltd, 2019. – 1010 p.
22. Network Security Assessment. Third edition/ Sh. McNab. – OReilly Media, Inc., 2017. – 546 r.
23. Wireless Networks [Elektronnyi resurs]/ J. Salazar. – Czech Technical University of Prague, 2017. – rezhym dostupu: http://standardsoui.ieee.org/oui/oui.txt
24. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.
25. Metody zabezpechennia harantozdatnosti i funktsionalnoi bezpeky bezprovodovoi infrastruktury na osnovi aparatnoho rozdilennia abonentiv: Monohrafiia./ V.L. Buriachok, V.Iu. Sokolov. – Kyiv : KUBH, 2019. - 164 s.
26. Problemy zabezpechennia kontroliu zakhyshchenosti korporatyvnykh merezh ta shliakhy yikh vyrishennia/ Buriachok V. L. ta in. /Naukovi zapysky Ukrainskoho naukovo-doslidnoho instytutu zviazku. - 2016. – №3. – C. 48-61.
27. Uiazvymosty korporatyvnыkh ynformatsyonnыkh system [Elektronnyi resurs]. – Positive Technologies, 2017. – rezhym dostupu: https://www.ptsecurity.com/upload/ corporate/ru-ru/analytics/Corp-Vulnerabilities-2017-rus.pdf
28. Kompiuterni merezhi. Knyha 1/ A.H. Mykytyshyn, M.M. Mytnyk, P.D. Stukhliak, V.V. Pasichnyk. – Lviv, «Mahnoliia 2006», 2013. – 256 s.
29. Kompiuterni merezhi. Knyha 2/ A.H. Mykytyshyn, M.M. Mytnyk, P.D. Stukhliak, V.V. Pasichnyk. – Lviv, «Mahnoliia 2006», 2014. – 312 s.
30. Osnovy informatsiinoi ta kibernetychnoi bezpeky. Navchalnyi posibnyk/ V. L.
31. Bezpeka bezprovodovykh i mobilnykh merezh: Navchalnyi posibnyk/ V. Yu. Sokolov, V. L. Buriachok, M. M. Tadzhdini / red. perekl. O. P. Raiter. – 2 vyd., dop. – K.: KUBH, 2019. – 130 s.

INFORMATION RESOURCES

1. Learning Platform. Web page: https://msn.khmnu.edu.ua.
2. University Electronic Library. Web page: http://lib.khmnu.edu.ua