БЕКІТЕМІН **«Л.Н. Гумилев атындағы Еуразия ұлттық университеті»** **Оқу ісі жөніндегі проректор** **_______________ Оңғарбаев Е.Ә.** **«26» ___02___ 20 21 ж.**	**УТВЕРЖДАЮ** **Проректор по учебной работе «Евразийский национальный университет» им. Л.Н. Гумилева**	**APPROVED BY** **Vice-Rector for Academic Affairs «The L.N. Gumilyov Eurasian National University»**

2021 жылы қабылданатын білім алушыларға арналған «7М06109 - Кәсіпорындардағы компьютерлік жүйелер мен желілерді әкімшілендіру, бақылау және қорғау» білім беру бағдарламасы бойынша пәндер каталогы

Каталог дисциплин по образовательной программе «7М06109 - Администратор по управлению и защите компьютерных систем и сетей на предприятиях» для обучающихся приема 2021 года

The course catalog of the education program «7М06109 - Administration, management and protection of computer systems and networks in the enterprises» for the students of the 2021 year admission

№	Пәннің циклі / Цикл дисциплины /Cycle of the course	Пәннің атауы / Название дисциплины / Name of the course	ECTS	Қысқаша аннотация/ Краткая аннотация / Annotation	Пререквизиттер/ Пререквизиты / Prerequisites
	1 семестр /1 семестр /semester 1				
	ЖОО компоненті / ВУЗовский компонент / University component				
1	КП/ЖООК ПД/ВК PD/ UC	Киберқауіпсіздік негіздері Основы кибербезопасности Basics of cyber security	5	Пән киберқауіпсіздіктің іргелі концепцияларын игеруге арналған. Киберқылмыскерлер сипаттамалары мен олардың тарапынан қолданылатын тактикалар қарастырылады. Сонымен қатар курс киберқауіпсіздік сарапшыларының киберқылмыспен күресу үшін қолданатын технологияларын, құралдары мен процедураларын оқытып, үйретеді. Дисциплина направлена на изучение фундаментальных концепций кибербезопасности. Рассматриваются характеристики киберпреступников и тактики, используемые ими. Кроме того, курс изучает технологии,	

				средства и процедуры, которые специалисты по кибербезопасности используют для борьбы с киберпреступностью. Discipline aims to explore the fundamental concepts of cybersecurity. The characteristics of cybercriminals and tactics used by them are considered. In addition, the course examines the technologies, tools and procedures that cybersecurity experts use to combat cybercrime.	
	Таңдау бойынша компонетттер /Компоненты по выбору / Optional components				
2	БП/ТК БД/КВ BD/EC	Киберқауіпсіздік жүйелерінің сәулеті Архитектура систем кибербезопасности Architecture of cyber security systems	5	Курста киберқауіпсіздік модельдері, қауіп-қатерлер, осалдықтар және деректер ағындарын талдау туралы мәліметтерді қамтитын киберқауіпсіздік жүйелерінің заманауи архитектурасын құру негіздері баяндалған. Сонымен қатар, желілік қауіпсіздік сұрақтары қарастырылады: маршрутизация; шифрлеу;IPv6, SSL / TLS VPN; желілік қауіпсіздік мониторингі; оқшауланған орындау ортасы (құмсалғыш), зиянды бағдарламаларды анықтау технологиясы, қауіпсіз қашықтан кіру В курсе изложены основы построения современной архитектуры систем кибербезопасности, включающие сведения о моделях кибербезопасности, угрозах, уязвимостях и анализе потоков данных. Рассмотрены также вопросы сетевой безопасности: маршрутизация; шифрование; IPv6, SSL / TLS VPN; мониторинг сетевой безопасности; среды изолированного исполнения (песочница), технологии детектирования вредоносных программ, безопасный удаленный доступ The course outlines the basics of building modern architecture of cybersecurity systems, including information about cybersecurity models, threats, vulnerabilities and analysis of data flows. The issues of network security are also considered: routing; encryption; IPv6, SSL / TLS VPN; network security monitoring; isolated execution environment (sandbox), malware detection technology, secure remote access	
	БП/ТК БД/КВ BD/EC	Киберқауіпсіздікті жоспарлау және басқару Планирование и управление кибербезопасностью Cyber Security Planning and Management	5	Пән ақпараттық жүйелердегі киберқауіпсіздік бұзылуының негізгі қауіптерін зерттеуге, киберқауіпсіздікті жоспарлауға және басқаруға мүмкіндік береді. Магистранттар ақпараттық шабуылдардың алдын алу дағдыларын меңгереді, жүйелер программалары мен құрылғыларында декларацияланбаған мүмкіндіктерді, жүйелер жұмысындағы істен шығулар мен қателерді, соның ішінде аппараттық және программалық іркілістер мен операторлардың қателерін, деректер қателерін зерделейді.	

				Дисциплина позволит изучить основные угрозы нарушения киберзащищенности в информационных системах, научиться планировать и управлять кибербезопасностью. Магистранты приобретут навыки предотвращения информационных атак, изучат недекларированные возможности в программах и устройствах систем, отказы и ошибки в работе систем, в том числе аппаратные и программные сбои и ошибки операторов, ошибки данных. Discipline will allow to study the main threats to cyber security in information systems, learn how to plan and manage cyber security. Undergraduates will acquire the skills to prevent information attacks, learn undeclared capabilities in programs and systems devices, failures and errors in the operation of systems, including hardware and software failures and operator errors, data errors.	
3	БП/ТК БД/КВ BD/EC	Ақпараттық қауіпсіздік жүйелерін басқару бойынша стандарттар Стандарты управления информационной безопасностью Standards of Information Security Management	5	Пән ақпараттық қауіпсіздік саласындағы негізгі халықаралық және қазақстандық стандарттарды зерттеуге бағытталған. Магистранттар ISO/IEC 27001-2015 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйесі. Талаптар» ҚР СТ стандарты бойынша АҚБЖ әзірлеу және енгізу бойынша нормативтік талаптарды, АҚБЖ үдерістерін құжаттандыру бойынша стандарттарды ұсынуды, ішкі және сертификаттау аудиттерін жүргізуді, тәуекелдерді талдау және АҚБЖ - ның тиімділігін өлшеуді үйренеді. Дисциплина направлена на изучение основных международных и казахстанских стандартов в области информационной безопасности. Магистранты изучат нормативные требования для разработки и внедрения СУИБ с соответствии со стандартом СТ РК ISO/IEC 27001-2015 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования", рекомендации стандартов по документированию процедур СУИБ, проведению внутренний и сертификационных аудитов, анализу рисков и измерениям эффективности СУИБ. Discipline is aimed at studying the main international and Kazakh standards in the field of information security. Students will study the regulatory requirements for the development and implementation of the ISMS in accordance with the standard ST RK ISO / IEC 27001-2015 "Information	

				technology. Methods and means of ensuring security. Information security management systems. Requirements", recommendations of standards for documenting the ISMS procedures, conducting internal and certification audits, risk analysis and measuring the effectiveness of the ISMS.	
	БП/ТК БД/КВ BD/EC	Бұлттық есептеулерді қорғау Защита облачных вычислений Protection of cloud computing	5	Пән бұлттық есептеулер технологиясы туралы теориялық және тәжірибелік білімдерді және бүгінгі бизнесте бұлттық технологияларды тәжірибеде тиімді іске асыру дағдыларын қалыптастыруға бақытталған. Магистранттар бұлттық технологияны қорғаудың құрал-саймандарын пайдану дағдыларын игереді. Дисциплина ориентирована на формирование теоретических и практических знаний о технологии защиты облачных вычислений, умений и навыков практической реализации защиты облачных технологий в современном бизнесе. Магистранты приобретут навыки применения инструментальных средств защиты облачных вычислений. Discipline is focused on the formation of theoretical and practical knowledge about the technology of protecting cloud computing, skills and practical implementation of the protection of cloud technologies in modern business. Students will learn how to use cloud computing tools.	
2 семестр /2 семестр /semester 2					
ЖОО компоненті / ВУЗовский компонент / University component					
4	КП/ЖОО ПД/ВК PD/ UC	Нақты уақыт жүйелерге арналған программалық қамтаманы құру технологиялары Технологии разработки программного обеспечения для систем реального времени Software engineering for real-time systems	5	Курс нақты уақыт режимінде жұмыс істейтін цифрлы ақпарат пен басқару жүйелерінде есептеу процестерін ұйымдастыру қағидаларын және осы жүйелердегі программалық және аппараттық құралдардың өзара байланысын, өзара әрекеттесу процестерін басқару және синхрондау әдістерін баяндайды. Сондай-ақ нақты уақыт режимінде программалық қамтаманы әзірлеу кезінде пайдаланылатын халықаралық және мемлекеттік стандарттар қарастырылған В курсе изложены принципы организации вычислительных процессов в цифровых информационно-управляющих системах, работающих в реальном масштабе времени и взаимосвязь программных и аппаратных средств в системах этого класса, методы управления памятью и синхронизации взаимодействующих процессов. Рассмотрены также международные и государственные стандарты, используемые при	

				разработке программного обеспечения для систем реального времени In this course the principles of the organization of computing processes into digital information and control systems operating in real time and the relationship between software and hardware in this class of systems, methods of memory management and synchronization of communicating processes. International and state standards used in the development of software for real-time systems are also considered	
Таңдау бойынша компонетттер /Компоненты по выбору / Optional components					
5	БП/ТК БД/КВ BD/EC	Ақпараттық технология жүйелеріндегі тәуекелдерді басқару Управление рисками в системах информационных технологий Risk Management in Information Technology Systems	5	Курста ақпараттық қауіпсіздікті басқару жүйесі саласындағы халықаралық және ұлттық стандарттардың талаптары, тәуекелдерді сапалық және/немесе сандық бағалау әдістемесі, сондай-ақ активтерді, қауіп-қатерлерді және осалдықтарды сәйкестендіруді жүргізу үшін мамандандырылған программалық қамтама мүмкіндіктері оқытылады. В курсе изучаются требования международных и национальных стандартов в области систем управления информационной безопасностью, методики качественной и/или количественной оценки рисков, а также возможности специализированного программного обеспечения для проведения идентификации активов, угроз и уязвимостей. There quirements of international and national standards on the information security management systems, methods of qualitative and / or quantitative risk assessment, as well as the possibility of specialized software for identifying assets, threats and vulnerabilities are considered in the course.	
	БП/ТК БД/КВ BD/EC	Ақпараттық қауіпсіздік жүйелерінің сенімділігі мен тиімділігі Надежность и эффективность систем защиты информации Reliability and efficiency of information security systems	5	Пән ақпаратты қорғау жүйесінің сенімділігі мен тиімділігі теориясында базалық білім алуға бағытталған. Магистранттар Webgoat қауіпсіз веб-қосымшасы арқылы веб-қосымшаға бағытталған арнайы шабуылдарды (XSS, SQL injection, сессия ауыстыру, прототип ауыстыру және т.б.) анықтауды және болдырмауды үйренеді. Дисциплина ориентирована на приобретение базовых знаний в теории надежности и эффективности систем защиты информации. Магистранты научатся определять и предотвращать специфические атаки направленные на веб-приложения (XSS, SQL injection, подмена сессии, подмена прототипа и т.д.) с помощью небезопасного веб-приложения WebGoat. Discipline is focused on the acquisition of basic knowledge in the theory of reliability and efficiency of information protection systems. Undergraduates	

				will learn to identify and prevent specific attacks directed at web applications (XSS, SQL injection, session substitution, prototype substitution, etc.) using an insecure WebGoat web application.	
6	КП/ТК ПД/КВ PD/EC	Ақпараттық қауіпсіздік аудиті Аудит информационной безопасности Information Security Audit	5	Пән ақпараттық қауіпсіздік аудитінің мазмұнына қойылатын негізгі ұғымдарды, талаптарды, процестер мен жүйелерді бақылау және тексеру негіздерін, ақпараттық қауіпсіздікті бағалау әдістерін зерделеуге бағытталған. Магистранттар ақпараттық қауіпсіздік аудиті саласындағы методологияны, стандарттарды және нормативтік талаптарды пайдалану дағдыларын меңгереді. Дисциплина направлена на изучненение основных понятий, требований к содержанию аудита информационной безопасности, основ контроля и проверки процессов и систем, методов оценивания информационной безопасности. Магистранты овладеют навыками использования методологии, стандартов и нормативных требований в области аудита информационной безопасности. Discipline is aimed at studying the basic concepts, requirements for the content of information security audits, the basics of monitoring and verifying processes and systems, methods for evaluating information security. Undergraduates will master the skills to use the methodology, standards and regulatory requirements in the field of information security auditing.	
	КП/ТК ПД/КВ PD/EC	Байланыс және ақпараттық жүйелер қауіпсіздігін бағалау Оценка безопасности коммуникационных и информационных систем Communication and Information Systems Security Assessment	5	Пән коммуникациялық және ақпараттық жүйелердің қауіпсіздік жағдайын бағалау, ақпаратты жинау және талдау, коммуникациялық және ақпараттық жүйелердің қауіпсіздік деңгейін оңтайландыру бойынша есептер дайындау және ұсыныстар әзірлеу дағдыларын меңгеруге бағытталған. Дисциплина ориентирована на приобретение навыков оценки состояния безопасности коммуникационных и информационных систем, сбора и анализа информации, подготовки отчётов и выработки рекомендаций по оптимизации уровня безопасности коммуникационных и информационных систем и защиты данных в от утечки. Discipline is focused on acquiring skills for assessing the security status of communication and information systems, collecting and analyzing information, preparing reports and making recommendations on how to optimize the security level of communication and information systems and protect data from leakage.	

3 семестр /3 семестр /semester 3					
ЖОО компоненті / ВУЗовский компонент / University component					
7	КП/ЖО ОК ПД/ВК PD/ UC	Қауіпсіздік мақсатындағы Java Java для целей безопасности Java for security purposes	5	Пәнді оқу Java программалау тілінің көмегімен әзірленген программалық қамтаманың сенімділігін, бүтіндігін және қол жетімділігін басқаруды үйретуге мүмкіндік береді. Ол Java программалау тілінде қауіпсіз кодтау ережелерінің жиынтығын ұсынатын кодтау стандарттарымен танысады. Бұл Ережелердің мақсаты-инженер-программистерді кодтаудың дұрыс емес әдістерінен қорғау. Оқу материалының негізі ретінде Java-кодтау үшін Java-CERT® Oracle Secure Coding Standard стандарты қолданылады. Изучение дисциплины позволит научить управлять надежностью, целостностью и доступностью программного обеспечения, разработанного с помощью языка программирования Java. Обущающиеся знакомятся стандартами кодирования, которые предоставляют набор правил безопасного кодирования на языке программирования Java. Цель этих правил - защитить инженеров-программистов от неправильных методов кодирования, которые могут привести к уязвимости созданных приложений. В качестве основы для учебного материала используется стандарт Java-CERT® Oracle® Secure Coding Standard для Java-кодирования. Studying the discipline will allow you to learn how to manage the reliability, integrity and availability of software developed using the Java programming language. Familiarize themselves with coding standards that provide a set of safe coding rules in the Java programming language. The purpose of these rules is to protect software engineers from incorrect coding methods that could lead to vulnerabilities of created applications. Java-CERT® Oracle® Secure Coding Standard for Java coding is used as the basis for the training material.	
8	КП/ЖО ОК ПД/ВК PD/ UC	Білімді басқару Управление знаниями Knowledge management	5	Пәнді оқуда компанияның білімі барлық қызметкерлерінің тәжірибесі мен білімдерінің жиынтығы ретінде, сондай-ақ компанияның деректер базасы мен репозитарийлерінде сақталған формальды білімі болып табылады. Бұл ретте білімді басқарудың екі құрамдас жүйесіне баса назар аударылады: ұйымдастырушылық және технологиялық. Негізгі назар білімді басқару теориясы туралы тұтас ұғымға, жаңа ұйымдастырушылық білімді құру процесіне, сондай-ақ білімді басқару бойынша негізгі процестер мен құралдарды іс жүзінде қолдануға бөлінеді.	

				Предметом изучения дисциплины являются знания компании как сумма опыта и знаний всех сотрудников компании, а также формализованные знания, хранящиеся в базах данных и репозитариях компании. При этом акцент делается на две составляющие системы управления знаниями: *организационную* и *технологическую*. Основное внимание уделяется целостному представлению о теории управления знаниями, процессу создания нового организационного знания, а также практическому применению основных процессов и инструментов по управлению знаниями. The subject of the discipline is the knowledge of the company as the sum of experience and knowledge of all employees, as well as formalized knowledge stored in databases and repositories of the company. The focus is on two components of the knowledge management system: organizational and technological. The focus is on a holistic view of knowledge management theory, the process of creating new organizational knowledge, and the practical application of key processes and tools for knowledge management.	
Таңдау бойынша компонетттер /Компоненты по выбору / Optional components					
9	КП/ТК ПД/КВ PD/EC	Компьютерлік криминалистика Компьютерная криминалистика Computer Forensics	6	Пән компьютерлік қылмыстарды және сараптамалық қызметті тексеруде компьютерлік технологиялар мен компьютерлік техниканы қолданудың теориялық білімі мен практикалық дағдыларын меңгеруге бағытталған. Магистранттар жоғары компьютерлік технологиялар мен қазіргі заманғы программалық қамтаманы пайдалана отырып, компьютерлік қылмыстардың дәлелдерін жинау және талдау дағдыларын алады. Дисциплина направлена на овладение теоретическими знаниями и практическими навыками применения компьютерной технологии и компьютерной техники при расследовании компьютерных преступлений и экспертной деятельности. Магистранты приобретут навыки сбора и анализа доказательств компьютерных преступлений с использованием высоких компьютерных технологий и современного программного обеспечения. Discipline is aimed at mastering the theoretical knowledge and practical skills in the use of computer technology and computer technology in the investigation of computer crimes and expert activities. Undergraduates will acquire the skills of collecting and analyzing evidence of computer crimes using high-end	

				computer technologies and modern software.	
	КП/ТК ПД/КВ PD/EC	Тәжірибелік вирусология Практическая вирусология Malware analysis	6	Пән өзекті зиянды программалардың мүмкіндіктерін және киберқауіпсіздіктің қазіргі жағдайын айқындауға мүмкіндік береді; VMWare ПҚ базасында зертханалық стенд құруды үйретеді; кодты талдауға арналған утилиттермен жұмыс істеуге дайындайды. Магистранттар зиянды программалық қамтама әсеріне байланысты инциденттерге (жұқтырудың пайдаланылған арналары, зиянды программалық қамтама мақсаттары, шабуылданған объектілер және нақты келтірілген залалдарды тексеру) тергеу жүргізуді үйренеді. Дисциплина позволяет осветить возможности актуальных вредоносных программ и современное состояние киберугроз; обучить созданию лабораторного стенда на базе ПО VMWare; подготовить к работе с утилитами, предназначенными для анализа кода. Магистранты научатся проводить расследования инцидентов, связанных с воздействием вредоносного ПО (использованные каналы заражения, цели вредоносного ПО, атакованные объекты и реально причиненный ущерб). Discipline allows you to highlight the capabilities of current malware and the current state of cyber threats; teach how to create a lab stand based on VMWare software; Prepare to work with utilities designed for code analysis. Undergraduates will learn how to investigate incidents involving exposure to malware (used infection channels, malware targets, attacked objects, and actual damage).	
10	КП/ТК ПД/КВ PD/EC	Көпагенттік жүйелер Многоагентные системы Extraction systems	6	Пән магистранттардың үлестірілген интеллектуалды жүйелерді программалау саласында теориялық білімдерін қалыптастыруға, көпагентті жүйелерді өңдеу технологиясымен танысуға бағытталған. Магистранттар көпагентті жүйелерді құрудың негізгі концепцияларын, агенттік архитектура түрлері және көпагентті жүйелерді басқару стратегиялары туралы білімді қалыптастыруды оқып, зерттейді. Дисциплина ориентирована на формирование у магистрантов теоретических знаний в области программирования распределенных интеллектуальных систем, знакомство с технологией разработки многоагентных систем. Магистранты изучат основные концепции построения многоагентных систем, формирования знаний о видах агентных архитектур и стратегиях управления многоагентными	

				системами. Discipline is focused on the formation of theoretical students in undergraduate knowledge in the field of programming of distributed intelligent systems, familiarity with the technology of developing multi-agent systems. Undergraduates will learn the basic concepts of building multi-agent systems, the formation of knowledge about the types of agent architectures and strategies for managing multi-agent systems.	
	КП/ТК ПД/КВ PD/EC	Ақпараттық қауіпсіздіктің интеллектуалдық платформасы Интеллектуальные платформы информационной безопасности Intelligent information security platform	6	Пән интеллектуалды платформаларды құру, ақпараттық қауіпсіздікті басқару мәселелерін қарастырады. Магистранттар ақпараттық қауіпсіздіктің жіктелуін, заманауи интеллектуалды платформалардың ерекшеліктерін зерттейді, зияткерлік платформаларды енгізу мен жобалаудың инновациялық тәсілдерін басқару дағдыларын игереді. Дисциплина рассматривает вопросы изучения построения интеллектуальных платформ, управления информационной безопасностью. Магистранты изучат классификацию информационной безопасности, особенности современных интеллектуальных платформ, приобретут навыки управления инновационными подходами к внедрению и проектированию интеллектуальных платформ. Discipline deals with the study of the construction of intelligent platforms, information security management. Undergraduates will study the classification of information security, the features of modern intellectual platforms, will acquire the skills of managing innovative approaches to the implementation and design of intelligent platforms.	
11	КП/ТК ПД/КВ PD/EC	Деректер базасының киберқауіпсіздігін жобалау Проектирование кибербезопасности баз данных Designing database cyber security	6	Пәнді оқу деректер базасының киберқауіпсіздігін жобалау технологиясы туралы түсінік береді. Пәнді оқытудың негізгі міндеті-магистранттарға киберқауіпсіздік құрылымдарын құру технологиясын формалдауда, практикалық дағдыларды меңгерту, деректер базасын қорғаудың негізгі әдістерін игерту. Изучение дисциплины дает представление о технологиях проектирования кибербезопасности баз данных. Основной задачей изучения дисциплины является овладение магистрантами практическими навыками в формализации технологии, построении структур кибербезопасности, освоение основных методов защиты баз данных. Discipline studies provide insights into database cybersecurity design	

				technologies. The main task of studying the discipline is to master the undergraduates practical skills in the formalization of technology, building structures of cybersecurity, mastering the basic methods of protecting databases.	
	КП/ТК ПД/КВ PD/EC	Киберқауіпсіздік және желілерді қорғау Кибербезопасность и защита сетей Cyber Security & Network Protection	6	Пән құралдар мен компьютерлік жүйелерге қол жетімділікті физикалық қорғау, компьютерлік жүйені қорғау негіздерін оқытуға бағытталған. Магистранттар периметрі бойынша шабуылдардың типтерін, қауіпсіздік аймақтары мен құрылғыларын, DMZ күйін, брандмауэрлерді, Nat, VPN маршрутизаторын, веб-қатерлерден қорғауды зерттейді, желіні қорғау (NAP) және сымсыз желілердің қауіпсіздігін қамтамасыз ету дағдыларын алады. Дисциплина ориентирована на изучение основ физической защиты доступа к средствам и компьютерным системам, защиты компьютерной системы. Магистранты изучат типы атак по периметру, зоны безопасности и устройств, настройку DMZ, брандмауэры, маршрутизатор NAT, VPN, защиту от веб-угроз, приобретут навыки защиты сети (NAP) и обеспечения безопасности беспроводных сетей. Discipline is focused on learning the basics of physical protection of access to tools and computer systems, protection of computer systems. Undergraduates will learn the types of attacks along the perimeter, security zones and devices, DMZ configuration, firewalls, NAT router, VPN, protection against web threats, will acquire network protection skills (NAP) and wireless security.	

Ақпараттық қауіпсіздік кафедрасы отырысында қарастырылды және бекітілді
Рассмотрено и утверждено на заседании кафедры информационной безопасности
Considered and approved at the meeting of the Department of Information security
Күні / дата / date 17.02 20 21 хаттама / протокол / Record № 6.3

Д.Ж.Сатыбалдина (Аты-жөні/ФИО/Name) — (подпись/қолы/signature) — 17.02.21 (дата/күні/date)