

СИЛЛАБУС
2025-2026 оқу жылының күзгі семестрі
«7M06302 Ақпараттық қауіпсіздік аудиті» білім беру бағдарламасы

Пәннің ID және атауы	Білім алушының өзіндік жұмысын (БӨЖ)	Кредиттер саны			Кредиттердің жалпы саны	Оқытушының жетекшілігімен білім алушының өзіндік жұмысы (ОБӨЖ)	
		Дәрістер (Д)	Семинар сабақтары (СС)	Зерт. сабақтары (ЗС)			
98849 Ақпараттық қауіпсіздік аудиті 1	4	1.7	-	3.3	5	7	
ПӘН ТУРАЛЫ АКАДЕМИЯЛЫҚ АҚПАРАТ							
Жаттығу форматы	Цикл, құрамдас	Дәріс түрлері	Практикалық сабақтардың түрлері		Пішін және платформа қорытынды бақылау		
Оффлайн	Б, ТК	Ақпараттық, аналитикалық дәріс	Ақпараттық қауіпсіздік аудитінің тапсырмаларын орындау		Ауызша, оффлайн		
Оқытушы - (лар)	Карюкин Владислав Игоревич						
электрондық пошта:	vladislav.karyukin@kaznu.kz						
Телефон:	+77019405992						
Көмекші - (лар)	-						
электрондық пошта:	-						
Телефон:	-						
ПӘННІҢ АКАДЕМИЯЛЫҚ ПРЕЗЕНТАЦИЯСЫ							
Пәннің мақсаты	Оқытудан күтілетін нәтижелер (ОН)*			ОН қол жеткізу индикаторлары (ЖИ)			
Ақпараттық қауіпсіздік аудитін ұйымдастыру және жүргізу негізінде ақпаратты қорғау жүйесінде іс-шаралар кешенін қолдану бойынша тәртіптік құзыреттерді игеру. Оқу нәтижесінде қарастырылады: Ақпараттық қауіпсіздік аудитінің құқықтық және әдіснамалық негіздері, аудит және ақпараттық қауіпсіздік негіздері бойынша Стандарттар мен нұсқаулықтар, ақпараттық қауіпсіздікті бағалау әдістері.	1. Когнитивті. Ақпараттық қауіпсіздік (АҚ) аудитінің теориялық негіздерін және нормативтік талаптарды зерделеу			1.1 Аудиттің халықаралық стандарттары мен әдістемелерін зерттеу (ISO/IEC 27001, NIST)			
				1.2 Ақпараттық қауіпсіздік саласындағы нормативтік құқықтық базаны білу			
	2. Функционалды. Ақпараттық қауіпсіздік аудиті процесін жоспарлай және ұйымдастыра білу			2.1 Аудит жоспарын құру және оның мақсаттарын анықтау			
				2.2 Ақпараттық жүйенің аудитінің объектілері мен көлемін анықтау			
	3. Функционалды. Аудит кезінде дәлелдемелерді жинау және талдау әдістерін меңгеру			3.1 Оқиғалар журналын тексеру және талдау әдістерін қолдану			
				3.2 Осалдықтарды анықтау үшін автоматтандырылған талдау құралдарын пайдаланыңыз			
	4. Жүйелік. Кибершабуылдарды болжау және анықтау үшін терең оқыту әдістерін қолданыңыз			4.1 Тәуекел мен осалдықты талдауды жүргізу			
				4.2 Кибершабуылдардан қорғау деңгейін өлшеу			
	5. Когнитивті. Ақпараттық қауіпсіздік аудитіне машиналық оқыту және деректерді өндіру әдістерін қолданыңыз			5.1 Желілік трафикті талдау және кеңейтілген қауіптерді анықтау үшін машиналық оқыту үлгілерін және нейрондық желілерді қолданыңыз			
				5.2 Шабуылдар мен зиянды әрекеттерді жіктеу үшін терең оқыту үлгілерін әзірлеу және үйрету			
Алғы шарттар	98856 – ОЖ қауіпсіздік талдауы						
Постреквизиттер	98851 – Ақпараттық қауіпсіздік аудиті 2						
Білім беру ресурстары	Әдебиеттер: негізгі , қосымша. Негізгі: 1. Ақпараттық технологияларды бақылау және аудит (5-ші басылым) - Angel R. Otero, 2018. АТ бақылау және АТ аудитіне толық шолу: процестер, тәуекелдер, процедуралар және мысалдар.						

	2. Сәйкестік үшін АТ-инфрақұрылымдарын тексеру (3-ші басылым) – Роберт Джонсон және т.б., 2022. Инфрақұрылымның талаптар мен заңдарға сәйкестігін тексеру тәжірибесі. 3. ISO 27001 Controls – A Guide to Implementing and Auditing (2nd ed., aligned to ISO/IEC 27001:2022) — IT Governance/Bridget Kenyon, 2023. 4. IT Security Audit – A Complete Guide (2019 Edition) — Gerardus Blokdyk, 2019. 5. Information System Audit: How to Control the Digital Disruption — Philippe Peret, 2022. Қосымша: 1. ISO 27001 Controls Handbook: Implementing and Auditing an ISMS (ISO/IEC 27001:2022), 2023. 2. Information Technology Control and Audit (4th ed.) — Senft, Gallegos, Davis, 2016. Зерттеу инфрақұрылымы 1. №12 бизнес-инкубатор 2. Зертханалық кабинет 514 3. Зертханалық кабинет 323 Кәсіби ғылыми мәліметтер базасы 1. Scopus – https://www.scopus.com 2. Elsevier – https://www.elsevier.com/ 3. Researchgate – https://www.researchgate.net/ Интернет ресурстары 1. https://www.coursera.org/learn/information-systems-audit 2. https://www.theiia.org/en/products/learning-solutions/course/fundamentals-of-it-auditing/ 3. https://www.acilearning.com/courses/audit/advanced-it-audit-school/ Бағдарламалық қамтамасыз ету 1. Windows 10, Windows 11 2. Anaconda Navigator 3. Tensorflow 4. Keras 3. Kali Linux
Пәннің академиялық саясаты	Пәннің академиялық саясаты әл-Фараби атындағы ҚазҰУ-дың <u>Академиялық саясатымен және академиялық адалдық Саясатымен</u> айкындалады. Құжаттар Univer ИЖ басты бетінде қолжетімді. Ғылым мен білімнің интеграциясы. Студенттердің, магистранттардың және докторанттардың ғылыми-зерттеу жұмысы – бұл оқу үдерісінің тереңдетілуі. Ол тікелей кафедраларда, зертханаларда, университеттің ғылыми және жобалау бөлімшелерінде, студенттік ғылыми-техникалық бірлестіктерінде ұйымдастырылады. Білім берудің барлық деңгейлеріндегі білім алушылардың өзіндік жұмысы заманауи ғылыми-зерттеу және акпараттық технологияларды қолдана отырып, жаңа білім алу негізінде зерттеу дағдылары мен құзыреттіліктерін дамытуға бағытталған. Зерттеу университетінің оқытушысы ғылыми-зерттеу қызметінің нәтижелерін дәрістер мен семинарлық (практикалық) сабақтар, зертханалық сабақтар тақырыбында, силлабустарда көрініс табатын және оқу сабақтары мен тапсырмалар тақырыптарының өзектілігіне жауап беретін ОБӨЗ, БӨЗ тапсырмаларына біріктіреді. Сабаққа қатысуы. Әр тапсырманың мерзімі пән мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген. Мерзімдерді сақтамау балдардың жоғалуына әкеледі. Академиялық адалдық. Практикалық/зертханалық сабақтар, БӨЖ білім алушының дербестігін, сыни ойлауын, шығармашылығын дамытады. Плагиат, жалғандық, шпаргалка пайдалану, тапсырмаларды орындаудың барлық кезеңдерінде көшіруге жол берілмейді. Теориялық оқыту кезеңінде және емтихандарда академиялық адалдықты сақтау негізгі саясаттардан басқа «<u>Қорытынды бақылауды жүргізу Ережелері</u>», «<u>Ағымдағы оқу жылының күзгі/көктемгі семестрінің қорытынды бақылауын жүргізуге арналған Нұсқаулықтары</u>», «<u>Білім алушылардың тестілік құжаттарының көшіріліп алынуын тексеру туралы Ережесі</u>» тәрізді құжаттармен регламенттеледі. Инклюзивті білім берудің негізгі принциптері. Университеттің білім беру ортасы гендерлік, нәсілдік/этникалық тегіне, діни сенімдеріне, әлеуметтік-экономикалық мәртебесіне, студенттің физикалық денсаулығына және т.б. қарамастан, оқытушы тарапынан барлық білім алушыларға және білім алушылардың бір-біріне әрқашан қолдау мен тең қарым-қатынас болатын қауіпсіз орын ретінде ойластырылған. Барлық адамдар құрдастары мен курстастарының қолдауы мен достығына мұқтаж. Барлық студенттер үшін жетістікке жету, мүмкін емес нәрселерден гөрі не істей алатындығы болып табылады. Әртүрлілік өмірдің барлық жақтарын күшейтеді. Барлық білім алушылар, әсіресе мүмкіндігі шектеулі жандар, телефон/e-mail vladislav.karyukin@kaznu.kz / +77019405992 немесе MS Teams-тегі бейне байланыс арқылы https://teams.microsoft.com/l/team/19%3AxxjqQB04Sn-

ОҚЫТУ, ОҚУ ЖӘНЕ БАҒАЛАУ ТУРАЛЫ АҚПАРАТ

Ұпайлық рейтинг оқу жетістіктерін бағалаудың әріптік жүйесі				Бағалау әдістері	
Баға	Сандық эквивалент ұпай	Ұпайлар, % мазмұны	Дәстүрлі жүйе бойынша бағалау	Критериялды бағалау – айқын әзірленген критерийлер негізінде оқытудың нақты қол жеткізілген нәтижелерін оқытудан күтілетін нәтижелерімен ара салмақтық процесі. Формативті және жиынтық бағалауға негізделген. Формативті бағалау – күнделікті оқу қызметі барысында жүргізілетін бағалау түрі. Ағымдағы көрсеткіш болып табылады. Білім алушы мен оқытушы арасындағы жедел өзара байланысты қамтамасыз етеді. Білім алушының мүмкіндіктерін айқындауға, қиындықтарды анықтауға, ең жақсы нәтижелерге қол жеткізуге көмектесуге, оқытушының білім беру процесін уақтылы түзетуге мүмкіндік береді. Дәрістер, семинарлар, практикалық сабақтар (пікірталастар, викториналар, жарыссөздер, дөңгелек үстелдер, зертханалық жұмыстар және т.б.) кезінде тапсырмалардың орындалуы, аудиториядағы жұмыс белсенділігі бағаланады. Алынған білім мен құзыреттілік бағаланады. Жиынтық бағалау – пән бағдарламасына сәйкес бөлімді зерделеу аяқталғаннан кейін жүргізілетін бағалау түрі. БӨЖ орындаған кезде семестр ішінде 4 рет өткізіледі. Бұл оқытудан күтілетін нәтижелерін игеруді дескрипторлармен арақатынаста бағалау. Белгілі бір кезеңдегі пәнді меңгеру деңгейін анықтауға және тіркеуге мүмкіндік береді. Оқу нәтижелері бағаланады.	
A	4,0	95-100	Өте жақсы		
A-	3.67	90-94			
B+	3.33	85-89	Жақсы		
B	3.0	80-84			
B-	2.67	75-79			
C+	2.33	70-74			
C	2.0	65-69	Қанағаттанарлық	Қалыптастырушы және жиынтық бағалау	Ұпай % мазмұны
C-	1.67	60-64		Дәрістердегі белсенділік	5
D+	1.33	55-59		Практикалық сабақтарда жұмыс істеуі	20
D	1.0	50-54		Өзіндік жұмысы	25
FX	0,5	25-49	Қанағаттанарлықсыз	Жобалық және шығармашылық қызметі	10
Ф	0	0-24		Қорытынды бақылау (емтихан)	40
				БАРЛЫҒЫ	100

Курс мазмұнын жүзеге асыруға арналған күнтізбе (кесте). Оқыту және оқу әдістері.

Аптасы	Тақырып атауы	Сағат саны	Макс. балл
МОДУЛЬ 1 Ақпараттық қауіпсіздік аудитіне кіріспе			
1	1-Д. Тұжырымдама, максаттар, халықаралық стандарттар (ISO/IEC 27001, COBIT, NIST)	1	
	1-3С. Windows/Linux ОЖ оқиғалар журналдарын талдау және күдікті әрекеттерді анықтау	2	
2	2-Д. Журналды талдау, осалдықты тексеру, қауіпсіздік саясатының аудиті	1	
	2-3С. Қол жеткізу саясаттарын орнату және тексеру	2	
3	3-Д. Тәуекелдер мен қауіптерді бағалау әдістемесін зерттеу	1	
	3-3С. Аудит жүйелері үшін осалдық құралдарын пайдалану	2	
4	4-Д. Жіктеу алгоритмдерін зерттеу, ауытқуларды анықтау	1	
	4-3С. Журналдардағы ауытқуларды анықтау үшін қарапайым машиналық оқыту үлгілерін енгізу	2	
5	5-Д. Желі трафигіндегі күрделі қауіптерді анықтау үшін нейрондық желілерді пайдалану	1	2
	5-3С. DDoS анықтау үшін нейрондық желілерді үйрету шабуылдар	2	10
	1-ОБӨЖ. 1-БӨЖ «Қолданыстағы аудит стандарттарын бағалау» орындау бойынша кеңес		20
	1-БӨЖ қабылдау		
МОДУЛЬ 2 Аудитте машиналық оқыту үлгілерін қолдану			
6	6-Д. Трафикті талдау үшін желіаралық қалқандарды конфигурациялау	1	1
	6-3С. Брандмауэр конфигурациясының аудитін енгізу	2	10
	2-ОБӨЖ. «Киберқауіптерді анықтау үшін машиналық оқыту алгоритмдерін енгізу» тақырыбы бойынша 2-БӨЖ енгізу бойынша кеңес		
7	7-Д. XSS классификация әдістерін зерттеу және фишингтік қауіптер	1	1
	7-3С. XSS классификациясы үшін оқыту үлгілері және фишингтік қауіптер	2	10
	3-ОБӨЖ. 2-БӨЖ қабылдау		35
8	8-Д. SQL классификациясының әдістерін зерттеу инъекциялар	1	1
	8-3С. SQL классификациясы үшін оқыту үлгілері инъекциялар	2	10
Аралық бақылау 1			100
9	9-Д. DDoS анықтау әдістері шабуылдар	1	1
	9-3С. DDoS анықтауға арналған оқыту үлгілері шабуылдар	2	10

	4-ОБӨЖ. «Киберқауіптерді анықтау үшін терең оқыту алгоритмдерін енгізу» тақырыбы бойынша 3-БӨЖ енгізу бойынша кеңес		
10	10-Д. Ортадағы адамды анықтау әдістері (MitM) шабуылдары	1	1
	10-ЗС. MitM анықтауға арналған оқыту үлгілері шабуылдар	2	10
МОДУЛЬ 3 Үлкен техникаларды қолдану Деректер аудитте			
11	11-Д. Зиянды бағдарламаларды анықтау әдістері	1	1
	11-ЗС. Зиянды бағдарламаларды анықтауға арналған оқыту үлгілері	2	10
	5-ОБӨЖ. 3-БӨЖ қабылдау		10
12	12-Д. АРТ шабуылдары мен инсайдерлік қауіптерді анықтау әдістері	1	1
	12-ЗС. АРТ анықтау үшін үлгілерді құру	2	10
	6-ОБӨД. «Киберқауіптердің аудиті үшін веб-қосымшаны әзірлеу» тақырыбы бойынша 4-БӨЖ енгізу бойынша кеңес		
13	13-Д. Ақпараттық қауіпсіздік аудитін визуализациялау үшін бизнес-аналитика құралдарын пайдалану	1	1
	13-ЗС. Power жүйесінде ақпараттық қауіпсіздік есептерін құру BI	2	10
14	14-Д. Ақпараттық қауіпсіздік аудитіндегі үлкен деректер әдістері	1	1
	14-ЗС. Үлкен әдістерді қолдану Деректер ақпараттық қауіпсіздік аудитінде	2	10
	7-БӨЖ. 4-БӨЖ қабылдау		13
15	15-Д. Ақпараттық қауіпсіздік аудитінде машиналық және терең оқыту үлгілерін қолдану арқылы веб-қосымшаларды талдау	1	1
	15-ЗС. Ақпараттық қауіпсіздік аудитінде машиналық және терең оқыту әдістерін қолдану арқылы веб-қосымшаны әзірлеу	2	10
			100
Аралық бақылау 2			100
Қорытынды бақылау (емтихан)			100
Пән үшін барлығы			100

ЖҢЙЫНТЫҚ БАҒАЛАУ РУБРИКАТОРЫ
ОҚУ НӘТИЖЕЛЕРІН БАҒАЛАУ КРИТЕРИЯЛАРЫ

БӨЖ 1. Қолданыстағы аудит стандарттарын бағалау (АБ1 100%-ның 20%)

Критерийі	«Өте жақсы» 16 - 20% макс. салмағы	«Жақсы» 11-15% макс. салмағы	«Қанағаттанарлық» 6-10% макс. салмағы	«Қанағаттанарлықсыз» 0-5% макс. салмағы
Негіздерді білу және түсіну аудит стандарттарын бағалау әдістері	Аудит стандарттарын бағалау әдістерін жақсы түсіну	Аудит стандарттарын бағалау әдістерінің көпшілігін білу	Аудит стандарттарын бағалау әдістері туралы шектеулі түсінік	Аудит стандарттарын бағалау әдістерін үстірт түсіну/түсінбеу
Аудит стандарттарын енгізу дағдылары	Аудиторлық стандарттарды енгізудің анық және нақты көрсетілімі	Сонда аудит стандарттарын енгізудегі логикалық қателер	Аудит стандарттарын енгізудегі логикалық қателердің үлкен саны	Аудит стандарттарының енгізілмеуі
Есеп жазу	Хат анықтықты, қысқалықты және дұрыстықты көрсетеді.	Хат анықтықты, қысқалықты және дұрыстықты көрсетеді. Ол әдетте қателерсіз.	Хатта кейбір негізгі қателер бар және анықтықты жақсарту қажет.	Жазба түсініксіз және оны орындау қиын. Мәтінде көптеген қателер бар.

БӨЖ 2. Киберқауіптерді анықтау үшін машиналық оқыту алгоритмдерін енгізу (АБ1 100%-ның 35%)

Критерийі	«Өте жақсы» 25 - 35% макс. салмағы	«Жақсы» 16-24% макс. салмағы	«Қанағаттанарлық» 6-15% макс. салмағы	«Қанағаттанарлықсыз» 0-5% макс. салмағы
Машиналық оқыту алгоритмінің параметрлерімен жұмыс істеу	Машиналық оқыту алгоритмдерін жақсы түсіну	Машиналық оқыту алгоритмдерінің көпшілігін түсіну	Машиналық оқыту алгоритмдерінің қалай жұмыс істейтінін түсіну шектеулі	Машиналық оқыту алгоритмдері қалай жұмыс істейтінін үстірт түсіну/түсінбеу
Машиналық оқыту моделін баптау дағдылары	Машиналық оқыту үлгілерін конфигурациялаудың анық және қысқа тұсаукесері	Машиналық оқыту үлгілерінің конфигурациясында шамалы логикалық қателер бар	Логикалық және синтаксистік конфигурация қателерінің үлкен саны машиналық оқыту үлгілері	Машиналық оқыту үлгілерін теңшеудің болмауы
Есеп жазу	Хат анықтықты, қысқалықты және дұрыстықты көрсетеді.	Хат анықтықты, қысқалықты және дұрыстықты көрсетеді. Ол әдетте қателерсіз.	Хатта кейбір негізгі қателер бар және анықтықты жақсарту қажет.	Жазба түсініксіз және оны орындау қиын. Мәтінде көптеген қателер бар.

БӨЖ 3. Киберқауіптерді анықтау үшін терең оқыту алгоритмдерін енгізу (АБ2 100%-ның 10%)

Критерийі	«Өте жақсы» 8-10% макс. салмағы	«Жақсы» 5-7% макс. салмағы	«Қанағаттанарлық» 3-4% макс. салмағы	«Қанағаттанарлықсыз» 0-2% макс. салмағы
Терең оқыту алгоритмін баптаумен жұмыс	Терең оқыту алгоритмдерін жақсы түсіну	Терең оқыту алгоритмдері қалай жұмыс істейтінін түсіну	Терең оқыту алгоритмдерінің қалай жұмыс істейтіні туралы шектеулі түсінік	Терең оқыту алгоритмдерінің қалай жұмыс істейтінін үстірт түсіну/түсінбеу

