СИЛЛАБУС
2023-2024 оқу жылының күзгі семестрі
«Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы

Пәннің ID және атауы	Білім алушының өзіндік жұмысын (БӨЖ)	Кредиттер саны			Кредит-тердің жалпы саны	Оқытушының жетекшілігімен білім алушының өзіндік жұмысы (ОБӨЖ)
		Дәрістер (Д)	Семинар сабақтар (СС)	Зерт. сабақтар (ЗС)		
89117 Телекоммуникациядағы ақпаратты қорғау	5	15	-	30	5	6

ПӘН ТУРАЛЫ АКАДЕМИЯЛЫҚ АҚПАРАТ				
Оқыту түрі	**Циклы, компоненті**	**Дәріс түрлері**	**Семинар сабақтарының түрлері**	**Қорытынды бақылаудың түрі мен платфомасы**
Оффлайн	П. БП. Міндетті	Проблемалық, аналитикалық	Мәселелерді шешу, кодтарды жазу	Жазбаша
Дәріскер (лер)	Иманбаева Ақмарал Каримовна			
e-mail:	Akmaral.Imanbaeva@kaznu.edu.kz			
Телефоны:	3773346			
Ассистент (тер)	Намазбаев Тимур			
e-mail:	tirnagog123@gmail.com			
Телефоны:				

ПӘННІҢ АКАДЕМИЯЛЫҚ ПРЕЗЕНТАЦИЯСЫ		
Пәннің мақсаты	**Оқытудан күтілетін нәтижелер (ОН)***	**ОН қол жеткізу индикаторлары (ЖИ)**
Телекоммуникациялық жүйелердегі ақпаратты қорғаудың негізгі принциптерін оқып үйрену	1. Атап өту: телекоммуникация жүйелеріне, қауіп түрлері мен олардың көздеріне, телекоммуникациялардағы қызметтер мен қорғау механизмдеріне қойылатын негізгі ақпараттық қауіпсіздік талаптарын.	1.1 Телекоммуникация жүйелеріне, қызметтеріне және қауіпсіздік механизмдеріне қауіп төндіретін қауіптерді жіктеу;
		1.2 желі деңгейінде ақпарат алмасу хаттамаларын білу;
		1.3 Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамалық және нормативтік құқықтық базасын білу.
	2. Қолдану: негізгі кестелік және криптографиялық алгоритмдерді және сымсыз байланыс арналары арқылы ақпаратты криптографиялық кодтау әдістерін.	2.1 Құпия мәтіндік ақпаратты кодтау үшін кестелік әдістерді қолдану;
		2.2 криптографияда қолданылатын сандар теориясының кейбір мәселелерін шеше білу;
		2.3 құпия ақпаратты кодтаудың классикалық криптографиялық әдістерін қолдану: симметриялық және асимметриялық шифрлау.
		3.1 Цифрлық қауіпсіздік сертификаттарын және

	3. Ажырату: сандық қауіпсіздік сертификаттарының түрлерін және көп арналы телекоммуникациялық жүйелерде рұқсатсыз кірудің ықтимал әдістерін.	оларды қолдану мүмкіндіктерін білу;
		3.2 енуді анықтау жүйесінің (IDS) құралдарын тану білу.
	4. Талдау: кодтау және қорғау әдістерінің тиімділігін	4.1 Криптоталдау әдістерін және криптоталдау қажеттілігін білу; криптографиялық хэш функцияларын білу;
		4.2 ақпаратты қорғаудың классикалық және заманауи алгоритмдерінің криптоталдау әдістерін қолдану
	5. Сыни тұрғыдан талдау: ақпараттық қауіпсіздіктің қолданбалы мәселелерін шешуде алынған нәтижелерді.	5.1 Құпия ақпараттың шығуынан қорғау жүйелерін білу, DLP жүйелерін жіктей білу;
		5.2 DMZ, DPI және WAF тани білу; олардың архитектурасы мен жүзеге асырылуын білу.
Пререквизиттер	IKT2104 Ақпараттық және коммуникациялық технологиялар. TCS3218 Сандық байланыс технологиясы	
Постреквизиттер	Өндірістік практика, дипломдық жұмыс	
Оқу ресурстары	Әдебиет: негізгі, қосымша. 1. Защита информации в телекоммуникационных системах: учеб. пособие / Г.П. Амочаева, Г.К. Алпысова, К.С. Рожкова; М-во образования и науки РК, КарГУ им. Е. А. Букетова. - 2-е изд. - Караганда: Medet Group, 2020. - 90 с. 2. Криптографические методы защиты информации: учеб. пособие для вузов / Б.Я. Рябко, А.Н. Фионов; УМО по образованию в обл. телекоммуникаций. - 2-е изд., стер. - М.: Горячая линия-Телеком, 2014. - 229, [1] с. 3. Задачи по криптографии: учеб.-практическое пособие / М.А. Мустафин. - Алматы: PRINT EXPRESS, 2018. - 45, [1] с. 4. Криптографиялық жүйелер = Криптографические системы: оқу құралы / М.Ю. Зарубин, Г.С. Ыбытаева; ҚР Білім және ғылым м-гі. - Алматы: Бастау, 2019. - 303 б. 5. Алгебраическая криптология: монография / В.А. Романьков; М-во науки и высш. образования РФ, ОГУ им. Ф. М. Достоевского. - Омск: Изд-во Ом. гос. ун-та, 2020. - 261, [1] с. 6. Ақпараттық қауіпсіздік және қорғау: техникалық құрылғылар: ЖОО арналған оқулық / А.У. Актаева, Р.С. Ниязова, А.Ә. Шәріпбай. - Алматы: ЭСПИ, 2021. 7. Ақпараттық қауіпсіздік және ақпаратты қорғау : пәні бойынша оқу құралы / С.К. Жұмағулова. - Алматы : ЭСПИ, 2021. **Зерттеушілік инфрақұрылымы** 1. Білім берушілік пен білім алушылық жүретін лабораториялар мен жерлер (орындар) 2. Компьютерлік класстар **Мәліметтердің кәсіби ғылыми базасы** 1. https://clarivate.com/ 2. https://www.owasp.org/index.php/Main_Page - осалдықтардың деректер базасы. **Интернет-ресурстар** 1. http://elibrary.kaznu.kz/ru 2. https://refdb.ru/look/1214614.html 3. http://www.4stud.info/networking/network-security.html 4. https://www.fortinet.com/ru/solutions/enterprise-midsize-business/network-security 5. https://intuit.ru/studies/courses/102/102/lecture/2971 **Программалық қамтамассыздандырылуы** 1. MatLab 2. Python	

Пәннің академиялық саясаты	Пәннің академиялық саясаты әл-Фараби атындағы ҚазҰУ-дың Академиялық саясатымен және академиялық адалдық Саясатымен айқындалады. Құжаттар Univer ИЖ басты бетінде қолжетімді. **Ғылым мен білімнің интеграциясы.** Студенттердің, магистранттардың және докоранттардың 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 ақпараттық 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 баллдардың 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 «Қорытынды бақылауды жүргізу Ережелері», «Ағымдағы оқу жылының күзгі/көктемгі семестрінің қорытынды бақылауын жүргізуге арналған Нұсқаулықтары», «Білім алушылардың тестілік құжаттарының көшіріліп алынуын тексеру туралы Ережесі» 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, e-mail Akmaral.Imanbaeva@kaznu.edu.kz. **MOOC интеграциясы (massive openlline course). MOOC**-тың пәнге интеграциялануы жағдайында барлық білім алушылар **MOOC**-қа тіркелуі қажет. **MOOC** модульдерінің өту мерзімі пәнді оқу кестесіне сәйкес қатаң сақталуы керек. **Назар салыңыз!** Әр тапсырманың мерзімі пәннің мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген, сондай-ақ **MOOC**-та көрсетілген. Мерзімдерді сақтамау баллдардың жоғалуына әкеледі.

БІЛІМ БЕРУ, БІЛІМ АЛУ ЖӘНЕ БАҒАЛАНУ ТУРАЛЫ АҚПАРАТ

Оқу жетістіктерін есептеудің баллдық-рейтингтік әріптік бағалау жүйесі

Баға	Баллдардың сандық баламасы	% мәндегі баллдар	Дәстүрлі жүйедегі баға
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
C-	1,67	60-64	
D+	1,33	55-59	Қанағаттанарлықсыз
D	1,0	50-54	

Бағалау әдістері

Критериалды 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 3-4 рет өткізіледі. Бұл оқытудан күтілетін нәтижелерін игеруді дескрипторлармен арақатынаста бағалау. Белгілі бір кезеңдегі пәнді меңгеру деңгейін анықтауға және тіркеуге мүмкіндік береді. Оқу нәтижелері бағаланады.

Формативті және жиынтық бағалау	**% мәндегі баллдар**
Практикалық сабақтарда жұмыс істеуі	30
Өзіндік жұмысы	25
Жобалық және шығармашылық қызметі	5
Қорытынды бақылау (емтихан)	40
ЖИЫНТЫҒЫ	100

Оқу курсының мазмұнын іске асыру күнтізбесі (кестесі). Оқытудың және білім берудің әдістері.			
Аптасы	**Тақырып атауы**	**Сағат саны**	**Макс. балл**
МОДУЛЬ 1 Ақпараттық қауіпсіздіктің негізгі принциптері			
1	**Д 1.** Кіріспе. Пәннің мақсаты мен міндеттері. Ақпараттық қауіпсіздік туралы жалпы түсінік, оның дамуының қысқаша тарихы.	1	
	ЗС 1. Шифрлау кестелері. Қарапайым ауыстыру.	2	2
2	**Д 2.** Қауіпсіздік қауіптерінің жалпы сипаттамасы	1	
	ЗС 2. Шифрлау кестелері. Ауыстыру шифрлары. Қос алмастыру шифры.	2	3
	ОБӨЖ 1. БӨЗ 1 орындау бойынша кеңестер The Open Systems Interconnection model (OSI model).	1	
3	**Д 3.** Ашық жүйелер идеологиясы шеңберіндегі қауіпсіздік қызметі	1	
	ЗС 3. Қарапайым алмастыру шифрлары. Цезарь шифрлау жүйесі	2	10
	БӨЗ 1. The Open Systems Interconnection model (OSI model). Ауызша сауалнама..	2	25
4	**Д 4.** Желілердегі мәліметтерді қорғау механизмдері	1	
	ЗС 4. Уитстон Қос квадраты. Playfair биграмма шифры	2	10
5	**Д 5.** Криптографияның негізгі міндеттері мен түсініктері. Ақпаратты криптографиялық қорғаудың принциптері.	1	
	ЗС 5. Vigenère шифрімен шифрлау және шифрды шешу	2	
МОДУЛЬ 2 Сандар теориясының элементтері			
6	**Д 6.** Сандар теориясының элементтері. Негізгі ұғымдар. Криптографияда қажет бес негізгі элемент. Эйлер теоремасы. Ферма теоремасы	1	
	ЗС 6. Күрделі алмастыру шифрлары	2	10
	БӨЗ 2 орындау бойынша кеңестер. 1-2 модуль материалдары бойынша тестілеуге дайындық.	1	
7	**Д 7.** Сандар теориясының элементтері. Салыстыру	1	
	ЗС 7. Эйлер функциясын есептеу. Евклид алгоритмімен GCD табу	2	15
	БӨЗ 2. 1-2 модуль материалдары бойынша тест (6 сұрақ және 1 тапсырма).	1	25
Аралық бақылау 1			**100**
МОДУЛЬ 3 Криптография әдістері			
8	**Д 8.** Симметриялық шифрлау. Кілтті тасымалдаусыз криптожүйе. Диффи-Хеллман кілттері алмасуы)	1	
	ЗС 8. Кілтті тасымалдаусыз криптожүйенің алгоритмі	2	10
	ОБӨЖ 3. БӨЗ 3 Ақпараттық қауіпсіздік саласындағы Қазақстан Республикасының заңдары.	1	
9	**Д 9.** Асимметриялық шифрлау. Ашық кілттердің криптожүйесі. RSA әдісі	1	
	ЗС 9. RSA ашық кілт криптожүйесінің алгоритмі	2	10
	БӨЗ 3 Қазақстан Республикасының: «Ұлттық қауіпсіздік туралы», «Ақпараттандыру туралы», «Мемлекеттік құпиялар туралы», «Дербес деректер және оларды қорғау туралы», «Электрондық құжат және электрондық цифрлық қолтаңба туралы», «Байланыс туралы» заңдарын талдау. Рефератты талдау.	2	5
10	**Д 10.** ЭЦҚ әдістері. ЭльГамаль әдісі.	1	
	ЗС 10. RSA цифрлық қолтаңба алгоритмі. ElGamal цифрлық қолтаңба алгоритмі.	2	10
	ОБӨЖ 4. БӨЗ 4 орындау бойынша кеңестер. 3-модуль бойынша сұрақтарға дайындық	1	
11	**Д 11.** Криптографиялық хэш функциялары. Хэширлеу процесінің негізгі қадамдары.	1	
	ЗС 11. Хэш-функцияларды практикалық қолдану	2	
	БӨЗ 4 Модуль 3 алгоритмдерін қолданып есептер шығару.	1	25
МОДУЛЬ 4 Телекоммуникациялық жүйелердегі қауіпсіздік			
12	**Д 12.** Жүйеге енуді анықтау және алдын алу. Енгізуді анықтау механизмдерінің үш моделі: аномалияға негізделген анықтау, қолтаңбаға негізделген анықтау және гибридті анықтау.	1	
	ЗС 12. Портқа негізделген VLAN желілері.	2	5
	БӨЗ 5. Қауіпсіздік сертификаттары. Қауіпсіздік сертификаттарының түрлері.	1	5
13	**Д 13.** DLP (Data Loss Prevention) жүйелеріне кіріспе. Олардың классификациясы	1	
	ЗС 13. Деректерді шифрлау стандарты (DES) алгоритмі	2	5
	ОБӨЖ 5. БӨЗ 6 орындау бойынша кеңестер. HIPSs	1	
14	**Д 14.** DMZ (демилитаризацияланған аймақ), DPI (Deep Packet Inspection) қолданатын желілер	1	

	ЗС 14. Сандық сүзгілерді енгізу әдістері		
	БӨЗ 6. Хостқа негізделген интрузияның алдын алу жүйелері (HIPS). Практикалық қолдануды талдау және зерттеу.	1	15
15	**Д 15.** Криптоталдау. Криптоанализ туралы түсінік. Криптоталдау әдістері.	1	
	ЗС 15. Криптографиялық алгоритмдерді криптографиялық талдау	2	5
Аралық бақылау 2			**100**
Қорытынды бақылау (емтихан)			**100**
Пән үшін жиынтығы			**100**

Декан _____Н.Ә. Бейсен

Кафедра меңгерушісі _____ М.Қ. Ибраимов

Дәріскер _____ А.К. Иманбаева