Әл-Фараби атындағы Қазақ Ұлттық Университеті
Ақпараттық технологиялар факультеті
«5В070200 – Автоматтандыру және басқару»
мамандығы бойынша

Силлабус
(6В229) Мұнайгаз секторы басқару жүйелерінің қауіпсіздігі-I
Автоматика құралдары
Күзгі семестр 2019-2020 оқу жылы

Пән коды	Пәннің аты	Тип	Кредиттер саны			Кредиттер саны	ECTS
			Дәріс	Практ/ семин	Зертханалық		
6В229	*Мұнайгаз секторы басқару жүйелерінің қауіпсіздігі-I*	ОК	2	0	1	3	5

Дәріскер	Ахметова Ардак Мергенбаевна ҚазНУ аға оқытушысы.	Офис-сағаты	Кесте бойынша
e-mail	ardak_66@mail.ru		
Телефоны	87476848125	Аудитория	420

Академиялық курс презентациясы	• **Курстың мақсаты:** компьютерлік жүйелердегі ақпараттарды қорғау әдістерін, объектісін; компьютерлік жүйелер мен желілерді қорғау мәселелерін зерттеу болып табылады. Қорғалған компьютерлік жүйелерді және желілерді құруда криптографиялық әдістердің ақпараттарды қорғаудағы рөлі ерекше. Криптографиялық әдістер екі жақты келісім шарттар жасасуда, ақпараттар алмасуда, транспорттық бағыныңқы компьютерлік жүйелерде оларға енушілерді анықтауда, компьютерлік объектілердің бүтіндігін тағайындауда қазіргі кезде негізгі әдістер ретінде қарастырылады. Курсты оқып үйрену зертханалық сабақтармен толықтырылған.
Пререквизиттер және постреквизиттер	Пәнді меңгеру үшін студент мектеп курсының «математика», «информатика» пәндерінің базалық ұғымдарын меңгерген болуы керек
Әдебиеттер және ресурстар	**Әдебиеттер**: 1. Дуйсебекова К.С. Ақпараттарды қорғау және ақпараттық қауіпсіздік. Алматы, Қазақ университеті 2013, 324б. 2. Байсалов Е.Р. Криптограияның математикалық негіздері. Алматы, Қазақ университеті 2013, 43б. 3. Шнайер Б. Прикладная криптография. Издательство Триумф. Москва. 2002 //http://www.ssl.stu.neva.ru/psw/crypto.html] Қосымша ОӘҚ univer.kaznu.kz жүйесінде жүктелген.
Университеттің моральдық-этикалық құндылықтары	**Академиялық ереженің тәртібі:** Студенттер сабақтарға міндетті түрде кешікпей қатысуы керек, сабаққа себепсіз қатыспауға болмайды. Сабаққа себепсіз қатыспаса, кешігіп келсе 0 бал қойылады.

на сай курстың академиялық саясаты	Тапсырмаларды (СӨЖ бойынша, аралық бақылау, зертханалық, практикалық/семинарлық, жоба жұмыстарын және т.б), қорытынды емтиханды уақытында орындауға және тапсыруға міндетті. Тапсырмаларды орындап, тапсыру барысында студент тапсыру мерзімін бұзған жағдайда жоспарланған максималды балдан айыппұл (50%) шегеріліп, бағаланады. **Академиялық құндылықтар:** Академиялық құндылық және адалдық: барлық тапсырмаларды өз бетінше орындау; плагиатқа, жалғандыққа, шпаргалканы пайдалануға жол бермеу, білімді бақылаудың барлық кезеңінде көшіруге, оқытушыны алдау және оған деген қарым-қатынасының нашарлығын болдырмау (ҚазҰУ студенттерінің ар-намыс кодексі). Мүмкіндігі шектеулі студенттер арнайы grfarida77@gmail.com бойынша көмек ала алады.
Бағалау саясаты және аттестаттау	Бағалау кезінде студенттердің сабақтағы белсенділігі мен сабаққа қатысуы ескеріледі. Толерантты болыңыз, яғни өзгенің пікірін сыйлаңыз. Қарсылығыңызды әдепті күйде білдіріңіз. Плагиат және басқа да әділсіздіктерге тыйым салынады. СӨЖ, аралық бақылау және қорытынды емтихан тапсыру кезінде көшіру мен сыбырлауға, өзге біреу шығарған есептерді көшіруге, басқа студент үшін емтихан тапсыруға тыйым салынады. Курстың кез келген мәліметін бұрмалау, Интранетке рұқсатсыз кіру және шпаргалка қолдану үшін студент «F» қорытынды бағасын алады.

Білімді бағалау шкаласы

Әріптік жүйе бойынша бағалау	Балдардың сандық эквиваленті	Балдар (%-дық қатынаста)	Дәстүрлі жүйе бойынша бағалау
A	4,0	95-100	Өте жақсы
A-	3,67	90-94	
B+	3,33	85-89	Жақсы Қанағаттанарлық
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	
C-	1,67	60-64	
D+	1,33	55-59	
D-	1,0	50-54	
FX	0,5	25-49	Қанағаттанарлықсыз
F	0	0-24	

Пәннің құрылымы			
Апта	**Тақырыптың атауы**	**Сағат саны**	**Максималды балл**
1	**Дәріс.** Кіріспе. Ақпараттық жүйелердегі ақпаратты қорғаудың жалпы мәселесі. Ақпаратты қорғаудың криптографиялық құралдары.	2	10
	Зертханалық сабақ. ДЭЕМ ақпараттарды қорғау әдістері. Шифрлеу.	1	
2	**Дәріс.** Ақпаратты қорғау. Симметриялық криптожүйелер. Алмастыру шифрлары.	2	20
	Зертханалық сабақ. Алмастыру шифры. Сиқырлы шаршылар. Аналитикалық өзгертулердің көмегімен шифрлеу.	1	
	СОӨЖ. Ақпараттық қауіпсіздік тапсырмалары. Қорғау әдістері. Ақпараттық қауіпсіздік сатылары.	1	
3	**Дәріс.** Ақпараттық қауіпсіздендіру. Ауыстырымдылық жүйесі. Шифрлеудің бір ретті жүйесі. Идеал шифр түсінігі.	2	10
	Зертханалық сабақ. Цезарь шифрлеу жүйесі. Вижинер кестесі бойынша деректерді шифрлеу.	1	
4	**Дәріс.** Криптографиялық әдістердің жүзеге асуы Электронды қол қою. Гаммирлеу әдісі.	2	20
	Зертханалық сабақ. Полибий шаршысы. Трисемус кестесі.	1	
	СОӨЖ. Компьютерлік жүйелердегі ақпараттарды қорғаудың мақсаты, объектісі және субъектісі.		
5	**Дәріс.** Шабуыл. Криптографиялық протоколдар. Жалған кездейсоқ сандар генераторы.	2	10
	Зертханалық сабақ. Плейфер криптожүйесі. Хилл шифры.	1	
6	**Дәріс.** Ашық кілтті криптожүйе. RSA криптожүйесінде шифрлеу. Гибрид криптожүйелер. Диффи-Хеллман алгоритмі.	2	20
	Зертханалық сабақ. RSA криптожүйесінің бағдарламасын құру.	1	
	СОӨЖ. Ақпараттарды кездейсоқ әсерлерден қорғау. Ақпараттарды заң жүзінде қорғау мәселелері. ДЭЕМ – ақпараттарды қорғау объектісі ретінде.	1	
7	**Дәріс.** Эль-Гамаль шифрлеу жүйесі (Elgamal). DES (Data Encryption Standard).	2	10
	Зертханалық сабақ. Эль-Гамаль шифрлеу жүйесінің бағдарламасын құру.	1	
	Аралық бақылау 1		100
	Midterm Exam		100
8	**Дәріс.** Бір бағытты хэш функциялар. Идентификация, аутентификация, авторизация. Ашық криптожүйеде кілт басқару. Сертификация.	2	15
	Зертханалық сабақ. Диффи-Хеллманның кілттерді алмастыру алгоритмі.	1	

	СОӨЖ. Ашық есептеу желілеріндегі қорғау жүйелерінің архитектурасы. Есептеу желілерін қорғау түсінігі.	1	
9	**Дәріс.** Қорғау объектілерін жіктеу. Иілгіш магниттік дискілеріндегі, «винчестер» типті сырткы есте сақтау құрылғысындағы, дисплейдегі, баспа құрылғысындағы, байланыс арналарындағы қорғау элементтерін жіктеу.	2	10
	Зертханалық сабақ. Хэш-функция және қатынас аутентификациясы.	1	
10	**Дәріс**. Қорғау процестерін тиімді басқару. Вирустардан қорғау.	2	15
	Зертханалық сабақ. Компьютерлік графология.	1	
	СОӨЖ. Идентификациялау және аутентификациялау механизмдері. Электрондық төлем жүйелеріндегі ақпаратты қорғау мәселелері.	1	
11	**Дәріс**. Қорғау жүйелеріне баға беру. Программалық жабдықтаманы рұқсатсыз қатынаудан қорғау.	2	10
	Зертханалық сабақ. Рұқсатсыз қатындаудан қорғауды ұйымдастыру	1	
12	**Дәріс**. Ақпараттық қорғау өлшемі. Ақпараттық ресурстарды қорғаудың керекті өлшемін анықтау. Ақпаратты қорғау өлшеміне баға беру әдістері. Ақпаратты қорғау деңгейіне баға берудің негізгі көрсеткіштері. Қорғау өлшемдерінің сипаттамалары.	2	15
	Зертханалық сабақ. Қорғалған ақпараттарды өлшеу сипаттамасы.	1	
	СОӨЖ. Компьютерлік графология. Ашық кілтті пайдаланушы хаттамалар.	1	
13	**Дәріс** 13. Компьютерлік жүйелердің қауіпсіздігі. Операциялық жүйелердегі ақпаратты қорғау. Компьютерлер мен желілердегі ақпаратты қорғаудың ұйымдық және техникалық құралдары.	2	10
	Зертханалық сабақ. Дербес идентификациялаушы нөмір. Банкоматтардағы қауіпсіздікті қамтамасыз ету шараларын орындау.	1	
14	**Дәріс**. Цифрлік қолтаңба қою. Цифрлік қол қою үшін негізгі талап, түзу және арбитраждық цифрлік қолтаңба қою, ГОСТ 3410 және DSS цифрлік қолтаңба қою стандарты.	2	15
	Зертханалық сабақ. Хабарламаларды қорғау әдістері. Олардың сипаттамалары және программалау мысалдары. Хабарламаларды тасымалдаудың хаттамаларын қорғау.	1	
	СОӨЖ. Желілердегі қауіп көздері. Желілік жүйелерге шабуылдар түрлері.	1	
15	**Дәріс** 15. Сандық сертификаттар. Сандық сертификаттарды басқару.	2	10
	Зертханалық сабақ. Қорғау механизмдерінің сенімділігін анықтау және бағалау.	1	
	Аралық бақылау 2		100

	Емтихан		100
	Барлығы (АБ1+АБ2+АБ3)*0,2+КЕ*0,4		100

Әдістемелік бюро төрағасы Гусманова Ф.Р.

Кафедра меңгерушісі Мансурова М.Е.

Дәріскер Ахметова А.М.