

Қазақстан Республикасы Білім және ғылым министрлігі

Қарағанды мемлекеттік техникалық университеті

БЕКІТЕМІН

**Ғылыми кеңес төрағасы,
ҚарМТУ ректоры
Ғазалиев А.М.**

«___» _____ 2015 ж.

**СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША
ОҚЫТУ БАҒДАРЛАМАСЫ
(SYLLABUS)**

КАКАК 3216 – «Компьютерлік ақпаратты қорғау әдістері мен
құралдары» пәні

КАК 23 – Кодтау және ақпаратты қорғау модулі

5B070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету»
мамандығы

Ақпараттық технологиялар факультеті

«Ақпараттық есептеу жүйелері» кафедрасы

АЛҒЫ СӨЗ

Студентке арналған пән бойынша оқыту бағдарламасын (syllabus) әзірлеген:
АЕЖ кафедрасының аға оқытушы Тайлақ Б.Е.

«Ақпараттық есептеу жүйелері» кафедрасының отырысында талқыланған

«__» _____ 2015 ж.

№ ____ хаттама

Кафедра меңгерушісі _____ Амиров А.Ж. «__» _____ 2015 ж.

Ақпараттық технологиялар факультетінің оқу-әдістемелік кеңесі
мақұлдаған

«__» _____ 2015 ж.

№ ____ хаттама

Төраға _____ Капжаппарова Д.У. «__» _____ 2015 ж.

Оқытушы туралы мәлімет және қатынас ақпараты

Тайлақ Бибігүл Елжасқызы - аға оқытушы.

«Ақпараттық есептеу жүйелері» кафедрасы ҚарМТУ-дың бас корпусында орналасқан (Бейбітшілік бульвары, 56), 300 ауд., байланыс телефоны – 56-59-35 қосымша 2054.

Пәннің еңбек көлемділігі

Оқу түрі	Семестр	Кредиттер саны	ECTS	Сабақ түрі					СӨЖ сағаттарының саны	Жалпы сағат саны	Бақылау түрі
				Қатынас сабақтарының саны			СӨЖ сағаттарының саны	Барлық сағат саны			
				дәріс	практикалық сабақтар	зертханалық сабақтар					
Күндізгі	6	3	5	15	-	30	45	90	45	135	емтихан
Күндізгі, қысқартылған	4	3	5	15	-	30	45	90	45	135	емтихан

Пән сипаттамасы

«Компьютерлік ақпаратты қорғау әдістері мен құралдары» пәні таңдау бойынша базалық пәндерінің циклына жатады.

Пәннің мақсаты

«Компьютерлік ақпаратты қорғау әдістері мен құралдары» пәні ақпаратты қорғаудың теориялық негіздері мен әдістерін оқып үйрену, ақпараттық қауіпсіздік саясатын, құпия жүйелерді оқып үйрену мақсатын ұстанады.

Пән міндеттері

Осы пәнді оқыту нәтижесінде студенттер:

түсінік алуы керек:

- жүйелердің үлгілерінің құрастыруы қағидалары және математикалық - пішіндеу схемалары;

- иерархияны және математикалық үлгілердің құрастыруын негізгі белгілерді;

- вариациялық қағида негізделген математикалық үлгілер;

білуы керек:

- тілдік жүйелердің анықтамасын және негізгі ақпараттық сипаттамасын;

- құпия жүйелерінің математикалық берілуі;

- мәтіндерді талдау әдісін және олардың артықшылығын анықтау;

істей алуы керек:

- ақпараттың математикалық берілуін, ақпараттық сипаттамаларды талдау әдістерін және тілдік жүйенің артықтығын білу;

- түзету жасаудың теориялық негіздерін және еркін мәтіндердің ақпараттық сипаттамаларын қалпына келтіруді білу;

- ақпаратты қорғаудың жүйесін құруды қарастыру, онымен қатар ақпаратты қорғаудың негізгі әдістерімен жабдықтарын меңгеру.

практикалық машықтануы керек:

- мәтіндердің ақпараттық-статистикалық сипаттамаларын трансформациялау жүйелерін құру әдістері;

- рұқсатсыз қатынас құрудан ақпаратты қорғау жүйелерін құрудың практикалық тәсілдері.

Пререквизиттер

Бұл пәнді оқу үшін келесі пәндерді игеру қажет:

Пән	Бөлімдердің (тақырыптардың) атауы
1. Есептеу жүйелерін және желілерін ұйымдастыру	Есептеу жүйелерін ұйымдастыру негіздері. Есептеу желілерін ұйымдастыру негіздері. Деректерді тасымалдаудың әдістері мен құралдары. Жобалануы және желілерді әкімшіліктендіру.
2. Операциялық орталар, жүйелер және қабықшалар	Үрдістерді басқару және ұйымдастыру. Енгізу-шығаруды басқару. Жадыны басқару. Телекоммуникациялық қатына құруды басқару.

Постреквизиттер

«Компьютерлік ақпаратты қорғау әдістері мен құралдары» пәнін оқу кезінде алынған білім «Компьютерлік жүйелерді жобалау», «Телекоммуникациялық технологиялар және желілер» пәндерін игеру кезінде қолданылады.

Пәннің тақырыптық жоспары

Тарау атауы, (тақырыптар)	Сабак түрлері бойынша еңбек көлемділігі, сағ.			
	дәріс	зертханалық	СОӨЖ	СӨЖ
Кіріспе. Ұлттық қауіпсіздендірудің негізгі түсініктері; қауіпсіздендірудің түрлері: мемлекеттік, экономикалық, қоғамдық, әскери, ақпараттық, экологиялық; ақпараттық қауіпсіздендірудің жүйелік қамтамасының ҚР ұлттық қауіпсіздендірудің жүйесіндегі ролі мен орны.	0,5		-	-
1. Ақпаратты қорғау. Ақпараттық қауіптер. Ақпараттық қауіптерге қарсы әрекет. Ақпаратты қорғау жүйелердің сипаттамалық қасиеттері. Қорғау пәні. Қорғау құралдары.	1,5		-	-
2. Ақпараттық қауіпсіздендіру. Ақпараттық қауіпсіздендіруді қамтамасыз ету жүйелердің сипаттамалық қасиеттері, ақпаратты қауіпсіздендіруді қамтамасыз ету құралдары, ақпаратты қауіпсіздендіруді қамтамасыз ету әдістері.	1		-	2

<p>3. Ақпараттық жүйелердің аппараттық және программалық платформасын анализдеу. Мәліметтерді өңдеу электрондық жүйелердің құрылысы; программалы қамтамасыздандырудың құрылысы; мәліметтерді өңдеудің жүйелік құралдары; мәліметтерді өңдеудің қолданбалы құралдары; ақпараттық қорғаудың аппараттық құралдары; ақпараттық қорғаудың программалық құралдары.</p>	1		-	2
<p>4. Ақпараттық жүйелердің қауіпсіздік модельдері. Формальды модельдер; қауіпсіздіктің модельдері; қауіпсіздіктің саясаты; есептеу техникасының құралдары мен автоматтандырылған ақпараттық жүйелердің қорғалуының критерийлері мен кластары; қорғалған жүйелерді бағалау бойынша стандарттар.</p>	1		10	2
<p>5. Қорғау және қауіпсіздендіру жүйелерін практикалық іске асыру мысалдары. Құпия сөз жүйелерінің құрылуы; криптографиялық әдістерді қолданудың ерекшеліктері; криптографиялық ішкі жүйелерді іске асырудың әдістері; симметриялық және бисимметриялық кілттері бар жүйелерді іске асырудың ерекшеліктері; стенографиялық жүйелерді іске асыру түрлері.</p>	1		15	4
<p>6. Қорғалған ақпараттық жүйенің негізгі сипаттамалары. Қорғалған ядроның концепциясы; тексеру әдістері; қорғалған домендер; иерархиялық әдісті қорғалған операциялық жүйені құрғанда қолдану.</p>	1		5	2
<p>7. Ақпаратты қорғау дұрыстығының әдістемесі. Қорғау жүйелерінің дұрыстығын зерттеу; қорғауды зерттеу мен жобалаудың әдістемесі; бүтіндікті тексеру саясатының моделі.</p>	1		-	2
<p>8. Ақпараттық қорғау өлшемі. Ақпараттық ресурстарды қорғаудың керекті өлшемін анықтау. Ақпаратты қорғау өлшеміне баға беру әдістері. Ақпараттық қорғау деңгейіне баға берудің негізгі көрсеткіштері. Қорғау өлшемдерінің сипаттамалары.</p>	1		5	2
<p>9. Қорғау процестерін тиімді басқаруы. Қорғаудың аппараттық құралдарын жобалауды; қорғаудың программалық жүйелерін жобалауды; қорғау өлшемдерін ұйымдастыруды жобалауды қауіпсіздендіруді қатамасыз ету процесстерін тиімді басқарудың әдістері мен модельдері.</p>	2		-	2
<p>10. Қорғау жүйелерге баға беру. Ақпаратты қорғау жүйесіне кешенді баға беру. Програмалық қамтамасыздандыру. Програмалық түлектерді тестілеу қыйындықтары, автоматтанған тестілеу, өзі тестілеу программаларды жазу принциптері. Тестерді дайын программаларға инсталляциялау. Қорғау механизмдердің сенімділігіне баға беру. Қорғау сенімділігіне принциптері.</p>	2		-	4
<p>11. Компьютерлік жүйелерінің қауіпсіздігі. Жергілікті тораптарда қорғау. Жеке ақпаратты қорғаудың</p>	2		10	5

программалық құралдары. Рұқсатсыз қатынауды табу үшін сараптық жүйелерді қолдану.				
Компьютерлік вирустар (4 сағат)		4	-	3
Рұқсат етілмеген енуден программалық қамтуды қорғау		4	-	3
Симметриялы криптожүйелер		6	-	3
Хабарламаға криптоанализ жасау үшін шифротексттердегі әріптердің жиілігін анықтау		4	-	3
Кілті ашық жүйелердегі мәліметтерді криптографилық әдіспен қорғау		6	-	3
Желідегі ақпаратты қорғау		6	-	3
БАРЛЫҒЫ:	15	30	45	45

Зертханалық сабақтар тізімі

1. Компьютерлік вирустар (4 сағат)
2. Рұқсат етілмеген енуден программалық қамтуды қорғау (4 сағат).
3. Симметриялы криптожүйелер (6 сағат)
4. Хабарламаға криптоанализ жасау үшін шифротексттердегі әріптердің жиілігін анықтау (4 сағат).
5. Кілті ашық жүйелердегі мәліметтерді криптографилық әдіспен қорғау (6 сағат).
6. Желідегі ақпаратты қорғау (6 сағат).

СӨЖ-ге арналған бақылау тапсырмаларының тақырыптары

1. Ақпараттық қауіпсіздендіру.
2. Ақпараттық жүйелердің аппараттық және программалық платформасын анализдеу.
3. Ақпараттық жүйелердің қауіпсіздік модельдері.
4. Қорғау және қауіпсіздендіру жүйелерін практикалық іске асыру мысалдары.
5. Қорғалған ақпараттық жүйенің негізгі сипаттамалары.
6. Ақпаратты қорғау дұрыстығының әдістемесі.
7. Ақпараттық қорғау өлшемі.
8. Қорғау процестерін тиімді басқаруы.
9. Қорғау жүйелерге баға беру.
10. Компьютерлік жүйелерінің қауіпсіздігі.
11. Шифрлеудің классикалық жүйелерін зерттеу.
12. Симметриясыз шифрлеу жүйелерін зерттеу.
13. Қорғауды оптималды басқаруды модельдеу программасын құру.
14. Қорғау процедураларын тестілеу программаларын құру.
15. Дизассемблерден және отладчиктен қорғау процедураларын құру.
16. Қорғау процедуралардың қыйындығына кешенді баға беру және зерттеу.
17. Қорғаудың сенімділігін анықтау программаларын құру.
18. Шабуылды бақылау үшін сараптамалық жүйе құру.

19. Ақпараттық қауіпсіздендіру және қорғау жүйелерінің кәзіргі ақпараттық процессіндегі ролі мен орны.

20. Ақпараттық қорғау жүйелері, ерекшілігі және негізгі сипаттамалары.

21. Ақпараттық қауіпсіздендіру жүйелері, ерекшілігі және негізгі сипаттамалары.

22. ҚР ақпараттық қорғау мен қауіпсіздендіру аймағындағы стандарттар құрылымы.

23. ҚР ақпараттық қорғау мен қауіпсіздендіру аймағындағы заңдар мен акттар.

Студенттер білімін бағалау критерийлері

Пән бойынша емтихан бағасы межелік бақылаулар бойынша максимум көрсеткіштер (60%-ға дейін) мен қортынды аттестаттаудың (емтихан) (40%-ға дейін) сомасы ретінде анықталады және кестеге сәйкес 100%-ға дейінгі мәнді құрайды.

Пән бойынша берілген тапсырмаларды орындау мен тапсыру кестесі

Бақылау түрі	Тапсырма мақсаты мен мазмұны	Ұсынылатын әдебиет	Орындау ұзақтығы	Бақылау түрі	Тапсыру мерзімі	Балл
Сабакқа қатысушылық	Ережелерді және процедураларды орындау	п.3 дәрісінің тақырыбына сәйкес	45 қатынас сағаттары	Ағымдағы	Әрбір дiрiсте	10
Зертханалық жұмыстарды қорғау	Тақырыптар бойынша материалдарды игеру	Бақылау жұмыстарды орындауға ЭН	30 қатынас сағаттары	Ағымдағы	2,4,6,7,9, 11,13,15 апта	20
СДЖ бақылау тапсырмалар	Тақырыптар бойынша материалдарды игеру. СДЖ бақылау тапсырмаларын орындау	[1-14], дәріс конспектілері	2 қатынас сағаттары	Ағымдағы	1-14 апта	10
СДЖ тапсырмаларының орындау	Тақырыптар бойынша материалдарды игеру. Тапсырмаларды орындау	[1-14]	2 қатынас сағаттары	Ағымдағы	1-14 апта	10
Модуль	Пән материалының меңгерілу деңгейін тексеру	Дәрістер конспекті	1 қатынас сағат	Межелік	7, 14 апта	10
Емтихан	Пән материалының игерілуін тексеру	Негізгі және қосымша әдебиеттер тізімі	3 қатынас сағаттары	Қорытынды	Сессия кезеңінде	40
Барлығы						100

Саясат және процедуралар

«Компьютерлік ақпаратты қорғау әдістері мен құралдары» пәнін оқу кезінде келесі ережелерді ұстануды сұраймын:

1. Сабаққа кешікпеу.
2. Сабақтан дәлелді себепсіз қалмау, ауырған жағдайда анықтама, ал басқа жағдайларда түсіндірме хат ұсынуды.
3. Сабақтың барлық түрлеріне қатысу студент міндеттерінің қатарына жатады.
4. Оқу процесінің күнтізбелік кестесіне сәйкес барлық бақылау түрін тапсыру.
5. Қатыспаған практикалық және зертханалық сабақтарды оқытушы көрсеткен уақытта өтеу.

Негізгі әдебиет тізімі

1. Алдажаров Қ.С. Ақпараттық қауіпсіздік негіздері: оқу құралы. – Алматы: Экономика, 2011.
2. Аяжанов Қ.С. Ақпараттық қауіпсіздік және ақпаратты қорғау: оқулық. – Алматы: «Дәуір», 2011.
3. Мүсірәлиева Ш.Ж. Қолданбалы криптография: Computer Science Еуропалық одақтық білім беру бағдарламасының оқу құралы. – Алматы: PRINT-S, 2004.
4. Яворский В.В. Компьютерлік жүйелерде ақпаратты қорғау әдістері және куралдары: оқу құралы. – Қарағанды: ҚарМТУ, 2007.
5. Әбдіқалықов Қ.Ә. Криптографияның негіздері. – Алматы: Білім, 2012.
6. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия - Телеком, 2011.
7. Герасименко В.А. Защита информации в автоматизированных системах. – М.: Высшая школа, 1995.
8. Домарев В.В. Защита информации и безопасность компьютерных систем. – Киев: Диасофт, 2005.
9. Аграновский А. В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Р, 2008.

Қосымша әдебиет тізімі

10. Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен куралдары. Ақпарат қауіпсіздігінің бұзылуларын басқару. – Астана: Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт), 2009.
11. Ақпараттық технология. Қорғау әдістері. Бақылау белгілері жүйелері. – Астана: Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт), 2009.
12. Ақпараттық технология. Қорғау әдістері. Электрондық цифрлық қолтаңбалар құралдарының жұмысқа қабілеттілігін қолдауға арналған ТТР сервистерінің спецификациясы. – Астана: Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт), 2009.
13. Зима В.М. и др. Безопасность глобальных сетевых технологий. – М.:ВНУ, 2007.
14. Домашев А.И. Программирование алгоритмов защиты информации. – М.: Нолидж, 2009.