Қазақстан республикасы Білім және ғылым министрлігі

Қарағанды мемлекеттік техникалық университеті

Бекітемін
Ғылыми кеңес төрағасы,
ректор, ҚР ҰҒА академигі
Ғазалиев А.М.

_____
«____» _____ 2016ж.

МАГИСТРАНТҚА ПӘН БОЙНЫША ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)

K 5308 «Криптология» пәні

АКҚТ 5 «Ақпаратты қорғаудың қазіргі технолгиялары» модулі

6М070400– «Есептеу техникасы және бағдарламалық қамтама» мамандығы

«Инновациялық технологиялар» факультеті

«Ақпараттық технологиялар және қауіпсіздік» кафедрасы

2016

Алғы сөз

Магистранттың пән бойынша оқыту бағдарламасын – syllabus әзірлеген
АТҚ кафедрасының аға оқытушысы, т.ғ.к. Исагулов С.Т.
АТҚ кафедрасының доценті т.ғ.к. Даненова Г.Т.

«Ақпараттық технологиялар және қауіпсіздік» кафедрасының отырысында талқыланған
№ _____ хаттама «____»_____2016ж.
Кафедра меңгерушісі _____ Көккөз М.М. «____»_____2016ж.

«Инновациялық технологиялар» факультетінің оқу-әдістемелік кеңесімен мақұлданған

№ _____ хаттама «___»_____2016ж.

Төрайымы_____ Мустафина Л.М. «___»_____2016ж.

Оқытушы туралы мәлімет және қатынас ақпараты

АТҚ кафедрасының аға оқытушысы, т.ғ.к. Исагулов С.Т.

«Ақпараттық технологиялар және қауіпсіздік» (АТҚ) кафедрасы ҚарМТУ (Қарағанды, Б.Мира 56) басты корпусында, 429 аудиторияда орналасқан, байланыс телефоны 56-75-98 (1028).

Пәннің еңбек көлемділігі

Семестр	Кредиттер саны	ECTS	Сабақ түрі					Жалпы сағаттар саны	Бақылау түрі
			Қатынас сабақтарының саны			МОӨЖ сағаттары-ның саны	Барлық сағаттар саны		
			дәріс	практикалық сабақтар	зертханалық сабақтар				
1	4	6	15	15	30	60	120	180	емтихан

Пән сипаттамасы

«Криптология» пәні профильді пәндердің цикліне, таңдау бойынша компонентке жатады.

Берілген пән магистранттарға ақпаратты жүйелердегі ақпаратты қорғау жүйелерін құру мен практикалық қолданылуының теориялық негіздерін, мәліметті қорғауды жүзеге асырудың принциптері, әдістері мен құралдары жайлы жүйелік ұғымын, жобалау мен қолдануға қажетті ақпараттық жүйелердегі ақпаратты қорғау бойынша практикалық икемдерін оқытады.

Пән мақсаты

«Криптология» білім беру процесі кезінде магистранттармен алынған негізгі теориялық білім мен оны практикалық тұрғыда тиімді қолдануын байланыстыруға қажетті пән.

Дамушы мақсаты шығармашылық тұлғаның қалыптасуына, есін, ойын, қиялын, сазын дамытуға, яғни кәсіптік қызметін қалыптастыруға бағытталған.

Практикалық мақсаты ақпараттық жүйелердегі ақпаратты қорғау жүйелерінде теориялық негіздерді құру мен практикалық қолданысын үйренуге бағытталған. Магистранттарды деректерді қорғаудың жүзеге асыруға қажетті принциптері, әдістері мен құралдары, жобалау мен қолдануға қажетті ақпараттық жүйелердегі ақпаратты қорғаудың практикалық дағдыларын алу жайлы жүйелік ұғымдарымен оқытылады.

Тәрбиелік мақсаты пәннің мазмұны ақпараттық қауіпсіздік пен ақпаратты қорғаудың заманауи өскелең ұрпақтың тәрбие талаптарына сәйкестігін көздейді, өз кезегінде оқушылардың азаматшылығын, көзқарасын, адамгершілігін және жоғары моралін қалыптастыруға бағытталған.

Пән міндеттері

Пән міндеттері: болашақ кәсіби мамандыққа қажетті икемділік пен дағдыларды қалыптастыру. Криптография мен криптологияның негізгі ұғымдарын, басты анықтамаларын, мазмұнын, мүмкіндіктерін шолу және практикалық мәліметтерді оқып білу.

Берілген пәнді оқу нәтижесінде магистранттар білуге міндетті:

- ақпараттық үрдістің ақпаратты енгізу, шығару, жіберу, өңдеу мен сақтауды жүзеге асырудың қорғау әдістері мен құралдары жайлы түсінік болу.
- ақпаратты қорғау объектілерінің ерекшеліктері мен классификациялары;
- ЖЭЕМ қорғау объектісі ретінде білу.
- ақпаратты қорғау құралдарын ақпараттық жүйелерді (АЖ) оңтайландыру мақсатында қолдану жайлы нақты міндеттерді қою мен орындау;
- вирустар мен ЖЭЕМ-ге рұқсатсыз қолжеткізуден қорғау жүйелерін қолдануын білу.
- АЖ-де қауіпсіздік деңгейін бағалаудың тәжірибелік дағдыларын иелену.
- ақпаратты қорғаудағы бағдарламалық жасақтамаларды құруда құзыретті болу.

Пререквизиттер

Берілген пәнді оқу үшін келесі пәндерді меңгеру қажет: «Дискретті математика», «Ақпарат теориясы».

Постреквизиттер

«Криптология» пәнін оқудан алынған білім келесі пәндерді меңгеруде қолданылады: «Жоғары жылдамдықты есептеу технологиялары», «Бағдарламалық жүйелерді жобалау технологиялары», «Жүйелер мен кешендерді модельдеу».

Пәннің тақырыптық жоспары

Тарау атауы, (тақырыптар)	Сабақ түрлері бойынша еңбек көлемділігі, сағ.				
	дәріс	практикалық	зертханалық	МОӨЖ	МӨЖ
1 Кіріспе. Компьютерлік жүйелер мен желілер қауіптерінің классификациясы.	1	-	2	4	4
2 Симметриялы криптожүйелер.	1	2	4	4	4
3 Кездейсоқ сандар генераторлары көмегімен гамма шығару.	1	2	4	4	4
4 Криптографиялау стандарттары.	1	2	4	4	4
5 ГОСТ 28147-89 шифрлеу стандарты.	1	-	-	4	4
6 Гаммирование режимінде шифрлау.	1	2	4	4	4
7 Ассиметриялы криптожүйелер.	1	-	-	4	4
8 Ассиметриялы шифрлау криптожүйесі.	1	2	4	4	4
9 Қайтымсыз бақылау реттіліктері.	1	-	-	4	4

10 Электронды цифрлық қолтаңба.	1	-	-	4	4
11 ГОСТ Р 34.11-2001 алгоритмы негізінде ЭЦҚ алу.	1	2	4	4	4
12 Аутентификация түрлері.	1	-	-	4	4
13 Аутентификация протоколдары.	1	2	4	4	4
14 Кілттер генерациясы.	1	-	-	4	4
15 Желі арқылы алыстан шабуылдан қорғаудың әдістері мен құралдары.	1	1	-	4	4
БАРЛЫҒЫ:	15	15	30	60	60

Практикалық (семинарлық) сабақтар тізімі

1 Сақталған паролді бұзудан қорғау қағидалары.

2. Сақталған паролді қорғауға қатысты бағдарламаны құрудың мүмкін нұсқалары.

3. Диффи-Хеллман бойынша шифрлау модельдері.

4. Сызықтық конгруэнтті генераторында кездейсоқ сан генераторының жұмысы.

5. Тіркелімде еркін ұзындықта жылжытудағы ПСЧ генераторына бағдарлама құру әдістемесі.

6. Кесте әдісі бойынша шифрлау әдістемесі.

7. Әртүрлі хэш-функциядағы ерікті мәтінді хэштеу модельдері.

8. Толық сенім режиміндегі симметриялы жүйе аутентификациясы.

9. Толық сенім емес режиміндегі симметриялы жүйе аутентификациясы.

10. Қатаң аутентификация протоколдары.

Зертханалық сабақтар тізімі

1 Тәжірибелік әдіс көмегімен сақталған паролді зерттеуден қорғау.

2 Диффи-Хеллман бойынша шифрлау әдістерін зерттеу.

3 Сызықтық контруэнтті кездейсоқ сан генераторына бағдарлама құру.

4 Тіркелімде еркін ұзындықта жылжыту генераторын моделдеу бағдарламасын құру.

5 Жай кестелік ауыстыру әдісімен файлды шифрлау бағдарламасын құру.

6 Hash әдісі көмегімен гамма циклді сызықсыз кіріспе мен оны файлға жүктеу шығару үшін бағдарлама құру.

МӨЖ-ге арналған бақылау тапсырмаларының тақырыбы

1. Сақталған паролді бұзудан қорғаудың қағидаларын тану.

2. Сақталған паролді қорғаудың қағидаларын желіде қарау.

3. Әр моделден регистрлер жылжыту негізінде кездейсоқ сан генераторын құру.

4. Құрылғының разрядты тордағы үлкен сан модулін алуға қажетті модулді арифметикамен жұмысқа тиіс әдістеме мен бағдарламаны қарау.

5. Жылдамдату әдісі көмегімен модулді арифметиканың үлкен сандарды көбейту модулін қарастыру.

6. Жылдамдату әдісі көмегімен модулді арифметиканың үлкен сандрады дәрежелеу моделін қарастыру.

7. Сызықты конгруэнтті генератордың үлкен сандарда орындалуын қарастыру.

8. 32-битті машинада жекелеген блоктардың ГОСТ 28147-89 орындалуын қарастыру.

9. Алдында құрылған рәсімдер негізінде шифрлау блогын жай ауыстыру режимінде құру.

10. SHA стандартында Hash моделін алуды зерттеу.

11. Бүтін санды арифметикаға қажетті үлкен бүтін сандармен жұмыс. Үлкен ұзындықты бүтін сандарды бөлу (мысалы, ұзындығы 20 байт).

12. Бүтін санды арифметикаға қажетті үлкен бүтін сандармен жұмыс. Үлкен ұзындықты бүтін сандарды алу (мысалы, ұзындығы 20 байт).

13. Үлкен сандарды көбейту мен бөлу моделдері.

14. Санды қарапайымдылыққа анықтау әдістемесі. Моделді құру.

15. Эль Гамаль алгоритмі негізінде ЭЦҚ моделін тану.

Магистранттар 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
Зертханалық	Зертханалық жұмыс №1 «Бағдарламалық жасақтаманы рұқсатсыз ие болудан қорғауды қарапайым әдіспен жүзеге асыру»	[1], [2], [3] [5]	3 апта	ағымдағы	3 апта	3
МОӨЖ	Зертханалық жұмыс 1 дайындық «Бағдарламалық жасақтаманы парольмен қорғау»	[1], [2], [3] [5]	3 апта	ағымдағы	3 апта	2
МОӨЖ	Зертханалық жұмыс 1 қорғау	[1], [2], [3], [5], [6],[10]	1 апта	ағымдағы	3 апта	2
Зертханалық	Зертханалық жұмыс №2 «Алгоритмдік шифрлеудің тура ауыстыру әдісін жүзеге асыру»	[1], [2], [3], [5], [6],[10]	2 апта	ағымдағы	5 апта	3
СРМП	Зертханалық жұмыс 2 дайындық «Тура ауыстыру әдістері (Цезарь,	Негізгі және қосымша әдебиеттер тізімі, дәріс	3 апта	ағымдағы	5 апта	2

	Еврейскйи)»	конспектілері				
МОӨЖ	Зертханалық жұмыс №2 рәсімдеу мен қорғау. Межелік бақылау.	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	1 апта	ағымдағы	5 апта	2
Зертханалық	Зертханалық жұмыс №3 «Алгоритмдік шифрлеудің ауыстыру әдістерін жүзеге асыру»	[1], [2], [3], [10], [14],[15]	2 апта	ағымдағы	7 апта	3
МОӨЖ	Зертханалық жұмыс №3 дайындық «Сиқырлы шаршы әдісін жүзеге асыру»	[1], [2], [3], [5], [12],[11]	3 апта	ағымдағы	7 апта	2
МОӨЖ	Зертханалық жұмыс №3 рәсімдеу мен қорғау.	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	7 апта	2
Зертханалық	Зертханалық жұмыс №4 «Блокті алгоритмдік шифрлеуді жүзеге асыру»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	2 апта	ағымдағы	9 апта	3
МОӨЖ	Зертханалық жұмыс 4 дайындық «Биграмм әдісін жүзеге асыру»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	3 апта	ағымдағы	9 апта	2
МОӨЖ	Зертханалық жұмыс №4 рәсімдеу мен қорғау.	[1], [2], [3], [5], [6],[10]	1 апта	ағымдағы	9 апта	2
Зертханалық	Зертханалық жұмыс №5 «Көпілмекті алгоритм шифрлеуін жүзеге асыру»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	2 апта	ағымдағы	11 апта	3
МОӨЖ	Зертханалық жұмыс 5 дайындық «Виженер әдісін жүзеге асыру»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	3 апта	ағымдағы	11 апта	2
МОӨЖ	Межелік бақылау	[1], [2], [3], [10], [14],[15]	1 апта	ағымдағы	10 апта	2
МОӨЖ	Зертханалық жұмыс №5 рәсімдеу мен қорғау.	[1], [2], [3], [10], [14],[15]	1 апта	ағымдағы	11 неделя	2

Лабо-раторная	Зертханалық жұмыс №6 «Кездейсоқ сандар тетігін жүзеге асыру»	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	13 апта	3
МОӨЖ	Зертханалық жұмыс 6 дайындық «Дискретті кездейсоқ шаманы моделдеу»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	3 апта	ағымдағы	13 апта	2
МОӨЖ	Зертханалық жұмыс 7 дайындық «Кездейсоқ сандар тетігін графикалық бағалау»	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	3 апта	ағымдағы	14 апта	2
Зертханалық	Зертханалық жұмыс 7 «Кездейсоқ сандар тетігінің сапасын бағалау»	[1], [2], [3] [5]	3 апта	ағымдағы	15 апта	3
МОӨЖ	Зертханалық жұмыс 7 рәсімдеу мен қорғау.	[1], [2], [3], [5], [6],[10]	1 апта	ағымдағы	15 апта	2
МОӨЖ	Межелік бақылау	[1], [2], [3], [5], [6],[10]	1 апта	ағымдағы	14 апта	2
№1 коллоквиум	Ақпаратты шифрлеу бойынша теориялық білім мен практикалық дағдыларды бекіту	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	1 қатынас сағаттары	аралық	7 апта	4,5
№2 коллоквиум	Ақпаратты шифрлеу бойынша теориялық білім мен практикалық дағдыларды бекіту	Негізгі және қосымша әдебиеттер тізімі, дәріс конспектілері	1 қатынас сағаттары	аралық	14 апта	4,5
Емтихан	Пән материалының игерілуін тексеру	Негізгі және қосымша әдебиеттер тізімі	3 қатынас сағаттары	Қорытынды	Сессия кезінде	40
Барлығы						100

Саясат және процедуралар

«Криптология» 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.

6. Курстастар мен оқытушыларға төзімді, ашық және аққөңіл болу.

Негізгі әдебиет тізімі

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком. 2007. -452с.
2. Герасименко В.А. – Защита информации в автоматизированных системах обработки информации. Книга 1,2 – М.: Энергоатомиздат, 2012. -176с.
3. Салома А. Криптография с открытым ключом.
4. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. — М.: Сов. радио, 2008.-264с.
5. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. Издательство агентства Яхтсмен М.- 2006 -71с.
6. Мельников В. В. Защита информации в компьютерных системах Москва «Финансы и статистика» «Электроинформ» 2007. -368с. 161
7. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях Издательство агентства «Яхтсмен» М.-, 2008. - 368с

Қосымша әдебиет тізімі

8. Анин Б. Защита компьютерной информации. - СП6.: БХВ-СанкПетербург, 2000.-384с.
9. Милославская Н.Г. Толстой А.И. Интрасети: доступ в Интернет, защита: Учебное пособие для вузов. - М.: ЮКИТИ-ДАНА, 2007.-527 с.
10. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях /Под ред. В.Ф. Шаньгина,- М.: Радио и связь, 2009.-328 с.
11. Домашев А.В., Попов В.О., Правиков Д.И., Прокофьев И.В., Щербаков А.Ю. Программированием алгоритмов защиты информации. Учебное пособие -М.: «Нолидж», 2008,-288с.
12. Гульев И.А. Компьютерные вирусы взгляд изнутри - М.: ДМК,2008-304с.
13. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 2011.-216с.
14. Гостехкомиссия РФ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. — М.: Воениздат, 2002.
15. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие, Алматы: КазНТУ, 2010-125с. ISB 9965-487-З 6-7 162.

МАГИСТРАНТҚА ПӘН БОЙНЫША
ОҚЫТУ БАҒДАРЛАМАСЫ (SYLLABUS)

K 5308 «Криптология» пәні

АККТ 5 «Ақпаратты қорғаудың қазіргі технолгиялары» модулі

31.03.2015 ж. № 50 мемл. бас. лиц.

Баспаға _____ 20__ж. қол қойылды. Пішіні 90х60/16. Таралымы _____ дана

Көлемі ___ оқу бас. п. № _____ тапсырыс Бағасы келісілген

_____

100027. ҚарМТУ баспасы, Қарағанды, Бейбітшілік бульвары, 56