

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

ҚАРАҒАНДЫ МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ

БЕКІТЕМІН

**Ғылыми кеңес төрағасы,
ҚарМТУ ректоры, ҚР ҰҒА
академигі Ғазалиев А.М.**

« ____ » _____ 2015 ж.

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

АТК 5202 «Ақпараттық технологиялар қауіпсіздігі» пәні
(коды және атауы)

AZhT 2 «Ақпараттық жүйелер және технологиялар» модулі
(коды және атауы)

6M070300 – Ақпараттық жүйелер мамандығы
(шифры және атауы)

Ақпараттық технологиялар факультеті

Ақпараттық-есептеуіш жүйелер кафедрасы

АЛҒЫСӨЗ

Магистрантқа арналған пән бойынша оқыту бағдарламасын (syllabus) әзірлеген:
Ph.D. докторы, каф. меңгерушісі Амиров А.Ж., т.ғ.к, доцент Баймұльдин М.К.
(аты-жөні, ғылыми дәрежесі, ғылыми атағы.)

«Ақпараттық-есептеуіш жүйелер» кафедрасының отырысында талқыланды
« ____ » _____ 2015 ж. № _____ хаттама
Кафедра меңгерушісі _____ Амиров А.Ж. « ____ » _____ 2015 ж.
(қолы) (А.Ж.Ә.)

Ақпараттық технологиялар факультетінің оқу-әдістемелік кеңесі
мақұлдаған

« ____ » _____ 2015 ж. № _____ хаттама
Төраға _____ Мустафина Л.М. « ____ » _____ 2015 ж.
(қолы) (А.Ж.Ә.)

Ақпараттық-есептеуіш жүйелер кафедрасымен келісілген
(кафедраның атауы)

Кафедра меңгерушісі _____ Амиров А.Ж. « ____ » _____ 2015 ж.
(қолы) (А.Ж.Ә.)

Оқытушы туралы мәлімет және қатынас ақпараты

А.Ж.Ә. Баймульдин Мурат Каирович

Ғылыми дәрежесі, лауазымы, қызметі т.ғ.к., доцент

АЕЖ кафедрасы ҚарМТУ-дың негізгі корпусында орналасқан (Бейбітшілік бульвары, 56), 301 аудитория, байланыс телефоны 56-59-35 қосымша 2054.

Пәннің еңбек көлемділігі

Семестр	Кредиттер саны	ECTS	Сабақ түрі					МӨЖ сағаттарының саны	Жалпы сағат саны	Бақылау түрі дәріс
			Қатынас сабақтарының саны			МӨЖ сағаттарының саны	Барлық сағат саны			
			дәріс	практикалық сабақтар	зертханалық сабақтар					
Оқыту түрі – күндізгі оқу										
2	3	5	15	-	30	45	90	45	135	Емтихан

Пән сипаттамасы

«Ақпараттық технологиялар қауіпсіздігі» пәні бейімдік пәндерінің (таңдау бойынша компонент) циклына жатады.

Пәннің мақсаты

«Ақпараттық технологиялар қауіпсіздігі» пәні қорғалған ақпараттық жүйелердің техникалық, бағдарламалық және ақпараттық қамтамасыз етуін ұйымдастырудың негізгі принциптерін зерттеуді, сонымен қатар, осындай жүйелерді пайдалану және теориялық, практикалық тәжірибе қалыптастыруды мақсат етеді.

Пән міндеттері

Осы пәнді оқыту нәтижесінде магистранттар:

түсінік алуы керек:

– криптографиялық стандарттар туралы;

– ашық мәтіндерді сипаттау жиіліктері және оларды қарапайым симметриялық криптожүйелерді талдауда қолдану туралы;

білу керек:

– негізгі криптографиялық қарапайымдар және оларды ақпаратты қорғаудың негізгі есептерін шешуде қолдануды;

– құру принциптерін және симметриялық және асимметриялық криптографиялық алгоритмдердің негізгі түрлерін;

істей алуы керек:

- симметриялық және асимметриялық криптографиялық алгоритмдерді дұрыс қолдануды;
- криптожүйелерді зерттеудің және сипаттаудың математикалық тәсілдерін қолдануды;
- практикалық машықтануы керек:
 - типтік криптографиялық алгоритмдерді қолдануды;
 - криптографиядағы математикалық моделдеу.

Пререквизиттер

Бұл пәнді оқу үшін «Бағдарламалаудың жаңа заманғы технологиялары» пәнін игеру қажет.

Постреквизиттер

«Ақпараттық технологиялар қауіпсіздігі» пәнін оқу кезінде алынған білім «Ақпараттық жүйелердің инфрақұрылымы», «Эксперименталді деректерді өңдеу алгоритмдері» пәндерін игеру кезінде қолданылады.

Пәннің тақырыптық жоспары

Тақырып атауы	Сабақ түрлері бойынша сыйымдылығы, с				
	дәріс	практикалық	зертханалық	МОӨЖ	МӨЖ
1 Кіріспе. Ақпарат қорғау жүйесін жобалау негіздері	2				
2 Ақпараттық үрдістерде ақпаратты енгізу, шығару, беру, өңдеу және сақтауды жүзеге асыру кезінде ақпаратты қорғау	2				
3 Ақпаратты қорғау әдістері мен құралдары. Ақпаратты қорғаудың теориялық әдістері	2				
4 Ақпаратты қорғаудың практикалық әдістері	2				
5 Компьютерлер мен желілердегі ақпаратты қорғаудың бағдарламалық құралдары	2				
6 Ақпаратты қорғаудың криптографиялық құралдары	2				
7 Компьютерлік және желілік ақпараттарды қорғауды ұйымдастыру және техникалық құралдары	3				
8 Ақпараттық технологиялар қауіпсіздігін қамтамасыз ететін				6	6

принциптеріне және негізгі құралдарына шолу					
9 Ақпараттық жүйелерде шектеулі қол жетімділікті қамтамасыз ететін принциптер және құралдар				6	6
10 Қазіргі криптографиялық құралдар. Операциялық жүйелердің және деректер базасының желілік қорғау құралдары.				9	9
11 PGP шифрлеу құралдары. Мәліметтерді тасымалдаудың қорғалған желілік протоколдары: SSL, TSL, HTTPS, IPSec, PPTP, PPPoE.				6	6
12 OpenVPN виртуалды желілерді құрудың технологиясы.				6	6
13 RAID мәліметтерінің сақтық көшірмелеу технологиялары. Бағдарламалық және аппараттық IPS, қызмет көрсетуде шабуылдарға қарсы әрекеттер құралдары.				6	6
14 ActiveDirectory қолданушыларымен және каталогтармен басқару қызметі. LDAP қолданушыларымен және каталогтармен басқару қызметі				6	6
15 Криптография. Ауыстыруға арналған шифрлар.			6		
16 Ашық мәтіннің статистикалық мінездемесі			6		
17 Хилла шифрі			6		
18 Мәтінді архивтеу			6		
19 Шифрация мәтінінің суреттегі әдісі			6		
20 Компьютер вирустары			6		
21 Пароль қорғауы			6		
22 Криптография			6		
23 Қатынастардың криптоанализға			6		

арналған мәтіндердегі әріптердің жиілігінің табылуы					
24 Желідегі ақпарат қорғауы			6		
БАРЛЫҒЫ	15		60	45	45

Зертханалық сабақтар тізімі

- 1 Криптография. Ауыстыруға арналған шифрлар.
- 2 Ашық мәтіннің статистикалық мінездемесі
- 3 Хилла шифрі
- 4 Мәтінді архивтеу
- 5 Шифрация мәтінінің суреттегі әдісі
- 6 Компьютер вирустары
- 7 Пароль қорғауы
- 8 Криптография
- 9 Қатынастардың криптоанализға арналған мәтіндердегі әріптердің жиілігінің табылуы
- 10 Желідегі ақпарат қорғауы

Магистрант пен оқытушының өздік жұмысының тақырыптық жоспары

МОӨЖ тақырыбының атауы	Сабақ мақсаты	Сабақ өткізу түрі	Сабақ мазмұны	Ұсынылатын әдебиет
1 Ақпараттық технологиялар қауіпсіздігін қамтамасыз ететін принциптеріне және негізгі құралдарына шолу	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[1-4]
2 Ақпараттық жүйелерде шектеулі қол жетімділікті қамтамасыз ететін принциптер және құралдар	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[1-4]
3 Қазіргі криптографиялық құралдар. Операциялық жүйелердің және деректер базасының желілік қорғау құралдары.	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[2-4]
4 PGP шифрлеу құралдары. Мәліметтерді тасымалдаудың қорғалған желілік протоколдары: SSL, TSL, HTTPS, IPSec, PPTP, PPPoE.	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[3-4]

5 OpenVPN виртуалды желілерді құрудың технологиясы.	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[2,3]
6 RAID мәліметтерінің сақтық көшірмелеу технологиялары. Бағдарламалық және аппараттық IPS, қызмет көрсетуде шабуылдарға қарсы әрекеттер құралдары.	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[2,3]
7 ActiveDirectory қолданушыларымен және каталогтармен басқару қызметі. LDAP қолданушыларымен және каталогтармен басқару қызметі	Осы тақырып бойынша білімдерді тереңдету	Кеңестер және әңгімелесу	Қойылған сұрақтарға жауап беру	[3-4]

МӨЖ-ге арналған бақылау тапсырмаларының тақырыптары

1 Ақпараттық технологиялар қауіпсіздігін қамтамасыз ететін принциптеріне және негізгі құралдарына шолу

2 Ақпараттық жүйелерде шектеулі қол жетімділікті қамтамасыз ететін принциптер және құралдар

3 Қазіргі криптографиялық құралдар. Операциялық жүйелердің және деректер базасының желілік қорғау құралдары.

4 PGP шифрлеу құралдары. Мәліметтерді тасымалдаудың қорғалған желілік протоколдары: SSL, TSL, HTTPS, IPSec, PPTP, PPPoE.

5 OpenVPN виртуалды желілерді құрудың технологиясы.

6 RAID мәліметтерінің сақтық көшірмелеу технологиялары. Бағдарламалық және аппараттық IPS, қызмет көрсетуде шабуылдарға қарсы әрекеттер құралдары.

7 ActiveDirectory қолданушыларымен және каталогтармен басқару қызметі. LDAP қолданушыларымен және каталогтармен басқару қызметі

Магистранттар білімін бағалау критерийлері

Пән бойынша емтихан бағасы аралық бақылау (60% дейін) және қорытынды аттестаттау (емтихан) (40% дейін) бойынша үлгерімнің ең жоғары көрсеткіштерінің сомасы ретінде анықталады және кестеге сәйкес 100% дейін мәнді құрайды.

Пән бойынша берілген тапсырмаларды орындау және тапсыру кестесі

Бақылау түрі	Тапсырма мақсаты мен мазмұны	Ұсынылатын әдебиет	Орындау ұзақтығы	Бақылау түрі	Тапсыру мерзімі	Балл
--------------	------------------------------	--------------------	------------------	--------------	-----------------	------

1	2	3	4	5	6	
Дәрістерге, зертханалық жұмыстарға, МООЖ, МӨЖ қатысу	Тақырыптар бойынша материалды игеру	Дәрістердің конспектісі	15 апта	АҒЫМДЫҚ	Әр дәрісте	10
№ 1-10 зертханалық жұмыстарды тапсыру	Тақырыптар бойынша материалды игеру	Зертханалық жұмыстарға әдістемелік нұсқаулар	15 апта	АҒЫМДЫҚ	2,4,7,9, 12,15 апталарда	20
МООЖ тапсырмалары	Тақырыптар бойынша білімді игеру	МООЖ тақырыптарына сәйкес	15 апта	АҒЫМДЫҚ	Әр апта	4
МӨЖ тапсырмалары	Тақырыптар бойынша білімді игеру	МӨЖ тақырыптарына сәйкес	15 апта	АҒЫМДЫҚ	Әр апта	4
Теориялық модуль	Пәннің материалын меңгеруін тексеру	Дәрістердің конспектісі	0,5 сағ.	Аралық	7, 14 апта	22
Емтихан	Пәннің материалын меңгеруін тексеру	Барлық ұсынылатын әдебиеттер тізімі	2 сағ.	Қорытынды	15 апта	40
Барлығы						100

Саясат және процедуралар

«Ақпараттық технологиялардың қауіпсіздігі» пәнін оқу кезінде келесі ережелерді сақтауды өтінеміз:

- 1 Сабаққа кешікпей келуді.
- 2 Дәлелді себепсіз сабақ босатпауды, ауырған жағдайда анықтама, ал басқа жағдайларда түсініктеме хат ұсынуды.
- 3 Магистранттың міндетіне барлық сабақтарға қатысу кіреді.
- 4 Оқу процесінің күнтізбелік жоспарына сәйкес бақылаудың барлық түрлерін тапсыру.
- 5 Жіберілген практикалық және зертханалық сабақтар оқытушы белгілеген уақытта қайта тапсыру.

Негізгі әдебиет тізімі

- 1 Б. Ю. Анин. Защита компьютерной информации: научное издание /Б.Ю. Анин. - СПб.: БХВ - Санкт-Петербург, 2000. - 368 с.
- 2 Криптография: скоростные шифры: научное издание /А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. - СПб. : БХВ - Петербург, 2002. - 493 с.
- 3 В. И. Ярочкин. Информационная безопасность: Учебник / В.И. Ярочкин. - М.: Фонд "Мир" : Академический Проект, 2003. - 640 с.

4. А. В. Соколов Методы информационной защиты объектов и компьютерных сетей научное издание / А. В. Соколов, О. М. Степанюк. М. : АСТ, 2000. - 272 с.

5 Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпарат қауіпсіздігінің бұзылуларын басқару [Текст] : 27.10.2009 ж. № 534-од бекітілді = Информационная технология. Методы и средства обеспечения безопасности. Управление нарушениями безопасности информации : утв. 27.10.2009 № 534-од / Қазақстан Республикасының Мемлекеттік стандарты = Государственный стандарт Республики Казахстан. - ресми басылым = офиц. издание. - Введ. с 01.07.2010 ж. с Алғаш рет енгізілді = Впервые. - Астана : Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт), 2009. - 124 б.

6 Шукаев, Д. Н. Ақпараттық процестерді талдау және модельдеу [Текст] : оқулық Қазақстанның жоғарғы оқу орындары техникалық мамандықтарының магистранттары үшін ұсынған / Д. Н. Шукаев ; Қазақстан Республикасы білім және ғылым министрлігі. - Алматы : Эверо, 2005. - 184 б.

Қосымша әдебиет тізімі

5 И. Конеев. Информационная безопасность предприятия : научное издание / И. Конеев, А. Беляев. - СПб. : БХВ - Петербург, 2003. - 733 с.

6 А. А. Садердинов. Информационная безопасность предприятия : учеб. пособие / А.А. Садердинов, В.А. Трайнёв, А.А. Федулов; МАН ИПТ. - М. : Изд.-торговая корпорация Дашков и К*, 2004. - 335 с.

7 В. М. Зима. Безопасность глобальных сетевых технологий : научное издание / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - СПб. : БХВ - Петербург, 2003. - 362 с.

8 Поточные шифры : учеб.-справ. пособие /А. В. Асосков [и др.]. - М. : Кудиц-Образ, 2003. - 334 с.

9 О. С.Зензин. Стандарт криптографической защиты - AES. Конечные поля : учеб.-справ. пособие / О.С. Зензин, М.А. Иванов. - М. : Кудиц-Образ, 2002. - 174 с.

10 А. В. Петраков. Охрана и защита современного предприятия / А.В. Петраков, П.С. Дорошенко, Н.В. Савлуков. - М.: ЭНЕРГОАТОМИЗДАТ, 1999. - 568 с.

11 Технические методы и средства защиты информации : научное издание / Ю. Н. Максимов [и др.]; Под ред. В. Г. Сонникова. - СПб. : Полигон, 2000. - 320 с.

12 Л. К.Бабенко. Защита информации с использованием смарт-карт и электронных брелоков : научное издание / Л.К. Бабенко, С.С. Ищуков, О.Б. Макаревич. - М. : Гелиос АРВ, 2003. - 352 с.

13 В. А. Галатенко. Основы информационной безопасности : курс лекций / В.А. Галатенко; под ред. В.Б. Бетелина. - М. : Интернет-Ун-т Информац. Технологий, 2004. - 277 с.

14 Скотт Бармен. Разработка правил информационной безопасности : пер. с англ. / С. Бармен. - М.; СПб.; Киев : ИД "Вильямс", 2002. - 207 с.

15 Норберт Польман. Архитектура брандмауэров для сетей предприятия : пер. с англ. / Н. Польман, Т. Кразерс. - М.; СПб.; Киев : ИД "Вильямс", 2003. - 420 с. :

16 Г.Д. Когай. Проектирование и защита корпоративных информационных систем: монография для студентов, аспирантов и преподавателей, специализирующихся в области компьютерных систем управления / Г. Д. Когай, Э. Г. Кесарева, Т. Л. Тен; М-во образования и науки РК, КарГТУ, Караганда : 2009. - 177 с.

17 В.Ю. Скиба. Руководство по защите от внутренних угроз информационной безопасности : научное издание / В. Ю. Скиба, В. А. Курбатов. - М.; СПб.; Нижний Новгород : Питер, 2008. - 318 с.

18 С.В. Гордейчик. Безопасность беспроводных сетей : научное издание / С. В. Гордейчик, В. В. Дубровин. - М. : Горячая линия - Телеком, 2008. - 288 с.

19 В. В. Платонов. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие / - М. : Академия, 2006. - 239 с. -.

20 Д.Донцов. Как защитить компьютер от ошибок, вирусов, хакеров: научное издание - М.; СПб.; Нижний Новгород : Питер, 2006. - 143 с. :

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

АТК 5202 «Ақпараттық технологиялар қауіпсіздігі» пәні
(коды және атауы)

AZhT 2 «Ақпараттық жүйелер және технологиялар» модулі
(коды және атауы)

31.03.2004 ж. № 50 мемл. бас. лиц.
Баспаға _____ 20__ ж. қол қойылды. Пішіні 90x60/16. Таралымы _____ дана
Көлемі _____ оқу бас. п. № _____ тапсырыс Бағасы келісілген