

Қазақстан Республикасы білім және ғылым министрлігі
Қарағанды мемлекеттік техникалық университеті

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

« ____ » _____ 2013ж.

СТУДЕНТКЕ АРНАЛҒАН ПӘН БОЙЫНША ОҚЫТУ
БАҒДАРЛАМАСЫ (SYLLABUS)

КАКАК 3302 «Компьютерлік ақпаратты қорғау әдістері және құралдары»
пәні

КАКАК 24 «Компьютерлік ақпаратты қорғау әдістері және құралдары»
модулі

5В100200 «Ақпараттық қауіпсіздік жүйелері» мамандығы

Ақпараттық технологиялар факультеті

Ақпараттық технологиялар және қауіпсіздік кафедрасы

Алғы сөз

Студентке арналған пән бойынша оқыту бағдарламасы (syllabus) әзірлегендер: АТҚ кафедрасының аға оқытушысы Мурых Е.Л., к.э.н., аға оқытушысы Жақсыбаев Қ.Р.

«Ақпараттық технологиялар және қауіпсіздік» кафедрасының отырысында талқыланған

« ____ » _____ 2013 ж. № ____ хаттама

Кафедра меңгерушісі _____ Көккөз М.М. « ____ » _____ 2013 ж.

(қолы)

Ақпараттық технологиялар факультетінің оқу-әдістемелік кеңесі мақұлдаған

« ____ » _____ 2013 ж. № ____ хаттама

Төраға _____ Мустафина Л.М. « ____ » _____ 2013 ж.

(қолы)

Оқытушы туралы мәліметтер және байланыс ақпарат

Мурых Елена Львовна АТҚ кафедрасының аға оқытушысы., к.э.н., аға оқытушысы Жақсыбаев Қуат Рахметоллаевич

«Ақпараттық технологиялар және қауіпсіздік» кафедрасы КарГТУ (Бейбітшілік бульвары, 56) бас корпусында, 429 аудитория, байланыс телефоны 56-75-98 қосымша 1028.

Пәннің еңбек көлемділігі

Семестр	Кредиттер саны	ECTS кредиттер	Сабақ түрі					СӨЖ сағаттар саны	Жалпы сағаттар саны	Бақылау түрі
			Қатынас сабақтарының саны			ОСӨЖ сағаттарының саны	Барлығы сағаттар саны			
			Дәріс	Практикалық сабақтар	Зертханалық сабақтар					
5	2	3	15		15	30	90	30	90	Емтихан

Пәннің сипаттамасы

«Компьютерлік ақпаратты қорғау әдістері және құралдары» пәні «Ақпарат қорғау құқықтық негіздері» модулінің құрамында негізгі компонент құрамына профильдік пәндер циклына кіреді.

Пәннің мақсаты

Бұл пәннің мақсаты студенттерді компьютерлік жүйелерде және желілерде ақпаратты қорғаудың негізгі принциптеріне үйрету, сонымен қоса ақпараттық қауіпсіздікті қамтамасыз ету.

Пәннің міндеттері

Пәннің мақсаты келесілер:

- жүйелерге және ақпаратқа негізгі қауіптерді анықтау;
 - қауіптерге қарсы әрекеттер әдісі;
 - криптографиялық жүйелер негізінде ақпаратты қорғау әдістері;
 - аутентификация және идентификацияның негізгі әдістері;
 - ақпаратты модификациялаудың қарсы әрекеттер әдістері;
 - ақпаратты тираждаудан қорғау әдістері;
 - электромагниттік сәулелену арқылы ақпараттарды ұстап алудан қорғау әдістері ;
 - желі бойынша ақпаратты беруді қорғау әдістерін оқу.
- Осы пәнді оқып үйрену нәтижесінде студент білуі керек:
- «Компьютерлік ақпаратты қорғау әдістері және құралдары» пәннің негізгі ережелері;
 - ақпаратты қорғаудың негізгі қауіптері;

- ақпаратты қорғаудың әдістері және негізгі принциптері;
- ақпаратты қорғау бойынша негізгі және нормативті құжаттар;
- ақпаратты қорғауды ұйымдастыру тәртібі, ақпараттық қауіпсіздік жүйесін эксплуатациялау және әзірлеу барысында қауіпсіздік шарттарын қамтамасыздандыру принциптері туралы ұғымы болуы керек.
- алгоритмді әзірлеу пинциптері;
- бағдарламаны тестілеу және отладка жасау;
- тағайындау және алгоритмдерді анализдеу принциптері;
- интерпретаторлар мен компиляторлар құру үшін формальды тілдерді орындауды білуі керек.
- ақпараттың ағу арнасын және қауіпті анықтау; ақпаратты қорғау үшін алгоритмдер мен хаттамаларды таңдау; ақпарат қауіпсіздігінің қауіпін бағалау;
- ақпаратты қорғау құралы және қолайлы әдістерді қолдану және сауатты қолдана білу;
- кең таралған бағдарламалық құралдарда криптографиялық алгоритмдерді қолдану, криптографикалық алгоритмдерді жүзеге асыру, олардың сапасын тексеруді жасай білуі керек
- ақпараттық қауіпсіздік шартын талдау және жобалау барысында ақпараттық қауіпсіздікті қамтамасыз ету бойынша жүргізілетін ұйымдастыру шаралары және техникалық таңдау ,
- критикалық ақпаратты өңдеу құралдарын эксплуатациялау және әзірлеу дағдысы болуы қажет.

Пререквизиттер

Бұл пәнді оқу үшін келесі пәндерді игеру қажет:

«Информатика», «Математика I», «Математика II», «Алгоритмдік тілдер және бағдарламалау»

Постреквизиттер

«Компьютерлік ақпаратты қорғау әдістері және құралдары» пәнін оқу кезінде алынған білім «Ақпаратты қорғау жүйелерін жобалау» пәндерін игеру кезінде қолданылады:

Пәннің тақырыптық жоспары

Тарау атауы, (тақыптар)	Сабақ түрлері бойынша еңбек көлемділігі, сағ.				
	Дәріс	Практикалық саб.	Зертханалық саб.	ОСӨЖ	СӨЖ
1. Кіріспе	1				
2. Компьютерлік жүйелердің қауіптерінің негізгі түрлері	1			2	
3. Қорғаудың негізгі компоненттері.	1				
4. Қолданушылардың және үрдістердің	1		2	2	

идентификациясы.					
5. Ақпаратқа қол жеткізуді бақылау әдістері.	1		1	2	
6. Мәліметтерді және бағдарламаларды криптографиялық қорғау.	5		7	14	
7. Ақпараттық ресурстарды бұзудан, түрлендіруден және көшіруден сақтау.	1		2	2	
8. Телекоммуникация желілері бойынша электромагниттік сәулелену арқылы ақпаратты ұстап алудан қорғау.	1			2	
9. Бағдарламалық және аппараттық закладкаларға қарсы әрекет.	1		1	2	
10. Антивирустық қорғау.	1			2	
11. Бағдарламаларды бұзу құралдарына қарсы әрекет.	1		2	2	
12. Отладчиктер арқылы бағдарламаны зерттеу қарсы әрекет әдістері.					3
13. Жіберу арналары арқылы ақпараттық ресурстарды қорғау.					3
14. Мәліметтер қорында ақпаратты қорғау.					3
15. Мәліметтер қорындағы ақпаратты қорғау ерекшеліктері.					3
16. Web- технологияларда ақпаратты қорғау.					3
17. Виртуальды жеке желілерде қорғау.					3
18. Жылжыту регистріндегі псевдокездейсоқ сандар генераторы.					3
19. Ақпараттық ресурстарды бұзудан, түрлендіруден және көшіруден сақтау.					3
20. Бағдарламалық модельдеу және ақпараттық қауіпті болжау.					3
21. Электронды құжат айналым жүйелерінде қорғау құралдары мен әдістері.					3
БАРЛЫҒЫ:	15		15	30	30

Зертханалық сабақтар тізімі

1. Қарапайым шифрлер. Алмастырып қою және орнына қою әдістері негізінде қарапайым криптографиялық алгоритмдерді талдау және әзірлеу

2. Файлдарды шифрлеу үшін қарапайым кестелік алмастыру әдісімен бағдарлама құру.

3. Ақпаратты қорғау жүйесінде псевдокездейсоқ сандар тізбегін генерациялау. Берілген ратату заңымен псевдокездейсоқ сандар статистикалық датчик сипаттамасын бағалау .

4. Криптография. Криптографиялық алгоритмді жүзеге асыру және әзірлеу. Алгоритм жұмысының жылдамдығын бағалау.

5. Diffie-Hellman алгоритм негізінде симметриялық кілтпен хаттама арқылы алмасуды бағдарламалық жүзеге асыру және әзірлеу.

6. Сандық дайджест хабарламасын есептеу алгоритмін бағдарламалық жүзеге асыру және әзірлеу
7. Сандық қол қоюдың алгоритмін бағдарламалық жүзеге асыру.
8. Аутентификациялаудың заманауи жүйелері
9. Желілік экранды баптау.
10. Парольдік аутентификация негізінде қолданушылардың құқықтары шектелген бағдарламаларды әзірлеу.
11. Қолданушылардың құқықтары шектелген және рұхсат етілмеген қолжеткізуден қорғау бағдарламалық құралдарды оқу.
12. Бағдарламалық қамтамасызданыдыруды рұхсат етілмеген қолданудан және көшіруден қорғау.
13. Ақпаратты қорғау үшін Windows криптографиялық интерфейс функциясын қолдану.

СӨЖ-ге арналған бақылау тапсырмаларының тақырыбы

1. Отладчиктер арқылы бағдарламаны зерттеу қарсы әрекет әдістері.
2. Жіберу арналары арқылы ақпараттық ресурстарды қорғау.
3. Мәліметтер қорында ақпаратты қорғау.
4. Мәліметтер қорындағы ақпаратты қорғау ерекшеліктері.
5. Web- технологияларда ақпаратты қорғау.
6. Виртуальды жеке желілерде қорғау.
7. Жылжыту регистріндегі псевдокездейсоқ сандар генераторы.
8. Ақпараттық ресурстарды бұзудан, түрлендіруден және көшіруден сақтау.
9. Бағдарламалық модельдеу және ақпараттық қауіпті болжау.
10. Электронды құжат айналым жүйелерінде қорғау құралдары мен әдістері.

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 тапсырмаларды орындау және тапсыру кестесі

Бақылау түрі	Тапсырманың мақсаты және мазмұны	Ұсынылатын әдебиет	Орындалу ұзақтылығы	Бақылау түрі	Тапсыру мерзімі	Баллы
1	2	3	4	5	6	7
Сабақтарға қатысу	Сабақтарға қатысуды бақылау		Семетр бойы	Ағымдағы	Апта сайын	1
СӨЖ бойынша есеп	«Отладчиктер арқылы бағдарламаны зерттеу қарсы	[1], [2], [3] [5]	2 апта	Ағымдағы	2 апта	1

беру	әрекет әдістері.» тақырыбы бойынша білімін тереңдету					
Зерт. жұм. қорғау №1	Қарапайым шифр- лер. Алмастырып қою және орнына қою әдістері негізін- де қарапайым крип- тографиялық алгоритмдерді талдау және әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	Ағымдағы	2 апта	2
Зерт. жұм. қорғау №2	Файлдарды шифрлеу үшін қарапайым кестелік алмастыру әдісімен бағдарлама құру.	[1], [2], [3], [5], [12],[11]	1 апта	Ағымдағы	3 апта	2
СӨЖ бойынша есеп беру	«Жіберу арналары арқылы ақпараттық ресурстарды қорғау» тақырыбы бойынша білімін тереңдету	[1], [2], [3] [5]	2 апта	Ағымдағы	3 апта	1
Зерт. жұм. қорғау №3	Ақпаратты қорғау жүйесінде псевдо- кездейсоқ сандар тізбегін генерация- лау. Берілген ратату заңымен псевдокез- дейсоқ сандар стати- стикалық датчик сипаттамасын бағалау .	[1], [2], [3], [5], [12],[11]	1 апта	Ағымдағы	4 апта	3
СӨЖ бойынша есеп беру	«Мәліметтер қорында ақпаратты қорғау» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [6],[10]	2 апта	Ағымдағы	5 апта	1
Зерт. жұм. қорғау №4	Криптография. Криптографиялық алгоритмді жүзеге асыру және әзірлеу. Алгоритм жұмысы- ның жылдамдығын бағалау.	[1], [2], [3], [5], [12],[11]	1 апта	Ағымдағы	5 апта	3
СӨЖ бойынша есеп беру	«Мәліметтер қорын- дағы ақпаратты қор- ғау ерекшеліктері» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [6],[10]	2 апта	Ағымдағы	6 апта	1
Зерт. жұм. қорғау №5	Diffie-Hellman алгоритм негізінде симметриялық кілт- пен хаттама арқылы	[1], [2], [3], [5], [12],[11]	1 апта	Ағымдағы	6 апта	3

	алмасуды бағдарламалық жүзеге асыру және әзірлеу.					
Жазбаша сұрау	Теориялық және практикалық білімдері бойынша алған білімдерін тексеру	[1-14] конспекты лекций	1 апта	аралық	7 апта	10
СӨЖ бойынша есеп беру	«Web- технологияларда ақпаратты қорғау» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [6],[10]	2 апта	ағымдағы	7 апта	1
Зерт. жұм. қорғау №6	Сандық дайджест хабарламасын есептеу алгоритмін бағдарламалық жүзеге асыру және әзірлеу	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	7 апта	2
Зерт. жұм. қорғау №7	Сандық қол қою алгоритмін бағдарламалық жүзеге асыру.	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	8 апта	3
СӨЖ бойынша есеп беру	«Виртуальды жеке желілерде қорғау.» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [10], [14],	2 апта	ағымдағы	9 апта	1
Зерт. жұм. қорғау №8	Аутентификациялаудың заманауи жүйелері.	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	9 апта	2
СӨЖ бойынша есеп беру	«Жылжыту регистріндегі псевдокездейсоқ сандар генераторы.» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [10],	2 апта	ағымдағы	10 апта	1
Зерт. жұм. қорғау №9	Желілік экрандарды баптау.	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	10 апта	2
Зерт. жұм. қорғау №10	Парольдік аутентификация негізінде қолданушылардың құқықтары шектелген бағдарламаларды әзірлеу.	[1], [2], [3], [5], [12],[11]	1 апта	ағымдағы	11 апта	2
СӨЖ бойынша есеп беру	«Ақпараттық ресурстарды бұзудан, түрлендіруден және көшіруден сақтау.» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	12 апта	1
Зерт. жұм. қорғау	Қолданушылардың құқықтары шектелген және рұхсат	[1], [2], [8]	1 апта	ағымдағы	12 апта	2

№11	етілмеген қолжеткізуден қорғау бағдарламалық құралдарды оқу.					
СӨЖ бойынша есеп беру	«Бағдарламалық модельдеу және ақпараттық қауіпті болжау» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	13 апта	1
Зерт. жұм. қорғау №12	Ақпараттық ресурстарды бұзудан, түрлендіруден және көшіруден сақтау	[1], [2], [3], [6],	1 апта	аралық	14 апта	2
СӨЖ бойынша есеп беру	«Электронды құжат айналым жүйелерінде қорғау құралдары мен әдістері» тақырыбы бойынша білімін тереңдету	[1], [2], [3], [5], [12],[11]	2 апта	ағымдағы	14 апта	1
Жазбаша сұрау	Теориялық және практикалық білімдері бойынша алған білімдерін тексеру	[1-14] конспекты лекций	1 апта	аралық	14 апта	10
Зерт. жұм. қорғау №13	Ақпаратты қорғау үшін Windows криптографиялық интерфейс функциясын қолдану.	[1], [2], [3], [5], [7],[14]	1 апта	ағымдағы	15 апта	1
Емтихан	Пәнді меңгеру деңгейін тексеру	[1-14] Негізгі және қосымша әдебиеттің жалпы тізімі	3 апта	Қорытынды	Сессия кезеңінде	40
Барлығы						100

Саясат және процедуралар

«Компьютерлік ақпаратты қорғау әдістері және құралдары» пәнін оқу барысында келесі ережелерді орындауы талап етеміз:

1. Сабаққа кешікпеу керек
2. Ескертусіз сабақты босатпау, егер ауырған жағдайда анықтама әкелу, басқа жағдайда түсініктеме жазу.
3. Босатқан сабақтарды тапсырмалар алып орындау.
4. Оқу үрдісіне белсенді түрде қатысу.
5. Жеке тапсырмаларды өз уақытында орындап және тапсыру керек.
6. Оқытушылармен және курстастарымен шыдамды, ашық-жарқын және кең пейілді болу керек.

Негізгі әдебиет тізімі

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: Учеб. Пособие. - М.: Академия, 2009. - 412 с.
2. Арутюнов В.В. Защита информации: Учебно-методическое пособие. - М.: Либерей-Бибинформ, 2010. - 56 с.
3. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие. - Владивосток: Изд-во ДВГТУ, 2010. - 318 с.
4. Бузов Г. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. - М.: Горячая Линия - Телеком, 2010, - 240 с.
5. Шаньгин В. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2010, - 544 с.
6. Шаньгин Ф. Комплексная защита информации в корпоративных системах. Учебное пособие. - М.: Форум, 2010, - 592 с.
7. Щербаков В., Ермаков С., Безопасность беспроводных сетей. Стандарт IEEE 802.11. - М.: РадиоСофт, 2010, - 256 с.
8. Хореев П.Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2007. 256 с.
9. Белов Е. Б. и др. Основы информационной безопасности: Учеб. пособие. М.: Горячая линия-Телеком, 2006. - 544 с.
10. Ярочкин В.И. Информационная безопасность: Учебник. - М.: Академический проект, Трикста, 2005. - 544 с.
11. Садердинов А.А. Информационная безопасность предприятия: Учеб. Пособие,- М.: Дашков и К, 2005. - 336 с.
12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. - М.: Горячая линия-Телеком, 2004. - 280 с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: ТРИУМФ, 2003. - 400 с.
14. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.

Қосымша әдебиет тізімі

1. Проскурин В.Г. Защита программ и данных. - М.: Академия, 2011, - 208 с.
2. Касперский К. Фундаментальные основы хакерства (искусство дизассемблирования). - М.: Солон-Р, 2008. - 288 с.
3. Яценко В.В. Введение в криптографию. Новые математические дисциплины. - М.: МЦНМО Питер, 2001. - 287 с.
4. Хорев А. А. Способы и средства защиты информации. Учеб. пособие. - М.: МОРФ, 2000.-316 с.
5. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-образ, 2001.- 363 с

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

КАКАК 3302 «Компьютерлік ақпаратты қорғау әдістері және құралдары» пәні

КАКАК 24 «Компьютерлік ақпаратты қорғау әдістері және құралдары» модулі

31.03.2004 берілген №50 мемлекеттік баспа лицензиясы

Басуға қол қойылды _____ Пішімі 60x90/16 Таралымы ___ дана. Есептік баспа
табағы _____ Тапсырыс _____ Бағасы келісімді.

100027, ҚарМТУ баспасы, Қарағанды, Бейбітшілік бульвары, 56