С.АМАНЖОЛОВ АТЫНДАҒЫ ШЫҒЫС ҚАЗАҚСТАН МЕМЛЕКЕТТІК УНИВЕРСИТЕТІ
ВОСТОЧНО-КАЗАХСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ С. АМАНЖОЛОВА

КЕЛІСІЛДІ / СОГЛАСОВАНО /
КГУ «Учебно-производственный комбинат» акимата г.Усть-Каменогорска /Өскемен қаласы әкімігінің «Оқу-өндірістік комбинаты» КММ /
Директор _____ Искаков Б.А
«_3_» ___06___ 2020 ж.

БЕКІТІЛДІ/УТВЕРЖДЕНО
Факультеттің кеңесі төрағасы/
Председатель совета факультета
_____ Мадияров М.Н.
Хаттама / Протокол
№ 10 «11» 06 2020ж/г

ПӘН БАҒДАРЛАМАСЫ (SYLLABUS)
ПРОГРАММА ДИСЦИПЛИНЫ (SYLLABUS)

Ақпаратты қорғаудың криптографиялық әдістері
Оқу пәнінің атауы/наименование учебной дисциплины

5В070300 –«Ақпараттық жүйелер»
(ББББ атауы және коды/код и название ОП)

Оқу түрі / Форма обучения / __*очное*_____
(күндізгі / очная, ОБ/СО)

Курс/Курс 4
Семестр/Семестр 7
Кредиттер саны/Количество кредитов в ECTS 5
Дәрістер/Лекции 20
Практикалық (семинар) сабақтар/
Практические (семинар) занятия -
Зертханалық сабақтар/
Лабораторные занятия -30
БОӨЖ / СРОП 25
БӨЖ / СРС 75
Емтихан / Экзамен 7 семестр

Өскемен, 2020 ж/г.

Құрастырушылар / Составители: Жантасова Ж.З.-т.ғ.к.,
КҮжАТкафедрасының меңгерушісі,
Қайдарова М.А.-педагогика
ғылымдарының магистрі, оқытушы

Пән бағдарламасы / Программа дисциплины (Syllabus)

Силлабус университет Академиялық кеңесі отырысында бекітілген оқу бағдарламасы негізінде жасалған / Силлабус разработан на основании учебной программы, утверждённой на заседании Академического совета университета
Хаттама / Протокол №_04__ «_21_» ___04__2020 ж./г. (*базалық және профильдік пәндер үшін / для базовых и профилирующих дисциплин*)

Кафедра отырысында ұсынылған / Рекомендована на заседании кафедры компьютерного моделирования и информационных технологий
Хаттама / Протокол № 10 «_03_» __06__2020 ж./г.

Кафедра меңгерушісі / Заведующий кафедрой_____Жантасова Ж.З.

1.Пән туралы ақпарат

Пәннің атауы Ақпаратты қорғаудың криптографиялық әдістері	Пәннің коды KMZI-4305	Кредит саны 7	Курс 4 Семестр 7
ББББ атауы Ақпараттық жүйелер	ББББ коды 5В070300	Кафедра КҮжАТ	Факультет ЖҒжТ
Пәнді өткізу уақыты және орны / Время и место проведения дисциплины *оқу кестесі бойынша № 7 корпус, ауд. 219*			
Кеңес беру уақыты – оқу кестесі бойынша			
Рейтинг кестесі: 7 және 15 апта			
Оқытушының аты-жөні Жантасова Ж.З., т.ғ.к., кафедра меңгерушісі, Қайдарова М.А., магистр, оқытушы	Байланыс ақпараты (телефон, e-mail) 8-777-263-90-16, zheniskul_z@mail.ru		

2. Пәннің қысқаша мазмұны:

Курстың қысқаша мазмұны. Ақпарат қорғаудың криптографиялық негіздері. Криптография ғылымының зерттейтін сұрақтары. Ақпаратты шифрлеу ережелері. Шифрлер классификациясы. Шифрлеу стандарттары. Симметриялық және ашық кілтті криптография. Криптотұрақтылық мәселелері. Криптографияның математикалық негіздері. Құпия хабарлама алмасу. Электрондық сандық қолтаңба.Криптографиялық жүйелердің цифрландыру есептерінде қолданылуы.

Мақсаты / Цель

«Ақпаратты қорғаудың криптографиялық әдістері» пәнінің мақсаты болып ақпаратты қорғау саласында зерттеушілік қабілеттіліктер криптографиялық әдістерін қарастыру негізінде қалыптастыру .

Міндеттері:

Пәнді оқу нәтижесіндегі студенттердің міндеттері:

1) Ақпаратты қорғаудың криптографиялық әдістерімен танысу;
2) Шифрлеу ережелерін меңгеріп, орындай алу;
3) Белгілі криптографиялық алгоритмдердің жұмысын меңгеру;
4) Криптографиялық алгоритмдердің криптотұрақтылық сұрақтарын талдау;
5) Ақпаратты шифрлеу үрдісінде мәтін алфавитін цифрландыру ережелерін үйрену;
6) Белгілі криптографиялық жүйелерде шифрлер жүйесінде құпия хабарламалар алмасу үрдісін ұйымдастыру;
7) Шағын жобалар даярлап қорғау.

Құзыреттіліктер

- Криптографиялық алгоритмді сипаттап беру;
- Шифрлеу белгілерді, жалпы қабылданған ережелерді ажырата алу;
- Криптографиялық жүйені ұйымдастыру кезеңдерін нақты қойылған есепке қолдана алады;
- Криптографиялық әдістер классификациясын талдай алу.

Оқыту нәтижелері

1) Шағын зерттеу тақырыбына жоспар жасап ізденіс жүргізе алу;
2) Әдебиеттерді қарап, интернет көздерінің деректерін тиімді іріктеп алу;
3) Криптографиялық алгоритмдердің мазмұнын қолданбалық аспектілерімен байланыстырып отыру;
4) Технологиялық және цифрленген экономика қоғамында кәсіби қызмет етуге дайындық.

3.Пререквизиттер

№	Пәндердің атауы, олардың бөлімдері (тақырыптары) / Название дисциплины, разделы (темы)
1	Ақпараттық коммуникациялық технологиялар
2	Алгоритмдер, деректер құрылымы және бағдарламалау

4.Постреквизиттер тізімі

№	Пәндердің атауы, олардың бөлімдері (тақырыптары) / Название дисциплины, разделы (темы)
1	Өндірістік тәжірибе
2	Дипломдық жұмыс

5. Күнтізбелік-тақырыптық жоспар / Календарно-тематический план

№	Пән тақырыптарының атауы	Апта	Сабақ түрі бойынша аудиториялық сағат саны		Сабақ түрі бойынша аудиториялық емес сағат саны		Барлығы (с.)
			Дәріс (с.)	Пр/сем./ зертх-қ./ студ (с.)	БОӨЖ (с)	БӨЖ (с)	
1	Ақпаратты қорғау мәселесі. Криптографияның даму тарихына шолу. Шифрлеу түсінігі	1	1	1	1	1	4
2	Ақпаратты қорғау аймағындағы қауіпсіздік стандарттар мен бағдарламалар. Криптографияны қолдану есептері	2	1	1	1	3	6
3	Криптографиялық жүйелер классификациясы. Дәстүрлі шифрлеу жүйелері. Ағымдық және блоктық жүйелер	3	1	1	1	1	4
4	Криптографиялық жүйелер классификациясы. Симметриялық және ашық кілтті криптография	3,4	2	1	2	3	8
5	Криптографияның математикалық негіздері. Қалдықтар класындағы есептеулер	4,5	1	1	2	1	5
6	Кері мәнді табу теоремасы. Салыстырмалар шешу әдістері	5,6	2	1	2	1	6
7	NP-есептерге кіріспе. Криптотұрақтылық сұрақтары	6,7	1	1	2	1	5
8	Ашық кілтті криптография. RSA алгоритмі бойынша хабар алмасу	7,8	2	3	2	3	10
9	Ортақ құпия үлестіру. Diffie-Hellman алгоритмі	9	2	2	2	3	9
10	Messey-Omura алгоритмі. Алгоритм осалдылығы	10	2	3	1	6	12
11	Электрондық сандық қолтаңба (ЭСҚ) жасау сызбасы. ЭСҚ қасиеттері	11	1	2	1	3	7
12	Базалық қорғау процедуралары. Аутентификация және криптография. Екікезеңді аутентификация.	11,12	1	2	1	3	7
13	Электрондық қызмет көрсету түрлері мен криптография	12,13	1	2	1	6	10

14	Криптография саласындағы зерттеу бағыттары. Жоба.	**13,14**	**1**	**3**	**1**	**6**	**11**
15	Шағын жобалар және нәтижелер	**15**	**1**	**6**	**5**	**34**	**46**
	Барлығы / Всего		**20**	**30**	**25**	**75**	**150**

6. Дәріс сабақтарының мазмұны

Тақырып 1. Ақпаратты қорғау мәселесі. Криптографияның даму тарихына шолу. Шифрлеу түсінігі

Тақырып бойынша қарастырылатын сұрақтар:

1. Криптография зерттейтін сұрақтар
2. Мәселе өзектілігі
3. Криптографияның негізін қалаған ғалымдар

Ақпаратты қорғау аймағы және ақпараттық қауіпсіздік информатикамен замандас және тез дамып келе жатқан бұтағы. Ақпараттың әртүрлі салада (коммерциялық, жеке және тағы басқа) электронды түрде жинақталуы оны қорғау мәселесін тудырады. Соған байланысты әлемде ақпаратты қорғау мәселесінің актуалдығын тудыратын обьективті процестер болып жатыр.Бұлар:

- Интернет және желілік технологияларды жиі қолдану;
- Қолданушылар санының өсуі;
- Ақпараттық технологияларды адам өмірінің әртүрлі салаларында үлкен көлемде қолдануы;
- Ақпаратты қорғау амалдарының жетіспеуі және шектеулігі;

Ақпаратты қорғау деп- ақпаратты жойылып кету қауіпінен сақтауға арналған нысаналы әрекет, құндылық ететін ақпаратқа бекітілмеген және әдейі емес әсер ету. Қауіпсіздік- қорғану күйі. Қауіпсіздікті жеткілікті деңгейде бағалаудың екі амалы болады:

1. Құндылық жақындығы қаскүнем ақпаратты алу жолында үлкен көлемде шығындалса, сонша ол ұтады деген көзқарасқа негізделген.
2. Уақыт жақындығы ақпаратты жою фактісіне негізделген.

Әдебиеттер: [1-2]

Тақырып 2. Ақпаратты қорғау аймағындағы қауіпсіздік стандарттар мен бағдарламалар. Криптографияны қолдану есептері

Тақырып бойынша қарастырылатын сұрақтар:

1) Дәстүрлі шифрлеу және шифрлеу стандарттары
2) DES, IDEA шифрлеу стандарттары
3) ГОСТ 28147-89
4) ҚР СТ 27001-2005

Шифрлеу принциптері, мемлекеттік шифрлеу стандарттары жасалу және бекітілу туралы деректер. DES стандартының шифрлеу сызбасы. Кілттер сипаттамасы.

Тұрғындарға қызмет көрсету орталықтары бір қатар электрондық қызмет көрсетуге жауаптанған. Олардың негізінде электрондық цифрлық қолтаңба (ЭЦҚ) жасап тұтынушыға беру қызметі де кіреді. ЭЦҚ комегімен көптеген сервистер-қызметтер алуға болады.

Қашықтан қызмет көрсетуде банктік жүйелерде екі кезеңді аутентификациялау немесе субъектінің қорғалған объектіге қатынауында шынайлылығын растау ұйымдастырылған.

Әдебиеттер: [3]

Тақырып 3. Криптографиялық жүйелер классификациясы.

Дәстүрлі шифрлеу жүйелері. Ағымдық және блоктық жүйелер

Тақырып бойынша қарастырылатын сұрақтар:

1) Цезарь жылжыту шифры.
2) Алмасу және ауыстыру шифрлері.
3) Аналитикалық өңдеулер

Классификация негізінде алынған ереже. Виженер, Уитстон, Трисемус, Полибий шифрлері. Сиқырлы шаршы негізінде шифрлеу күрделілігі. Вернам шифры. Хилл шифры.

Әдебиеттер: [3-4]

Тақырып 4. Криптографиялық жүйелер классификациясы. Симметриялық және ашық кілтті криптография

Тақырып бойынша қарастырылатын сұрақтар:

1. Заманауи шифрлердің классификациясы
2. Біркілтті және екікілтті жүйелер;
3. Криптотұрақтылық мәселелері. Кілттерді тарату, шифрлеу жылдамдығы;

Симметриялық пен симметриялық емес жүйелердің салыстырмасы. Ашық жабық кілт идеологиясы. Кілттерді тарату мәселесі және шифрлеу жылдамдығы параметрлері

Әдебиеттер: [1-4]

Тақырып 5.

Криптографияның математикалық негіздері. Қалдықтар класындағы есептеулер

Тақырып бойынша қарастырылатын сұрақтар:

1) Модуль бойынша есептеу.
2) Салыстырмаларды шешу.
3) Кері мәнді табу әдістері.

Қалдықтар класындағы есептеулердің ЭЕМ да орын алатын ерекшеліктері. Кері мәнду іздеуде салыстырмаларды шешу. Тура іріктеу әдісі. Эйлер функциясы көмегімен кері мәнді тауып алу. Кеңейтілген Евклид алгоритмі

$ax \equiv 1 \bmod n$ (1), салыстырымы берілсін.

Мұнда a, n- белгілі сандар. x: $x = a^{-1} \bmod n$ - табу қажет, мұндағы a^{-1} - a санының кері мағынасы. x- белгісізін үш жолмен табуға болады.

- Тура іріктеу әдісімен.
- Эйлер функциясы арқылы.
- Евклид алгоритмі арқылы.

Әдебиеттер: [3-5]

Тақырып 6. Кері мәнді табу теоремасы. Салыстырмалар шешу әдістері

Тақырып бойынша қарастырылатын сұрақтар:

1. Жабық кілттің бар болуы туралы теорема
2. Жабық кілт және шифрлеу –шифрден ашу үрдістері.
3. Ақпараттық қауіпсіздікті қамтамасыз етудің жеткілікті деңгейі
4. Есептеу күрделілілгі

Ең үлкен ортақ бөлгіш түсінігі. Өзара жай сандардың қасиеттері. Ашық кілтті криптография және ашық-жабық кілт түсініктері.

RSA алгоритмі 1978 жылы өзінің жасаушылары: R. Rivest, A. Shamir и L. Adleman есімдерімен аталып жарияланған. Бұл қазіргі заманда ең кең тараған ашық кілті бар криптожүйе. Бұл алгоритм тар жолды біржақты функцияны қолдануға негіздеоген (trapdoor one-way function). 2 қарапайым P,Q сандарын біліп, оларды көбейту арқылы N=P*Q теңдеуін алу өте оңай, ал оны N- қарапайым санға бөлу «лазейка (тар жол)» деп аталады. N-ді P мен Q-ға бөлу мүмкін емес, егер P мен Q ұзындығы 100 ондық белгілерден тұрса. 1994 жылы 8 айдың ішінде 1600 компьютерлік желілерде 129 ондық цифрдан тұратын сан табылды (А.Мистра, М.Манасси математигімен). Осы мысалдан криптотұрақтылық туралы ой қозғауға болады

Әдебиеттер: [1,3-4]

Тақырып 7. NP-есептерге кіріспе. Криптотұрақтылық сұрақтары

Тақырып бойынша қарастырылатын сұрақтар:

1) Криптотұрақтылық мәселесі
2) NP есептер түсінігі

3) Ашық кілтті криптография негізінде алынған NP есептері

Қиын- шешілетін математикалық есептер. Адам өміріне компьютерлік технолгиялардың енуі, криптографиялық жүйелердің өзгеруіне әкелді. 1976 жылға дейін шифрлеу және шифрден шығару кілттері жасырын түрде болатын симметриялы жүйелер қарастырылған. Криптографияда жаңа ағым болған дешифрлеу кілті жасырын болатын ашық кілті бар жаңа жүйе пайда болды. Өзінің жасаушыларының есімімен аталған R.L.Rivest, A.Shamir, L.M. Adleman. W.Diffie и M.E.Hellman RSA криптожүйесі 1978 жылы танымал болған жасырын кілтті бөлу сұлбасы жасап шығарылды. Ашық кілтті қолдану жүйесін ендірген және қолданудың беріктасының негізі болып математика танылады, ол құрылымын және келетін функцияны анализдеуді қамтамасыз етеді. Осы қиын-шешілетін математикалық есептер, ашық кілтті криптожүйенің нәтижелі болуын қамтамасыз етеді. Үлкен натурал сандарды қолданатын N=P*Q, мұнда P,Q- үлкен қарапайым сандар болатын RSA алгоритмі де осындай негізде болады. P,Q- қарапайым натурал сандарды құрастыру өте қиын. RSA шифрлеу алгоритмінің негізінде $f(x)=x^e \bmod n$ біржақты функциясы жатыр. Егер $\mathbf{y= x^e \bmod n,}$ e-ашық кілтінің мағынасы белгілі болса, n- модуль болса, онда біз d: $y^d=x^{ed=1} \bmod n=x$ дешифрлеу кілтін білмесек x-ті қалпына келтіру қиын.

Diffie и Hellmana сұлбасындағы $f(x)=g^x$, $f: P^* \to P^*$ (P- соңсы аймақ, g- қолданылу элементі) функциясы қарастырылады. Егер $\mathbf{g^x=f}$,болса онда **x-** g ге негізделеді. f, g-дің негізі. x-ті f және g арқылы табу дискретті алгоритм мәселесі деп танылған және шығымы қиын болып табылады.

Әдебиеттер: [3]

Тақырып 8. Ашық кілтті криптография. RSA алгоритмі бойынша хабар алмасу

Тақырып бойынша қарастырылатын сұрақтар:

1. Алгоритм кезеңдері. Құпия хабар алмасу
2. Аутентификациялау мәселесі

N=P*Q натурал сандарын аламыз, мұнда P,Q- қарапайым сандар.

Кілт генерациясын қарастырайық. RSA алгоритмінде екі кілт қолданылады.

- e- ашық кілт;
- d-жабық, жасырын кілт;

e ашық кілті келесі шарттардан таңдалады:

$$НОД(e, \varphi(N)) \equiv 1$$

Мұнда $\varphi(N)$ - Эйлер функциясы.

d- жасырын кілті келесі теңдік бойынша мына формуламен анықталады:

$$e \cdot d = 1 \bmod \varphi(N)$$

Криптографиялық жүйені жасырын ақпаратты алушы құрастырады, былайша айтқандакілттің генерациясын орындайды және жариялайды (e,N).

Осылайша (e,N)- ашық ақпарат, (d,P,Q)- жасырын ақпарат

Шифрлеу және шифрден шығару келесі сұлба бойынша жүргізіледі.

- pt бастапқы мәтінін цифрлеу;
- шифрлеу келесі формула бойынша жүргізіледі:

$$pt^e \bmod N = ct$$

Іс- әрекет жіберушімен орындалады.

- Шифрден шығару келесі формула бойынша жүргізіледі:

$$ct^d \bmod N = (pt^e)^{d \bmod \varphi(N)} = pt$$

Іс- әрекет ақпаратты алушымен жүргізіледі.

Мысал1: $pt = YES$

1. $p = 11, q = 3 \Rightarrow N = 33$
   $\varphi(33) = 20 \Rightarrow E = 7$
   $7 \cdot D = 1 \bmod 20 \Rightarrow D = 3$

2. $YES \leftrightarrow 24 \quad 4 \quad 18$

$$\left.\begin{array}{l} 24^7 \bmod 33 = 18 \rightarrow S \\ 4^7 \bmod 33 = 16 \rightarrow Q \\ 18^7 \bmod 33 = 6 \rightarrow G \end{array}\right\} \Rightarrow ct = SQG$$

3. $SQG \leftrightarrow 18 \quad 16 \quad 6$

$$\left.\begin{array}{l} 18^3 \bmod 33 = 24 \rightarrow Y \\ 16^3 \bmod 33 = 4 \rightarrow E \\ 6^3 \bmod 33 = 18 \rightarrow S \end{array}\right\} \Rightarrow pt = YES$$

Әдебиеттер: [8-13]

Тақырып 9. Ортақ құпия үлестіру. Diffie-Hellman алгоритмі

Тақырып бойынша қарастырылатын сұрақтар:

1. Ортақ құпия қажеттілігі
2. Дискретті логарифм мәселесі
3. Алгоритм негізінде құпия хабар алмасу

Diffie-Hellman алгоритмі. Z_p-айрымдар сақинасы, p- жай сан

$Z_p = \{0,1,2,\ldots, , p-1\}$ кері элементтері бар тобын қарастырамыз

Дискретті логарифм ұғымы. Дана Z_p- мультипликативті топ , q-туындайтын элемент =>

$\forall f \in Z_p^*$

$f=q^R, 1 \le R \le p-1$

R дискретті логарифм $R=\log_g f$

R мәнін табу күрделі есептеу мәселесі болып келеді

Жалпы түрде $q^x=f \quad x-?$

q-берілген мәнді өзгерте есептейміз f, $f_1=q^{x1}$ $f_2=q^{x2}$

Бұл мәселе құпия кілттер қалыптастыруға қолданылып тарихта Diffie-Hellman хаттамасы(1976) деп аталған.

2 хабар алмасушы абоненттер $A \leftrightarrow B$

1. 2 абонент Z^*_P туралы келісімге келеді q→туындайтын элемент
2. A а құпия санын таңдап B абонентіне жібереді $Z^*_P \rightarrow B.q^a$
3. B дәл солай $Z^*_P \rightarrow A\ q^b$ b- B абонентінің құпия саны
4. B : q^{ab}-есептейді
5. A : q^{ba}-есептейді

Қастандық жасаушы тек қана q^a, q^b мәндерін көре алады, ал q^{ab}, q^{ba} мәндері оған белгісіз

Мысал:

1. $Z^*_7, q=3$
2. A: $a=4 \rightarrow B\ q^a=3^4 \bmod 7 = 4$
3. B: $b=2 \rightarrow A\ q^b=3^2 \bmod 7=2$
4. B : $q^{ab}=(3^4)^2 \bmod 7=4^2 \bmod 7=2$ жалпы құпиялы сан =2
5. A: $q^{ba}=(3^2)^4 \bmod 7=(2)^4 \bmod 7=2$

Әдебиеттер: [8-13]

Тақырып 10. Messey-Omura алгоритмі. Алгоритм осалдылығы

x- ашық мәтін

x тиісті Z_r, g- тудыратын элемент

x- цифрленген күй

A, B- екі элемент

A абонентінің әрекеті:

A: a құпия сан ойлайды(кілт) және $x^* g^a$ есептейді де B абонентіне жібереді

B: в құпия сан ойлайды және өзінің құлпын жабады да A- ға жібереді

$(x^*g^a)^*g^в \rightarrow A$

А: өз құлпын кілтпен ашады

$(x*g^a)* g^в*g^a \rightarrow x* g^в \rightarrow В$

В: өз кілтімен ашады

$(x* g^в)* g^{-в} =x$

Қарастырылған алгоритм сызбасында хабарлама жіберу арнасына еніп өзін құқықты абонент ретінде жариялап ортақ құпияға қол жеткізуге мүмкіншілік алгоритмнің осалдылығын көрсетеді.

Massey Omura алгоритміне

1-мысал:

Z_7^*, g=3, x=6

1) А: a=4 $6*3^4 \bmod 7 = 6*(3^2)^2 \bmod 7=6*9^2 \bmod 7=6*81 \bmod 7=6*4 \bmod 7=$
$=24 \bmod 7=3 \rightarrow Б$
2) Б: b=5 $3*3^5 \bmod 7=3*(3^2)^2*3 \bmod 7=9*9^2 \bmod 7=9*81 \bmod 7=$
$=9*4 \bmod 7=36 \bmod 7=1 \rightarrow А$
3) А: $1*3^{-4} \bmod 7=1*5^4 \bmod 7= (5^2)^2 \bmod 7 =25^2 \bmod 7=$
$=4^2 \bmod 7=16 \bmod 7=2$
4) Б: $2*3^{-5} \bmod 7=2*5^5 \bmod 7=2*(5^2)^2*5 \bmod 7=10*25^2 \bmod 7=3*4^2 \bmod 7=$
$=3*16 \bmod 7=3*2 \bmod 7=6$

$3^{-4}=3^{-1} \bmod 7$

$3x=1 \bmod 7$

X=5

Әдебиеттер: [8-13]

Тақырып 11. Электрондық сандық қолтаңба (ЭСҚ) жасау сызбасы. ЭСҚ қасиеттері

Тақырып бойынша қарастырылатын сұрақтар:

1. Электрондық қолтаңба функциялары

Электронды цифрлық қолтаңбаны арнайы мойындау қажеттігі келесі екі мәселеге байланысты болды. Бір жағынан электронды құжаттың өспелі ағымы, екінші жағынан қорғаудың жоғарғы деңгейі қамтылған электронды цифрлік қолтаңба алгоритмінің пайда болуы (яғни, жалған түрлі жасауға мүмкіндік береді). Электронды цифрлық қолтаңбаның электронды құжаттарды безендіру тәжірбиесіне өткен 100 жылдықтың 80 жылдарында ене бастауына қарамастан көпшілік оның не екенін дұрыс түсіне бермейді. Ең алдымен электронды цифрлық қолтаңбаның қандай мақсатта қолданылатынын анықтап алу қажет (кез келген қолтаңба қарапайым және электронды).Ең кем дегенде 3 функция атқарады:

1. *Авторизациялау* функциясы – қолтаңба иесінің нақты біз білетін адам екенін дәлелдейді.
2. *Бастартпаушылық* – құжатқа қол қоюшының сол құжатттан бас тартпайтынын қамтамассыз етеді.
3. *Құжатты* аутентификациялау – жіберушінің нақты жіберген қол қоюы.

Бастапқы екі функция адресаттың (құжат алушы) қауіпсіздігін қамтамассыз етеді. Ал, үшінші функция корреспонденттің (қолтаңба қоюшы) ойындағысын қамтамассыз етеді. Барлық жағдайда қолтаңбаның *аутентикалық* қасиеті байқалады. Қолтаңбаның аутентикалық қасиеті бүкіл құжатқа толыңымен беріледі.

Электронды цифрлық қолтаңба келесі кезеңдерден тұрады:

- Х корреспонденті У адресатқа жіберуге арналған құжатты арнайы алгоритммен өңдейді. Бұл алгоритмді қолдану нәтижесінде құжатты толығымен сипаттайтын интегралды параметрлер алынады. Алынған параметрлердің жад көлемі барлық құжаттардың көлемінен неғұрлым кішірек болады.
- Бұдан кейін Х корреспондент құпия кілт көмегімен алынған параметрлерді шифрлейді. Осы жолмен шифр Х корреспонденттің Электронды цифрлық қолтаңбасы болып табылады.
- Х корреспондент У адресатқа құжатты және өзінің электронды цифрлі қолтаңбасын жібереді.
- У адресат алынған құжатқа Х корррреспондент қолданған алгоритмді қолданады.

- Бұдан кейін У,Х корреспонденттен алынған ашық кілтті пайдаланып электронды цифрлық қолтаңбаны дешифрлейді.
- Ең соңында У төртінші қадамда алынған параметр мәнін шифрден ашылған электронды цифрлық мәнімен салыстырады. Егер бұл мәндер сәйкес келсе онда қолтаңба жалған емес және құжат берілу кезінде өзгертілмеген болып табылады. Кері жағдайда – құжат оқылған және қолтаңба жалған дегенді білдіреді. Электронды цифрлық қолтаңбаны қолдану жіберілетін құжаттың толығымен шифрленуін қажет етпейді.

Электронды цифрлық қолтаңба – электронды құжаттың шынайлылығын растайтын алгоритм.

Электронды цифрлық қолтаңбаның екі түрі болады.

1) қосарланған (pt-1 файл, электронды цифрлық қолтаңба-1файл)
2) туындайтын (pt, электронды цифрлық қолтаңба-1 файл)

Әдебиеттер: [5-7]

Тақырып 12. Базалық қорғау процедуралары. Аутентификация және криптография. Екікезеңді аутентификация.

Тақырып бойынша қарастырылатын сұрақтар:

1. Ақпаратқа қатынауды шектеу үлгілері
2. Базалық қорғау процедуралары
2. Банк жүйелеріндегі екікезеңдік аутентификация

Заманауи компьютерлік жүйелерде электронды түрде жасалып, өңделіп сақталатын ақпараттық ағымдардың көлемі, оларды пайдаланатын қолданушылардың саны өсуіне байланысты, ақпараттың тұтастығын, қол жеткізу тиімділігін және де конфиденциалдық қажеттілігін қамтамасыз ету мақсатымен қатынауға шектеу қойылады. Шектеу қоюдың тәртібі қандай, операциялық жүйе, ақпараттық жүйе болсын жасалатын жұмыстар, орындалатын ережелер қандай, нәтижесінде қамтитін қауіпсіздік деңгей қандай? Осы сұрақтарға жауап іздеп көрейік.

Анықтама. Ақпаратқа қатынау үлгісі - жүйенің қауіпсіздігін қамтамасыз ететін, ақпаратқа, ақпарат ағымдарына қатынауды басқаратын ережелер жиынтығы. Негізгі болып дискреционды, өкілетті және рөльдік басқару үлгілері есептеледі (Сурет 1). Олардан қолдану аймақтары нақтыланып пайда болған Биба тұтастық, домендік типтер, Қытай қабырғасы, Кларк-Вильсон, Сазерленд үлгілерін де атап кетуге болады

Екі кезеңді аутентификация (Two-Step Verification, **2SV**). Жүйеге кіруге рұқсат екі қадам негізінде беріледі: ең алдымен тіркелген жазбаға кіру үшін пароль енгізу, сосын SMS арқылы жіберілген код енгізу.

Әдебиеттер: [5-7]

Тақырып 13. Электрондық қызмет көрсету түрлері мен криптография

Негізгі сұрақтар:

1. Электрондық қызмет көрсету түрлері
2. Криптографиялық жүйелер және электрондық қызмет көрсету
3. Электрондық сандық қолтаңба негізінде алынатын криптографиялық алгоритмдер

Әдебиеттер: [5-13]

Тақырып 14. Криптография саласындағы зерттеу бағыттары. Жоба.

Шешілмеген мәселелер. Кванттық криптография, Эллипстік криптография.Атрибуттық қатынауды бақылау. Бұлттық есептеулерді қорғау. Жоба құрылымы мен мазмұны.

Әдебиеттер: [6]

Тақырып 15. Шағын жобалар және нәтижелер

Шағын жобалық қызмет. Зерттеушілік реферат. Программалық өнім. Оқушының технологиялық және цифрлық экономика қоғамында қауіпсіз өмір сүру дайындығы.

Әдебиеттер: [2-5]

7. Практикалық (семинарлық) сабақтар

Тақырып 1.

1. Пәннің әдебиеттер көздерімен қамтылу кестесін толтыру

Тапсырмаларды орындауға әдістемелік нұсқаулар: Кесте үлгісі берілген. Әдебиеттер көздері университет кітапханасынан іздестіріледі. Басылымнан шыққан жылдары- соңғы 5 жыл. Интернет көздері іздестірілген жағдайда .pdf форматтағы оқу құралдың нұсқасын көрсету қажет *(Практикалық жұмыс 1)*

Әдебиеттер:[1-5]

Тақырып 2.

1. Дәстүрлі шифрлеу жүйелерінде ақпаратты шифрлеу *(Практикалық жұмыс 2)*

Әдебиеттер:[5]

Тақырып 3.

Шифрлеу стандарттарының жалпы сипаттамасын беру *(Практикалық жұмыс 3)*

Әдебиеттер:[6-13]

Тақырып 4.

Симметриялық және ашық кілтті криптографиялық алгоритмдерге салыстырмалы сипаттама беру. Ерікті формада.

Әдебиеттер:[1]

Тақырып 5.

Қалдықтар класындағы есептеулерді жасау. Қалдықтар класындағы есептеулердің артықшылықтары. Тура іріктеу әдісімен кері мәнді табу *(Практикалық жұмыс 4)*

Әдебиеттер:[3-4]

Тақырып 6.

Эйлер функциясы көмегімен кері мәнді табу *(Практикалық жұмыс 4)*

Тақырып 7.

Кеңейтілген Евклид алгоритмі негізінде кері мәнді табу. «Кері мән» мен құпиялы кілт арасында аналогия жүргізу. *(Практикалық жұмыс 4)*

Әдебиеттер:[6-13]

Тақырып 8.

1. RSA ашық кілтті криптожүйені қолдану арқылы құпия хабарлама алмасу. *(Практикалық жұмыс 5)*

Әдебиеттер:[3]

Тақырып 9.

1. DH жүйесінде ортақ құпия жасау. *(Практикалық жұмыс 6)*

Әдебиеттер:[6-13]

Тақырып 10.

Massey –Omura алгоритміне мысал құрастыру

Әдебиеттер:[1-5]

Тақырып 11.

Электрондық сандық қолтаңба жасау және тексеру сызбаларын құру

Әдебиеттер:[2]

Тақырып 12.
Аутентификация түрлеріне сипаттама беру
Әдебиеттер: [15]

Тақырып 13.
Электрондық үкімет порталындағы электрондық қызметтер классификациясын жасау
Әдебиеттер: [2,3]

Тақырып 14.
Ұсынылған тақырыптардан таңдау жүргізіп жоба сипаттамасын жасау. *(Практикалық жұмыс 7)*
Әдебиеттер: [1-5]

Тақырып 15.
Жобаның презентациясын әзірлеп қорғау. *(Практикалық жұмыс 7)*
Әдебиеттер: [1, 4-7]

Тапсырманы орындау бойынша әдістемелік нұсқау (қысқаша):

Практикалық жұмыстарда келесі мүмкіндіктер қарастырамыз:

1) Кітапханалардан, интернет желісінен әдебиеттерді жинақтаймыз, соңғы 5 жылдық аралығында шыққан әдебиеттерді кестеде берілген талаптарға сәйкес толтырамыз (Практ. жұм №1);
2) Дәстүрлі шифрлеу жүйелерінде жұмыс жасау; (Практ. жұм №2);
3) Шифрлеу стандарттарына сипаттама беру. Сипаттама критерийлері кесте түрінде берілген (Практ.жұм №3);
4) Қалдықтар класындағы есептеулерді жасау. Салыстырмалар шешу. Есептерге нұсқаулықтар, шығару жолдары берілген (Практ. жұм №4)
5) RSA ашық кілтті криптожүйені қолдану арқылы құпия хабарлама алмасу. (Практ. жұм №5)
6) DH жүйесінде ортақ құпия жасау. (Практ. жұм №6)
7) Криптожүйелерді қолдану есептерін айқындау. Жобалық жұмыс жасау Жұмысты қорғау.(Практикалық жұмыс №7)

8. БӨЖ мен БОӨЖ бойынша тапсырма

№	Тақырып атауы	БӨЖ мен БОӨЖ тапсырмаларының мазмұны	Бақылау түрі	Тапсыру мерзімі
1 тақырып	АҚ өзектілігі	Қазіргі АҚ жағдайын талдау	Өзектілік негіздемесі	1 апта
2 тақырып	Ақпаратты қорғау мәселесі	Криптография туралы бейне материалдар жинақтау, көру	Бейнематериалдар тізімі	2 апта
3 тақырып	Криптографиялық жүйелер классификациясы	Шифрлеу түрлерін сипаттау	Баяндама (3 мин)	3 апта
4 тақырып	Криптографияның математикалық негіздері	Практикалық дағдылар қалыптастыру	Есеп шығару	4 апта
5 тақырып	Тура іріктеу әдісі. Эйлер функциясы көмегімен кері мәнді табу	Есептер шығару	Толық шығарылған есептер (3-5 есеп әр әдіске)	5 апта

6 тақырып	Кеңейтілген Евклид алгоритмі	Есептер шығару	Толық шығарылған есептер (3-5 есеп әр әдіске)	6 апта
7 тақырып	NP-есептер	NP-есептерге 2-3 мысал келтіру, түсініктеме беру	2-3 мысал	7 апта
8 тақырып	RSA алгоритміндегі аутентификация мәселесі	Аутентификация мәселесін сипаттап беру	сипаттама	8 апта
9 тақырып	DH алгоритміндегі ортақ құпия мәніне талаптар	Талаптарға сәйкес ортақ құпия құрастыру	мысал	9 апта
10 тақырып	Ашық кілтті криптография	Месси Омура алгоритмінің сызбасын жасап, құпия хабар алмасу	Мысал құрастыру	10 апта
11 тақырып				11 апта
12 тақырып	Аутентификация түрлері	Аутентификация сызбалары	Сызба	12 апта
13 тақырып	Криптографияның қолдану есептері	Эль Гамаль электрондық цифрлық қолтаңба алгоритмін орындау Ақпаратқа қатынауды шектеу үлгілері	1. Алгоритм қадамдарын сипаттау 2. үлгілер туралы мәлімет беру	13 апта
14 тақырып	Жоба таңдау	Жобаның сипаттамасын беру	Жоба сипаттамасы	14 апта
15 тақырып	Жоба тақырыбы	Жобаны даярлау	Жоба қорғау	15 апта

Барлық сұрақтар бойынша кеңес беру - кестеге сәйкес

9. Ұпай қою саясаты

Кредиттік технология жағдайында оқу процесін ұйымдастыру элементтерінің бірі білім алушылардың оқу жетістіктерін бағалаудың балдық-рейтингтік жүйесін қолдану болып табылады. Ұпай қою саясаты объективтілік, ашықтық, икемділік және жоғары саралаушылық принциптеріне негізделеді.

Пәнді оқыту барлық өтілген материалды қамтитын, әртүрлі формада (жазбаша немесе ауысша емтихан, тестілеу) емтихан қабылдаумен аяқталады. Емтихан тапсыруға рұқсат алудың негізгі шарты – бағдарлама бойынша барлық тапсырмаларды орындау.

Әр тапсырма 0-100 баллмен бағаланады.

№	**Жұмыс түрі**	Бір тапсырмаға қойылатын баға (max балл)	Тапсырма саны	Жиынтық баға
Рейтинг 1				
1.	Ақпаратты қорғаудың криптографиялық әдістері аймағындағы әдебиет көздерін іздестіру, жүйелеу	100	1	100
2.	Дәстүрлі шифрлеу жүйелерімен танысу, тапсырмаларды орындау	100	1	100

3.	Шифрлеу стандарттарының жалпы сипаттамасын беру	100	1	100
4.	Симметриялық және ашық кілтті криптожүйелердің салыстырмалы талдауын жасау	100	1	100
			Барлығы	100
Рейтинг 2				
1.	Қалдықтар класындағы есептеулер жүргізу	25	4	100
2.	RSA ашық кілтті криптожүйені қолдану арқылы құпия хабарлама алмасу	100	1	100
3.	DH жүйесінде ортақ құпия жасау	100	1	100
4.	Жоба құрылымы мен сипаттамасы	100	1	100
5.	Жоба даярлап қорғау	100	1	100
			Барлығы	100

Емтиханға жіберу рейтингісінің бағасы академиялық кезең бойынша алынған барлық ағымдық және аралық бақылаулар бағасы қосындысының орташа арифметикалық мәні болып табылады:

$$ЖР = (АБ_1 + АБ_2 + АБ_3 + \ldots. + АБ_n + АрБ_1 + АрБ_2) / (n+2),$$

мұндағы ЖБ –емтиханға жіберу рейтингісі; АБ – ағымдық бақылау; АрБ – аралық бақылау; n – ағымдық бақылаулар саны; 2 – аралық бақылаулар саны.

Пән бойынша қорытынды бақылауға пән бағдарламасының барлық талаптарын орындаған (барлық практикалық (семинарлық, зертханалық) жұмыстарды және БОӨЖ, БӨЖ бойынша тапсырмаларды орындаған және тапсырған), емтиханға жіберу рейтингісін (50 баллдан кем емес) жинаған білім алушы жіберіледі. Пән бойынша емтиханға жіберу рейтингісі оң баға болмаса (50 баллдан кем емес) білім алушы емтиханға жіберілмейді.

Пән бойынша қорытынды баға автоматты түрде төмендегі формула бойынша есептеледі:

$$Қ = (Р_1+Р_2)/2*0,6+емтихан\ бағасы*0,4,$$

мұндағы $Р_1$ – бірінші аралық бақылау бағасы; $Р_2$ – екінші аралық бақылау бағасы.

Пән бойынша қорытынды баға білім алушы тек емтиханға жіберу рейтингісі бойынша да, қорытынды бақылау бойынша да оң баға (50 баллдан кем емес) алған жағдайда есептеледі. Қандай да бір дәлелді немесе дәлелсіз себептермен қорытынды бақылауға келмеген жағдайда «Емтихан бағасы» бағанасына «0» (нөл) қойылады. Пән бойынша аралық аттестация нәтижелері білім алушыға сол күні хабарланады.

Білім алушылардың оқу жетістіктерін бағалаудың төрт баллдық жүйе бойынша сандық эквивалентке сәйкес әріптік жүйесі

Әріптік жүйе бойынша бағалар	Баллдардың сандық эквиваленті	Баллдар (%-тік құрамы)	Дәстүрлі жүйе бойынша бағалар
A	4,0	95-100	Өте жақсы
A-	3,67	90-94	
B+	3,33	85-89	Жақсы
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	Қанағаттанарлық
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	

10. Оқытушы талабы, саясаты мен тәртібі

Студенттердің оқу жетістіктерін бағалау саясаты академиялық адалдық, талаптардың бірлігі, объективтілік пен адалдық, ашықтық және ашықтық принциптеріне негізделген.

Бірінші сабақта мұғалім студенттерге пәннің жұмыс оқу жоспары (силлабусы), академиялық пәннің жоспарланған оқу нәтижелері және оларды бағалау тәртібі туралы таныстырады.

Академиялық әділетсіздік байқалған жағдайда ЖОО білім алушылары тарапынан:

- аудиториядағы және аудиториядан тыс сабақтар кезінде: бірінші жол берілген тәртіп бұзғаннан кейін құрылған комиссия білім алушылармен әңгімелесу өткізеді; актіде шығарылған ескерту және қабылданатын шара (бағаланатын жұмыс үшін бағаны төмендету; білім алушының жазбаша жұмысын жою, бақылау іс-шарасын қайта өткізуге ұсыныс және т.б.) тіркеледі. Академиялық адалдық фактілеріне қайта жол берілген жағдайда оқу жылы ішінде қайта комиссия құрылады, акт жасалады және одан әрі шешімдер қабылдау үшін тәртіптік-сыбайлас жемқорлыққа қарсы кеңеске (бұдан әрі – ТСЖҚК) беріледі;

- аралық немесе қорытынды аттестаттау кезінде: Академиялық әділетсіздік көрсеткен білім алушы сол академиялық кезеңде емтиханды қайта тапсыру құқығынсыз аудиториядан шығарылады. Бұл ретте емтихан ведомосына «Академиялық әділетсіздік танытқаны үшін емтиханнан алынды» деген жазба жазылады, оның түрі көрсетіледі. Емтиханды қайта тапсыру жазғы семестрде немесе келесі академиялық семестрде ақылы негізде жүзеге асырылады. Бұл ретте білім алушы осы оқу пәніне қайта жазылады, оқу сабақтарының барлық түрлеріне қатысады, жұмыс оқу бағдарламасына сәйкес оқу жұмысының барлық түрлерін орындайды және емтихан тапсырады. Емтиханнан қайта шығарылған жағдайда (ЖОО-да оқудың барлық кезеңі ішінде) білім алушы ШҚМУ-ға қайта қабылдану құқығынсыз оқудан шығарылады.

Білім алушының барлық аудиториялық сабақтарға кешікпей, сабаққа қатысуы міндетті болып табылады. Сабақтан қалған жағдайда деканатта тағайындалған тәртіппен өтелінеді.

Берілген курстың білім алушылар контингентіне кірмейтін бөгде адамдардың дәріске қатысуына тыйым салынады.

Жұмысты көрсетілген мерзімде тапсыру қажет. Барлық тапсырмаларды тапсырудың соңғы мерзімі емтихан сессиясына 5 күн қалғанға дейін беріледі.

Әрбір оқу сабағы бойынша тақырыпты қайталау мен өтілген материалды өтеу міндетті. Оқу материалының меңгерілу дәрежесі жазбаша жұмыстармен немесе тестпен тексеріледі білім алушыларды тестілеу ескертусіз жүргізілуі мүмкін.

Білім алушының оқытушымен өзіндік жұмысын (БОӨЖ) орындау кезінде келесі негізгі функциялар ескеріледі:

- бірінші – оқу пәні бойынша бағыттау-бағдарлау сабақтары кезінде оқытушы берген ақпаратты студенттердің белсенді қабылдауын іске асыруды көздейді;

- екінші - оқытушының ұсынымы негізінде студенттердің өздігінен оқу-әдістемелік құралдарды, әдебиеттерді оқуын, үй тапсырмаларын, бақылау, курстық жұмыстарды және т.б. орындауын көздейді.

Бұл кезеңде студенттерден жұмыс істеудің әдіс-тәсілдерін білу, қиындықтарды анықтау, өзін-өзі ұйымдастыру және өзіндік тәртіп талап етіледі;

- Білім алушының үшінші функциясы – өздерінде қиындық тудырған жағдайларды талдау мен жүйелеу, оқу материалын түсіну мен меңгерудегі қиындықтар себебін анықтау, басқа оқу әрекетін орындау.

Білім алушы шешімі табылмаған қиыншылықтарды оқытушыларға арналған сұрақтар жүйесіне айналдырады (оларды саралайды, реттейді, ресімдейді), бұл сұрақтарға өз жауаптарының нұсқаларын дайындайды;

- Білім алушының төртінші функциясы түсініктеме, ақыл-кеңес, консультация алу үшін оқытушымен сұхбаттасуын білдіреді.

11. Емтихан сұрақтары

1) Курстың жалпы мазмұны. Ақпаратты қорғау мәселесінің өзектілігі. Криптографияға кіріспе
2) Киберқалқан бағдарламасының мазмұны
3) Компьютерлік инциденттерге жауап беру қызметі (KZ-CERT). Кибершабуылдарды талдау және тергеу жүргізу орталығы қызметі
4) Шифрлеу жүйелерінің даму тарихынан деректер
5) К.Шеннон еңбектері мен криптографияға қосқан үлесі
6) Криптографиялық жүйелерді классификациялау белгілері
7) Криптографияның математикалық негіздері. Қалдықтар класындағы есептеулер
8) Кері мәні туралы теорема. Қалдықтар туралы қытай теоремасы (Сунь Це теоремасы).
9) Кері шамаларды есептеу. Тура іріктеу әдісі
10) Кері шамаларды есептеу. Эйлер әдісі
11) Эйлер функциясының мағынасы және криптографияда қолдануы
12) Кеңейтілген Евклид алгоритмі
13) Идентификация, аутентификация және авторизация процедуралары
14) Шифрлеу жүйелерінің жіктелуі (Симметр- Ассимметр)
15) Ағымдық алмастыру шифрлері (Мысал келтіру)

16) Цезарь шифры. Шифрлеу бағдарламасын жазу
17) Блоктық шифрлер сипаттамасы. Сиқырлы шаршылар негізінде шифрлеу
18) Виженер, Уитстон, Полибий, Трисемус шифрлері
19) Аналитикалық өңдеулер. Хилл шифры
20) DES шифрлеу стандартының негізгі ұстанымдары
21) NP-мәселелерге кіріспе. Натурал сандардың жай сандар көбейтіндісіне жіктелуі. Дискретті логарифм мәселесі
22) Ашық кілтті криптография. RSA алгоритмі
23) RSA алгоритміндегі аутентификациялау мәселесі
24) Ортақ құпияны қалыптастыру. Diffie-Hellman алгоритмі
25) Масси- Омура хаттамасы. Алгоритм осалдылығы
26) Электронды сандық қолтаңба. El-Gamal алгоритмі
27) Ақпаратқа қатынауды шектеу модельдері.
28) Дискрециондық (өкілеттік матрица негізінде құрастырылған) модель
29) Мандаттық (мандаттар ұсыну, Белл-Ла Падулл моделі).
30) Рольдік (қатынаумен роль арқылы басқару) модельдері.
31) Банк жүйелеріндегі екі кезеңдік аутентификация сипаттамасы
32) Электрондық қызметтер және криптографиялық алгоритмдер
33) Криптографияның болашақ даму бағыттары. Шешілмеген есептер
34) Жобалық қызметі. Қолданбалы есептер
35) Жобаны қорғауға қойылатын талаптар. Презентация құралдары

12. Әдебиеттер тізімі

Негізгі әдебиеттер:

1. Асылбеков У.Б., Исмаилова А.А. Киберқауіпсіздік. Оқу құралы/ I бөлім. Алматы: «Бастау», 2019.-360 б.
2. Асылбеков У.Б., Исмаилова А.А. Киберқауіпсіздік. Оқу құралы/ II бөлім. Алматы: «Бастау», 2019.-256 б.
3. Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 б.
4. Zhantassova Zh., Nugumanova A. Unstructured data and text analytics: Next generation informatics. Монография. Өскемен: ШҚМУ «Берел», 2016 ж.-168 б.
5. Жантасова Ж.З. Тлебалдинова А.С., Карменова М.А., Кадырова А.С., Уалханова А.Т. The terms and definitions in computer science. Методические указания. Усть-Каменогорск, ВКГУ им.С.Аманжолова, Издательство «Берел», 2017.-173 с.

Қосымша әдебиеттер:

1. Фергюсон Н., Шнайер Б. Практическая криптография.-М.:Вильямс, 2005
2. Романьков В.А. Введение в криптографию. Омск: ОМГУ 2009.-239
3. Смарт Н. Криптография, серия «Мир программирования», - М.: Техносфера, 2006г.
4. Жуан Г. Математики, шпионы и хакеры. Кодирование и криптография. Научно-популярное издание в 40 т. Т.2 М.: Де Агостини, 2014.-144с.
5. Актаева А., Давлеткереева Л., Муканова А. Надежность систем: тестирование и защита информации. Учебник. Алматы, TechSmith, 2018 г.-324 с.
6. Татаринова Л.Ф. Преступления в сфере компьютерных технологий. Монография. Алматы: КазНУ им. аль-Фараби, 2014.-223 с.
7. Задирака В.К., Абдикаликов К.А. Элементы современной криптологии и методы защиты банковской информации.- Алматы: Респ.изд.каб.- 1999.- 337 с.

Анықтамалық әдебиеттер:

1. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. СПб:Питер, 2017.-256 с.
2. Международный стандарт ISO/IEC 27001:2013 Взгляд в будущее индустрии ИБ.
3. Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемдері 2-бөлім/ ҚР Мемлекетік стандарты - Астана: Мемстандарт, 8-9 б.
4. Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпарат қорғауды басқару жөніндегі ережелер жиынтығы/ ҚР Мемлекетік стандарты - Астана: Мемстандарт, IV-1 б.

Интернет-көздері / Интернет источники

1. В. А. Галатенко, АО "Инфосистемы Джет" http://www.osp.ru/os/1995/04/178667/#part_5
2. http://www.ssga.ru/metodich/Edit_secbasics/index.html
3. http://www.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-270012013.-vzglyad-v-buduschee-industrii-ib#sthash.xASuPEU8.dpuf / Журнал "Information Security/ Информационная безопасность" #2, 2013 //
4. http://www.finam.ru/dictionary/wordf01FE100014/default.asp?n=1

<u>Ақпаратты қорғаудың криптографиялық әдістері</u> пәні бойынша
20_____/_____ оқу жылына арналған
пән бағдарламасына толықтырулар мен өзгерістер енгізу

Пән бағдарламасына төмендегідей өзгерістер енгізіледі:

1. _____
2. _____
3. _____
4. _____

Пән бағдарламасы қайтадан қаралды, енгізілген өзгерістер _____кафедра отырысында бекітілді
Хаттама № _____ «_____»_____20 ж.

Оқытушы _____ Жантасова Ж.З.

Кафедра меңгерушісі _____ Жантасова Ж.З.

Енгізілген өзгертулер келісілді:

Факультеттің Кеңесі төрағасы _____ Мадияров М.Н.

Хаттама № _____ «_____»_____20 ж.