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

КЕЛІСІЛДІ / СОГЛАСОВАНО

ВКГТУ имени Д.Серикбаева, кафедра Информационных технологий / Ақпараттық технологиялар кафедрасы Д. Серікбаев атындағы ШҚМТУ

Зав.кафедрой, к.т.н. _____ Кумаргажанова С.
«_3_» _____ 2019 ж./г.

БЕКІТІЛДІ/УТВЕРЖДЕНО

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

ПӘН БАҒДАРЛАМАСЫ (SYLLABUS)
ПРОГРАММА ДИСЦИПЛИНЫ (SYLLABUS)

Компьютерлік жүйелерде ақпаратты қорғау
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 Компьютерлік жүйелерде ақпаратты қорғау	Пәннің коды ZIKS-4306	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 қорғау мәселесін негіздеу. Ақпаратты қорғау құралдарын жіктеу. Ақпаратты қорғау құралдарының тиімділігін бағалау принциптері мен әдістері. Ақпараттық үрдістерде ақпаратты енгізу, шығару, беру, өңдеу және сақтауды жүзеге асыру кезінде қолданылатын ақпаратты қорғау құралдары. Ақпараттық қауіпсіздік саясаты. Қорғау үлгілері мен механизмдері. Университеттің академиялық саясатындағы қауіпсіздік ұстанымдары.

Мақсаты / Цель

«Компьютерлік жүйелерде ақпаратты қорғау» пәнінің мақсаты ақпаратты қорғау жүйелерін қолданудың теориялық негіздерін анықтау, қауіпсіздік үлгілердің, әдістердің қолдану тәжірибесін талдау болып табылады.

Міндеттері:

1) Университетте қабылданған академиялық саясатпен танысып орындау;
2) Ақпараттық қауіпсіздік саясаты, қорғау технологияларымен танысу;
3) Компьютерлік гигиена ережелерін меңгеріп, орындау;
4) Компьютерлік жүйелерді қорғауда қолданылып жүрген технологиялармен танысу;
5) Ақпараттық қауіпсіздік тақырыптарын меңгеруде логикалық құрылымын қолдану;
6) Заманауи қорғау программалық құралдарды орнатып баптау.

Құзыреттіліктер

- Компьютерлік гигиена ережелерін орындау қабілеттілігі;
- Ақпаратты қорғау технологияларын сипаттап беру;
- Зияткерлі ақпаратты қорғау құраладрын пайдалана алу;
- Қауіпсіздік саясатын қалыптастыру қабілеттілігі;
- Ақпараттық жүйенің қауіпсіздік деңгейін бағалау.

Оқыту нәтижелері

1) Ақпараттық қауіпсіздікті қамту қағидаларын ұлттық қауіпсіздік бағыттарымен байланыстыра әлеуметтік, кәсіби деңгейде құндылықтар қалыптасуы;
2) Ақпаратты қорғау технологияларына салыстырмалы талдау жасау;
3) 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	Ақпараты қорғау мәселесінің өзектілігі мен негіздемесі.	1	1	1	1	1	4
2	Ақпаратты қорғау аймағындағы қауіпсіздік стандарттар	2	1	1	1	3	6
3	Қауіпсіз жүйенің концептуалды моделі	3	1	1	1	1	4
4	Қауіпсіздік кластары мен қауіпсіздік критерийлер	3,4	2	1	2	3	8
5	Қауіпсіздік критерийлер негізінде мекеменің қауіпсіздік деңгейін бағалау	4,5	2	1	2	1	5
6	Қауіпсіз жүйені жобалау сұрақтары. Қауіпсіздік жүйенің өмірлік циклі.	5,6	1	1	2	1	6
7	АҚ қауіп-қатер жүйесі. Қаскүнем моделі.	6,7	1	1	2	1	5
8	Тәуекелділіктермен басқару.	7,8	2	3	2	3	10
9	Зияткерлік ақпаратқа заңсыз қатынау	9	1	2	2	3	9
10	Ақпаратты қорғау технологиялары мен әдістері. Ақпаратты қорғаудың криптографиялық әдістері	10	2	3	1	6	12
11	Заманауи қорғау технологиялары. Вирусқа қарсы қорғау	11	1	2	1	3	7
12	Заманауи қорғау технологиялары. Желілік сүзгілеу	11,12	1	2	1	3	7
13	Тунелдеу VPN арналарын қолдану	12,13	1	2	1	6	10
14	Ақпаратқа қатынауды шектеу модельдері.	13,14	2	3	1	6	11
15	Компьютерлік жүйелерде ақпаратты қорғау механизмдері	15	1	6	5	34	46
	Барлығы / Всего		20	30	25	75	150

6. Дәріс сабақтарының мазмұны

Тақырып 1. Ақпараты қорғау мәселесінің өзектілігі мен негіздемесі.

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. Ақпараттық қауіпсіздіктің басқару жүйесі (ISMS).ISO/IEC 27001: 2005 стандарты. Ақпараттық қауіпсіздіктің басқаружүйесі(information Security Management System)- халықаралық стандарт ақпараттың құпиялылығын, тұтастығын және қол жетімділігін сақтау арқылы кәсіпорынның ақпараттық активтерін қорғау менеджментіне қойылатын талаптарды ұсынады, сонымен қатар аталмыш стандарт процестік кіріске және Деминг цикліне негізделген.

Әдебиеттер: [3]

Тақырып 3. Қауіпсіз жүйенің концептуалды моделі

Концептуалды модель, қорғау процедуралары. ШҚМУ-ің қауіпсіздік жүйесінің сызбасы.

Қорғалған жүйенің концептуалды моделінің негізгі параметрлері

№	Қорғау процедурасының атауы	Қамтамасыз етілетін қауіпсіздік құраушысы	Қорғауды жүзеге асыру элементтері	Қосымша мәліметтер
1	Техникалық қорғау	қолжетерлік	Бейнекамералар, идентификациялау құралдары	
2	Резервті көшірме жасау	тұтастық	Көшіру командалары **copy, xcopy**	
3	Вирустан қорғау	Тұтастық, қолжетерлік	DrWeb, AVP, архивтеу	Әрдайым жаңартып отыру қажеттілігі
4	Құпия ақпаратты шифрлеу	Конфиденциалдық, тұтастық	Шифрлеу бағдарламалары (PGP, т.б.)	
5	Қатынауды басқару	Конфиденциалдық, тұтастық	Аутентификация, авторизациялау процедуралары (пароль тексеру), ЭЦҚ тарату	
6	Үрдістерді бақылау (мониторинг)	қолжетерлік	Firewall, Proxy-server, MTA (mail transfer agent)	Firewall- байланыс арналарынан өтетін желілік пакеттерін бақылаушы техникалық және программалық құралдар. Вирус пен ішкі мәліметердің жоғалуынан қорғамайды. Proxy-server – Ауқымды желіге қатынауды қамтамасыз ету. Сыртқы қатынаудан қорғау, сыртқа қатынауды шектеу MTA спамдардан қорғау (Outlook)

Әдебиеттер: [3-4]

Тақырып 4. Қауіпсіздік кластары мен қауіпсіздік критерийлер

Қауіпсіздік критерийлер, кластар. Критерийлердің күрделену динамикасы.

Қауіпсіздіктің барлық алты класы бар (C_1, C_2, B_1, B_2,B_3, A_1). Сертификация кезінде жүйені белгілі бір кластарға жатқызу үшін, оның қауіпсіздік саясаты мен кепілдеме деңгейі маңызды талаптарды қанағаттандыру қажет.

Әдебиеттер: [1-4]

Тақырып 5.

Қауіпсіздік критерийлер негізінде мекеменің қауіпсіздік деңгейін бағалау
Мекеменің ақпараттық қауіпсіздігін бағалау әдіснамасы. Қауіпсіздік саясат қағидалары. Бүгінгі күнде көптеген мекемелер ақпараттық технологияларды кең қолдануда: электрондық құжаттар жинақталуда, дайын программаларды пайдалану, Интернет арқылы байланыста болу, әлеуметтік желіде көптеген қызмет атқару. Құндылығы бар мәліметтерді аяқ астынан жоғалтып алудан, көшірмесін жасаудан сақтау, вируспен зақымдалуынан қорғау әр күннің тәртібіне кіруде. Бүгінгі күнде қолданылып жүрген құралдарымыз да белгілі.

Әдебиеттер: [3-5]

Тақырып 6. Қауіпсіз жүйені жобалау сұрақтары. Қауіпсіздік жүйенің өмірлік циклі.
Қауіпсіз жүйені жобалау кезеңдері, өмірлік цикл ұғымы

Қорғау жүйесін жобалау принциптері:

– Жүйелік принципі ақпараттық қауіпсіздік мәселелерін шешуде бір біріне байланысты жағдайлардың, факторлардың барлығының ескерілуін талап етеді;
– Құзіреттілік принципі барлық қауіптерден қорғауды қамтитін жан-жақты құралдардың қолданылуын қарастырады;
– Үздіксіз қорғау дегеніміз ақпараттық жүйенің жобалану кезеңінен бастап қолдану кезеңінде жалғасып жатқан уақыт пен кеңістік бойынша үзілмейтін үрдіс;
– Орындылық жеткіліктілік принципі қорғау жүйесіне қаржылардың жұмсалуы барынша көп қайтарыммен жүзеге асырылуы тиісті;
– Басқару мен қолданудың икемділігі қорғау жүйесінің оңай бапталуын қамтамасыз ету тиісті;
– Қорғау механизмдері мен алгоритмдерінің ашықтығы қорғау алгоритмін білгенмен оны бұзуға мүмкіншілік бермейді;

Қорғау құралдарының қолдану ыңғайлылығы.

Әдебиеттер: [1,3-4]

Тақырып 7. АҚ қауіп-қатер жүйесі. Қаскүнем моделі.

Қауіп көздері, қаскүнем үлгісі. Қауіп дегеніміз қорғалған нысанға қатысты моральды немесе материалды зиян келтіре алатын іс-әрекеттер орындалу ықтималдығы. Қауіп-қатерлерді тауып, талдау ықтимал зиянның мөлшерін алдын ала есептеуге мүмкіншілік береді. Қауіп көздерін анықтау, түрлерін айыру алдын ала шаралар қабылдап зиян болдырмау амалдарын іздеуге жағдай жасайды.

Әдебиеттер: [3]

Тақырып 8. Тәуекелділіктермен басқару.
Тәуекел, тауекелді есептеу әдістемелері.

Халықаралық ақпаратты қорғау тәжірибесіне сәйкес ақпараттық қауіпсіздікті (АҚ) қамтамасыз етуде ақпараттық тәукелдерді талдау маңызды орын алады. АҚ-ің нормативті-құқықтық базасы бүгінгі жағдайда қалыптасуда: бір қатар басқарушылық құжаттар, стандарттар қабылданған. Дегенмен тәуекелдерді талдау сұрақтары әлі де регламенттелмеген. Осы себептен мекемелер тәуекелді талдау құралдарын өз бетімен таңдауға мәжбүр.

Әдебиеттер: [8-13]

Тақырып 9. Зияткерлік ақпаратқа заңсыз қатынау

Азаматтық-құқықтық қатынастардың көпшілігі зияткерлік, әсіресе, шығармашылық жұмыстың – ғылым, әдебиет, өнер туындылары, өнертабыстар, ЭЕМ үшін бағдарламалар, өнеркәсіптік үлгілер және т.б. нәтижелерін жасау және қолданумен байланысты қалыптасады.

Шығармашылық қызметтің туындылары материалдық емес игіліктерге жатады. Мысалы, ғылым, әдебиет, өнер туындылары, яғни жаңа идеялар, бейнелер, ұғымдар жиынтығы; өнертабыс, пайдалы үлгі және тиімді ұсыныс – есептің техникалық шешімдері; өндірістік үлгі – бұйымның сыртқы түрін көркем құрастыру және т.с.с. Бірақ олар басқалар қабылдай алатындай объективті түрге келгенде ғана азаматтық құқықтық қарым-қатынастар объектісі ретінде болады. Мысалы,

ғылыми жоба қағазға, немесе магниттік таспаға жазылуы мүмкін; өнертабыс сызба, үлгі немесе т.б. ретінде көрсетілуі мүмкін.
Әдебиеттер: [8-13]

Тақырып 10. Ақпаратты қорғау технологиялары мен әдістері. Ақпаратты қорғаудың криптографиялық әдістері

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 $f(x)=x^e modn$ біржақты функциясы жатыр. Егер **$y=x^e modn$,** e-ашық кілтінің мағынасы белгілі болса, n- модуль болса, онда біз d: $y^d=x^{ed=1} modn=x$ дешифрлеу кілтін білмесек x-ті қалпына келтіру қиын.

Әдебиеттер: [8-13]

Тақырып 11. Заманауи қорғау технологиялары. Вирусқа қарсы қорғау

Вирус – басқа бағдарламаларды олардың түрлендірілген көшірмесін жасау жолымен зақымдайтын, алдағы уақытта көбейіп кету мүмкіндігі бар бағдарлама.

Вирус екі негізгі сипаттамасымен ерекшеленеді деп есептелінеді:

а) Өздігінен көбею мүмкіндігімен;

б) Есептеу процесіне кедергі келтіру мүмкіндігімен (яғни басқару мүмкіндігіне ие болу).

Резидентсіз вирус бұзылған программа қосылғанда жұмыс атқарады. Вирус программасы программа жұмыс істеп отырған уақытта қауіпті.

Вирустар түрлері, файлдарды зақымдау механизмдері. Антивирустық қызмет. Белгілі вирусқа қарсы бағдарламалар.

Әдебиеттер: [5-7]

Тақырып 12. Заманауи қорғау технологиялары. Желілік сүзгілеу

Көптеген ұйымдар үшін желіаралық экранды орнату ішкі желі қауіпсіздігін қамтамасыз етудің қажетті шарты болып табылады. Жалпы қатынайтын жүйеден қатерлерді бұғаттау үшін, «желіаралық экран» (Firewall) атауын алған арнайы бағдарламалық немесе ақпараттық-бағдарламалық құрал пайдаланылады. Негізінен, желіаралық экран бөлінген ЭЕМ-де жүзеге асырылады және сол арқылы қорғалған, бөлінген коммуникациялық желі (оның фрагменті) жалпы қатынау желісіне қосылады. Желіаралық экран, қорғалған жүйеден шығатан және қорғалған бөлінген коммуникациялық жүйеге түсетін ақпараттарды бақылауды жүзеге асырады. Windows операциялық жүйеде брандмауэр функциялары.

Әдебиеттер: [5-7]

Тақырып 13. Тунелдеу VPN арналарын қолдану

VPN (virtual private network) қорғалған виртаулды желілер технологиялары. Техникалық шешімдердің архитектурасына байланысты VPN–ің 3 түрін атап өтуге болады:

1) Корпорацияның ішінде құрылған (Intranet VPN);
2) Қашықтан қатынаулы (Remote Access VPN);
3) Корпорациялар арасында құрылған (Extranet VPN).

Әдебиеттер: [5-13]

Тақырып 14. Ақпаратқа қатынауды шектеу модельдері.

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. *Ақпаратқа қатынау үлгісі - жүйенің қауіпсіздігін қамтамасыз ететін, ақпаратқа, ақпарат ағымдарына қатынауды басқаратын ережелер жиынтығы.* Ақпаратқа қатынау үлгілерінің негізгі сипаттамалары. Дискреционды (матрицалық) қатынау үлгісі немесе таңдамалы үлгі Өкілетті немесе мандатты үлгісі (еріксіз басқару). Рөлдік басқару үлгісі. *"Қытай қабырғасы"*(The Chinese Wall) *үлгісі. Гоген-Мезигер (Goguen-Meseguer) үлгісі. Биба (Biba) үлгісі Кларк-Вилсон үлгісі (Clark-Wilson model*)

Әдебиеттер: [6]

Тақырып 15. Компьютерлік жүйелерде ақпаратты қорғау механизмдері.

Сенім көрсетілген база және қауіпсіздік периметрі түсініктері. Қарапайым, көп түйінді, көп деңгейлі үлгілер сызбалары. Мекеменің ақпараттық қауіпсіздік саясаты.

Әдебиеттер: [2-5]

7. Зертханалық сабақтар

Тақырып 1. Пәнге қатысты әдебиеттермен жұмыс жасап, іріктеу

Кітапханалардан, интернет желісінен әдебиеттерді жинақтаймыз, соңғы 5 жылдық аралығында шыққан әдебиеттерді кестеде берілген талаптарға сәйкес толтырамыз. Кесте үлгісі Зертханалық жұмыстар файлында берілген.

Тақырып 2. Қауіпсіздік терминдеріне глоссарий толықтыру

Үлгіде берілген терминологиялық глоссарийді әр студент 3-5 жаңа түсініктермен толықтырады. Глоссарий толтыру үлгісі Зертханалық жұмыстар файлында берілген.

Тақырып 3. Қаупсіздік саясатты қалыптастыру тәртібі. Мекеменің қауіпсіздігін бағалау

Келесі әдебиетте: Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 берілген 1.4 тарауын «Қауіпсіз критерийлері негізінде мекеменің ақпараттық қауіпсіздігін бағалау» қолданып 1-2 тапсырмаларды орындау, 3-ші тапсырма әзірлеу

Тапсырма 4:

1. Ақпараттық қауіпсіздік деңгейін бағалау тапсырмаларын құрастыру. Қаскүнем үлгісін жасау. Жұмысты орындауда қосымша деректерді негізгі әдебиеттер тізіміндегі [3-4] үлгілерді негізге алуға болады.

Тақырып 5. Зияткерлі ақпаратты қорғау

Антиплагиат бағдарламаларымен жұмыс істеуді меңгеру. Зияткерлі ақпаратты иемдену (плагиат) деңгейін тексеру жолдарын көрсету. Берілген файлды плагиатқа тексеру.

Тақырып 6.

Макровирустардан қорғау жүргізу. Жүктелетін вирустардан қорғау. Шағын нұсқаулықтар құрастыру және бір кешенге біріктіру. Электрондық кітапша түрінде (верстка) құрастырылған нұсқаулықтар *Әдебиеттер:[6-13]*

Тапсырма 7. Ақпаратқа қатынауды шектеу үлгілері.

Келесі үлгілерді қарастырып:

1) Дискреционды (матрицалық) қатынау үлгісі немесе таңдамалы үлгі
2) Өкілетті немесе мандатты үлгісі (еріксіз басқару).

3) Рөлдік басқару үлгісі.

Қосымша жаңа үлгілердің сипаттамасын беріңіз. Жоғарыда берілген үлгілердің сипаттамасы оғарыда берілген үлгілердің сипаттамасы, салыстырмалы талдауы 3-ші әдебиетте берілген.

8. БӨЖ мен БОӨЖ бойынша тапсырма

№ п/п	Сабақтардың тақырыптары	БОӨЖ тапсырма	Тапсырманың мақсаты мен мазмұны	Бақылау түрі	Өткізу мерзімі
1	Бейнересурстар топтамасы	Ақпарат арналарынан еліміздегі ақпараттық қауіпсіздікке қатысты бейнересурстар қарап компьютерлік гигиена ережелерін тізімдеу	Ағымдағы ахуалды білу, түсіну	Бейнересурс іріктеп алу	1-2 апта
2	Пәннің терминологиялық негіздемесі	Ақпараттық қауіпсіздік глоссариін толықтыру	Терминологиялық қорын қалыптастыру	Жаңа терминдер сипаттамасы	3-4 апта
3	Қауіпсіздік критерийлерге негізінде жүйенің деңгейін бағалау	Жүйе сипатамасын қауіпсіздік критерийлерге сәйкестендіру	Қауіпсіздік критерийлердің мазмұнын түсіну	Сәйкестендіру кестесі	5-6 апта
4	Қауіптер классификациясы	Қаскүнем үлгісін жасау	Компьютерлік жүйелердің шабуылдарға осал жақтарын білу	Қаскүнем сызбасы	7 апта
5	Зияткерлі ақпаратты қорғау құралдары	Зияткерлі ақпаратты иемдену (плагиат) деңгейін тексеру жолдарын көрсету	Антиплагиат бағдарламаларымен жұмыс істеуді меңгеру	Берілген файлды плагиатқа тексеру	8-9 апта
6	Вирустан қорғау іс-шаралары. Вирусқа қарсылық көрсету ұсыныстары	Макровирустардан қорғау жүргізу. Жүктелетін вирустардан қорғау.	Шағын нұсқаулықтар құрастыру және бір кешенге біріктіру	Электрондық кітапша түрінде (верстка) құрастырылған нұсқаулықтар	10-11 апта
7	Ақпаратқа қатынауды шектеу саясаты	Қатынауды шектеу үлгілерінің салыстырмалы таладуын жасау	Ақпаратқа қатынауды шектеу үлгілерін бағалау	Салыстырмалы кесте	12-13 апта
8	Қорытынды бақылау	Тесттік тексеру	Білім алушылардың құзіреттіліктерін бағалау	тест	14-15 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.	Глоссарий қалыптастыру	100	1	100
3.	Жүйедегі қауіпсіздік жағдай сипатының қауіпсіз критерийінің сипаттамасына сәйкестігін орнату	100	1	100
4.	Өзіндік қаскүнем үлгісін тұрғызу	100	1	100
			Барлығы	100
Рейтинг 2				
1.	Антиплагиат бағдарламамен жұмыс жасау	100	1	100
2.	Макровирустардан қорғау жүргізу. Жүктелетін вирустардан қорғау.	100	1	100
3.	Ақпаратқа қатынауды шектеу үлгілерінің салыстырмалы талдауын жасау	100	1	100
4.	Тест	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. Ақпараты қорғау мәселесінің өзектілігі мен негіздемесі.
2. АҚ және АҚ ұғымдарының өзара байланысы.
3. Ақпараттық қауіпсіздік құрауыштары.
4. ҚР АҚ стратегиясы.

5. Компьютерлік жүйелердің қорғалу нормаларының концепциясы.
6. АҚ аймағындағы заңдық құжаттарына шолу.
7. АҚ аймағындағы стандарттар мен спецификациялар.
8. «Қызғылт сары кітабы»-ның бағалау стандарттары.
9. Тиімді ақпараттық қауіпсіздік саясатын қалыптастыру сұрақтары
10. Қауіпсіздік критерийлер негізінде мекеменің ақпараттық қауіпсіздігін бағалау
11. Ақпаратты қорғаудың концептуалды моделі
12. АҚ қауіп-қатер жүйесі.
13. Ақпараттың жойылу каналдары. Қаскүнем үлгісі
14. Тәуекелділіктермен басқару. Тәуекелді азайту бағыттары.
15. Қауіпсіз жүйенің өмірлік циклі. Қауіпсіз жүйені жобалау принциптері
16. Ақпаратты қорғаудың криптографиялық әдістері.
17. Электорндық қызмет көрсету порталының қорғау функциялары
18. Ақпаратты қорғаудың көпдеңгейлі моделі.
19. Ақпаратты қорғау құралдарының жіктелуі.
20. Ақпараттық қауіпсіздіктің ұйымдастырушылық, құқықтық, ақпараттық қамсыздандырылуы.
21. Ақпаратты қорғау құралдарының жіктелуі.
22. Ақпараттық қауіпсіздіктің техникалық және программалық қамсыздандырылуы.
23. VPN технологияларды қолдану аспектілері
24. Желіаралық терезелер қызметтері
25. Брандмауэр Windows қызметінің конфигурациясын баптау
26. Ақпаратқа қатынау модельдері.
27. Дискрециондық (өкілеттік матрица негізінде құрастырылған) модель.
28. Ақпаратқа қатынау модельдері.
29. Мандаттық (мандаттар ұсыну, Белл-Ла Падулл моделі).
30. Рольдік (қатынаумен роль арқылы басқару) модельдері.
31. Зияткерлі ақпаратты қорғау тәсілдері
32. Банктік жүйелердегі екі кезеңді аутентификацияның жұмыс жасау принциптері
33. Антивирустық бағдарламаларға қарсылық көрсету шаралары
34. Қауіпсіздік өзегі түсінігі. Қауіпсіздік периметрін құру
35. Мекеменің қорғалған жүйесінде серверлік бөлімнің қауіпсіздігі

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. Зарубин М.Ю. Противовирусная защита. Учебное пособие. Алматы. ИП «Отан», 2014 г.

2. Зияткерлік ақпаратты заңсыз қатынаудан қорғау технологиялары мен тәжірибесі [Электрондық ресурс]. - http://kk.wikipedia.org/wiki/Зияткерлік _ақпаратты _заңсыз_қатынаудан_ қорғау_технологиялары_мен_тәжірибесі.
3. Актаева А., Давлеткереева Л., Муканова А. Надежность систем: тестирование и защита информации. Учебник. Алматы, TechSmith, 2018 г.-324 с.
4. Татаринова Л.Ф. Преступления в сфере компьютерных технологий. Монография. Алматы: КазНУ им. аль-Фараби, 2014.-223 с.
5. 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.