ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И.СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ

6М100200 - АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ МАМАНДЫҒЫНЫҢ ЭЛЕКТИВТІ ПӘНДЕР КАТАЛОГЫ

Алматы 2015

Элективті пәндер каталогы Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің ғылыми-әдістемелік кеңесінде бекітілген 2015 жылғы «15» маусым (№5 хаттамасы). Алматы, ҚазҰТЗУ, 2015.

Каталог элективті пәндердің (таңдау бойынша компоненттердің) тізімін, пәндердің пререквизиттері мен постреквизиттерін, пәнді оқыту мақсатын, олардың қысқаша мазмұнын, күтілетін нәтижелерін қамтиді.

БІЛІМ АЛУШЫ МЕН ЭДВАЙЗЕРГЕ АРНАЛҒАН ЖАДНАМА

Мамандықтың барлық пәндері модульдер мен циклдер (бакалавриатта ЖБП, БП, ПП; магистратура мен докторантурада БП, ПП) бойынша бөлінген. Олардың ішінде пәндер міндетті және элективті (таңдау) пәндеріне бөлінген. Оқуға міндетті пәндердің тізімі мамандықтың үлгілік оқу жоспарында (ҮОЖ) келтірілген. Мамандықтың әр курсы үшін элективті пәндер тізімі элективті пәндер каталогында (ЭПК) келтірілген. ЭПК мамандықтың таңдау пәндерінің жүйеленген аннотацияланған тізімі болып табылады. ЭПК білім алушыларға оқытудың таңдалған траекториясына сәйкес элективті оқу пәндерінің альтернативті таңдау мүмкіндігін беруі керек.

Мамандық бойынша ҮОЖ бен ЭПК негізінде білім алушының оқу жылына жеке оқу жоспары (ЖОЖ) құрылады. ЖОЖ-ды шығарушы кафедра тағайындаған эдвайзердің көмегімен бакалаврлар мен магистранттар құрастырады. Докторанттар ЖОЖ-ды өздері құрастырады. ЖОЖ мамандық шегінде әрбір білім алушының жеке білім алу траекториясын анықтайды. ЖОЖ-ға ҮОЖ-дан міндетті компонент пәндері мен оқу қызметінің түрлері (практикалар, зерттеу жұмысы, мемлекеттік (кешенді) емтихан, дипломдық жұмысты (жобаны) жазу, диссертацияны ресімдеу және қорғау) және ЭПК-дан таңдау компоненті пәндері кіреді.

Еңбек нарығының және жұмыс берушілердің талаптарының есебімен нақты жұмыс саласына бағытталған білім беру траекториясының бакалаврларына көмек ретінде ЭПК шегінде білім алушыларға көзделген білім беру траекториясын меңгеруді кепілдейтін пәндер тізімі берілуі керек.

Элективті оқу пәндерін таңдаған кезде мыналарды есепке алу керек:

1 Бір семестрде міндетті түрде оқылатын оқытудың қосымша түрлерін (ОҚТ) есептемегенде, күндізгі оқыту бөлімінің студенті 18-22 кредитті (міндетті және элективті), сырттай оқыту бөлімінің студенті 9-12 кредитті (міндетті және элективті) игеруі тиіс.

2 Оқытудың барлық кезеңіндегі жалпы кредит саны мамандықтың ҮОЖ-нда көрсетілген саннан аспауы керек.

3 Элективті пәндер тиісті нөмірі бар таңдау топтарына біріктірілген. Пәндердің әр тобынан бір ғана элективті оқу пәнін таңдауға болады.

Академиялық дәрежесі: әскери ғылым магистрі

_____1_____
(оқу курсы)

№	Модуль атауы	Пән циклі	Пән коды	Пән атауы	Кредиттер саны	Семестр
1	Қауіпсіздік жүйелерін ұйымдастыру модулі	БД	SBS 5205	Желілік ОЖ-дің қауіпсіздік құралдары	3	1
1.1		БД	MSZ 5205.1	ОЖ қорғау әдістері мен құралдары	3	1
2	Жоғары өнімді технологиялар модулі	БД	APVS 5206	Параллель есептеу жүйелерінің сәулеті	3	1
		БД	VTVS 5206.1	Есептеу жүйелеріндегі жоғары өнімділікті технологиялар	3	1
		БД	PaV 5207	Ақпаратты қорғау және параллель есептеулер	3	2
		БД	MPV 5207.1	Ақпаратты қорғаудағы параллель есептеу әдістері	3	2
	Қорғау модулі	ПД	PSSZ 5302	Желілердің хаттамалары мен стандарттары және оларды қорғау	3	2
		ПД	YBS 5302.1	Желі қауіпсіздігін басқару	3	2
		ПД	KMZI 5303	Ақпаратты қорғаудың криптологиялық әдістері мен құралдары	3	2
		ПД	AKZI 5303.1	Ақпаратты криптологиялық қорғау алгоритмдері	3	2

		ПД	OZBD 5304	ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру	3	2
		ПД	ASBS 5304.1	ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті	3	2

(көрсетілген курста оқылатын әрбір элективті пәннің сипаттамасы)

SBS 5205, Желілік ОЖ-дің қауіпсіздік құралдары, 3 кр

Пререквизиттер: Операциялық жүйелердің ұйымдастырылуы, Компьютерлік ақпаратты қорғау әдістері мен құралдары.

Оқыту мақсаты: Желілік операциялық жүйелерде (ОЖ) ақпараттық қауіпсіздік жүйелерін құру принциптерін игеру. ОЖ қорларына рұқсатсыз қатынас құру әдістері мен құралдары.

Қысқаша мазмұны: Желілік ОЖ ақпараттық қауіпсіздігін қамтамасыз ету негіздері. Бағдарламалық қамтамасыз етудің бүтіндік бақлауы және өзгертуден қорғау. Көпфакторлы аутентификацияның принциптері. Идентификация мен аутентификацияның техникалық құрылғылары. Идентификацияның мен аутентификацияның құпиялық бағыныңқы жүйелері. Биометриялық құрылғылардың колдануымен пайдаланушылардың идентификциясы мен аутентификациясы. Шифрлаудың бағдарламалы-аппаратты құралдары. Желілік операциялық жүйелердің қауіпсіздігі. Windows, Unix жүйелерінде қауіпсіздікті қамтамасыз ету. Басып кыруды анықтайтын жүйелер. Желіаралық экрандардың сәулетінің негізгі компоненттері. Желіаралық экрандарға қойылатын заманауи талаптар.

Күтілетін нәтижелер: Желілік ОЖ қауіпсіздік сенімділігін және тиімділігін бағалау. Заманауи желілік ОЖ әкімшілеуді игеру. Желіаралық экрандар мен басып кіруді анықтау жүйелерін қолдану.

Постреквезиттер: Желінің қауіпсіздігін басқару, магистерлік диссертация

MSZ 5205.1, ОЖ қорғау әдістері мен құралдары, 3кр

Пререквизиттер: Операциялық жүйелердің ұйымдастырылуы, Компьютерлік ақпаратты қорғау әдістері мен құралдары.

Оқыту мақсаты: Операциялық жүйелерде ақпаратты қорғауды құру принциптерін игеру және қорғаудың сенімділігіне талдау жасау. ОЖ қорларына рұқсатсыз қатынау әдістері мен құралдары.

Қысқаша мазмұны: Опреациялық жүйелердегі ақпаратты қорғаудың нұсқаулары мен негізгі түсіктері. Ақпаратты-есептеу жүйелеріндегі ақпараттың қауіпсіздік қатерлері. ОЖ қауіпсіздік қатерлері. ОЖ қауіпсіздікке қойылатын талаптары. Заманауи операциялық жүйелердің қауіпсіздігін талдау. Windows, Unix, Mac OS құрамдасқан қауіпсіздік құралдары. Заманауи ОЖ шабуылдар негізінде жатқан әдістердің статистикасы. ОЖ қатынауды шектеу. ОЖ пайдаланушылардың идентификациясы мен аутентификациясы. Windws, Unix, Mac OS ОЖ қорларға қатынауға шектеулер орнату. ОЖ аудиті. Бағдарламалық қамтаманы қорғау жүйелері.

Күтілітін нәтижелер: ОЖ қорғау құралдарының сенімділік және тиімділік бағаларының критерилерін білу. ОЖ қауіпсіздік саясатын жоспарлау. ОЖ қауіпсіздік тетіктерін бағалау.

Постреквезиттер: Желі қауіпсіздігін басқару, магистерлік диссертация

APVS5206 Параллель есептеу жүйелерінің сәулеті 3кр.

Пререквизиттер: Цифырлық афтоматтардың қолданбалы теориясы, ЭЕМ сұлбатехниканы есептеу машиналарын ұйымдастыру.

Оқыту мақсаты: Параллель өңдеу тәсілдерін меңгеру арқылы өнімділігі жоғары әртүрлі сипатты есептеу жүйелерін құру жолдарын білу.

Қысқаша мазмұны: Параллель өңдеу деңгейлері, параллель есептеу өлшемдері, параллель есептеу заңдылықтары. ЕЖ жады жуйесін ұйымдастыру. ЕЖ тонологиясы. SIMD сипатты есептеу жуйелерінің түрлері: векторлық, матрицалық, ассоциативтік және систоликалық ЕЖ. MIMD сипатты есептеу жүйелері: MPP жүйесі, кластерлік жүйелер және негізінде құрылған жүйлер.

Күтілетін нәтиже: Әртүрлі сипатты есептеу жұйелеін құру жолдарын білу және оларда әртүрлі есептерді шығаруға машықтану.

Постреквезиттер: Ақпаратты қорғау және параллель есептеулер, Ақпаратты қорғаудағы параллель есептеу әдістері

VTVS5206.1 Есептеу жүйелеріндегі өнімділігі жоғары технологиялар 3кр

Пререквизиттер: ЭЕМ сұлбатехникасы, Цифрлық автоматтардын қолданбалы теориясы, Есептеу жүйелерінің сәулеті.

Оқыту мақсаты: Параллель өңдеулерге негізделген технологияларда меңгеру арқылы өнімділігі жоғары есептеу жүйелерін құру жолдарын білу.

Қысқаша мазмұны: Параллелизм негізінде құрылған есептеулер технологиясы, параллель есептеулер заңдылықтары. Өнімділігі жоғары есептеу жүйелерін жіктеу ЕЖ жады құрылғыларын ұйымдастыру. Векторлық, матрицалық, ассоциативтік, систоликалық есептеу жүйелері. Компьютерлер негізінде құрылған ЕЖ: MPP, және класстерлік ЕЖ. Транспортерлер негізінде құрылған ЕЖ.

Күтілетін нәтижелер: Өнімділігі жоғары технологиялар негізінде құрылған ЕЖ меңгеріп әртүрлі есептерді тиімді жүйелерде шығару.

Постреквезиттер: Ақпаратты қорғау және параллель есептеулер, Ақпаратты қорғаудағы параллель есептеу әдістері

PaV 5207, Ақпаратты қорғау және параллель есептеулер, 3кр

Пререквизиттер: Операциялық жүйелерді ұйымдастыру

Оқыту мақсаты: Симметриялық және асимметриялық криптожүйелерді криптоталдауда ақпаратты параллель өңдеу принциптерін қолдану.

Қысқаша мазмұны: Параллель есептеудің негізгі прининтері. Есептеу тапсырмаларын параллельділігінің түрлері. Параллель есаептеу тәсілдері. Есептеу құралдары өнімділігін көтеру. Үлестірілген көппроцессорлық есептеу принциптерін қолдану. Кластерлік есептеу жүйелерінің заманауй қолданбалы бағдарламалары. Шифрлаудың симметриялық алгоритмдерін талдау. Ақпаратты параллель өңдеу құралдарын құру үшін MPI интерфейсін қолдану. Криптоқорғау алгоритмдері үшін дифференциалды талдау әдістерін қолдану. Параллельдік үлестірілген есептеуді қорғау мәселелері.

Күтілетін нәтижелер: Ақпаратты қорғау мәселелерін шешу үшін ақпаратты параллельді үлестірілген өңдеу принциптерін пайдалана білу.

Постреквизиттер: Ақпаратты қорғаудың криптологиялық әдістері мен құралдары, Ақпаратты криптологиялық қорғау алгоритмдері

MPV 5207.1, Ақпаратты қорғаудағы параллель есептеу әдістері, 3кр

Пререквизиттер: Операциялық жүйелерді ұйымдастыру

Оқыту мақсаты: Ақпаратты қорғау жүйелерін құру кезінде ақпаратты параллель өңдеу әдістерін қолдану.

Қысқаша мазмұны: Параллельді есептеудің негізгі әдістері. Есептеу тапсырмаларын параллельділігінің түрлері. Параллель есаептеу тәсілдері. Есептеу құралдары өнімділігін көтеру. Үлестірілген көппроцессорлық есептеу принциптерін қолдану. Кластерлік есептеу жүйелерінің заманауй қолданбалы бағдарламалары. Шифрлаудың симметриялық алгоритмдерін талдау. Ақпаратты параллель өңдеу құралдарын құру үшін MPI интерфейсін қолдану. Криптоқорғау алгоритмдері үшін дифференциалды талдау әдістерін қолдану. Параллельдік үлестірілген есептеуді қорғау мәселелері. Үлестірілген параллельді есептеу жүйелерін қорғау.

Күтілетін нәтижелер: Ақпаратты қорғау мәселелерін шешу үшін ақпаратты параллельді үлестірілген өңдеу принциптерін пайдалана білу.

Постреквизиттер: Ақпаратты қорғаудың криптологиялық әдістері мен құралдары, Ақпаратты криптологиялық қорғау алгоритмдері

PSSZ 5302, Желілердің хаттамалары мен стандарттары және оларды қорғау, 3кр

Пререквизиттер: Желілік ОЖ-дің қауіпсіздік құралдары, ОЖ қорғау әдістері және құралдары, Ақпараттық қауіпсіздік жүйелерінің ұйымдастырылуы, Ақпарат қорғаудың криптографиялық әдістері мен құралдары.

Оқыту мақсаты: компьютерлік желілердің хаттамалары мен стандарттары, сәулеті мен жұмыс істеу қағидаттары, сондай-ақ желілердегі ақпарат тасымалдау қауіпсіздігі жайындағы білімдерді меңгеру.

Қысқаша мазмұны: Компьютерлік желілердің қазіргі жағдайы. OSI модельдері деңгейлеріне сәйкес хаттамалар. Желілердің аппараттық құралдары. Жергілікті желілердің базалық технологиялары (сәулеттері). Ауқымды желілер және олардың технологиялары. Қорғанылған корпоративтік желінің құрылымы. Желілердің қауіпсіздік хаттамалары. Ауани желілер. Жоғары жылдамдықты жергілікті желілер және олардың болашағы. Сымсыз байланыстың болашағы. Сымсыз қатынастар технологиялары. Ұяшықтық сымсыз желілердің тұжырымдамалары және мүмкіндіктері. Сымсыз Интернет. Желілердегі ақпарат тасымалдау қауіпсіздігі. Компьютерлік желілерде ақпарат қорғау құралдарының негізгі даму бағыттары.

Күтілетін нәтижелер: Компьютерлік **ж**елілердің хаттамалары мен стандарттары, желілердегі ақпаратты қорғау жайындағы білімдерді және оларды қолдану дағдыларын дамыту.

Постреквизиттер: Ақпараттың сыртқа кету арналарын іздеудің және табудың аппараттық құралдары, Ақпаратты инженерлік-техникалық қорғау.

YBS 5302.1, Желі қауіпсіздігін басқару, 3кр

Пререквизиттер: Ақпарат қорғаудың криптологикалық әдістері мен құралдары, Ақпаратты криптографиялық қорғау алгоритмдері, ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті

Оқыту мақсаты: Желілік қорғаныш жүйесінің сәулетін, қауіпсіздік хаттамаларын, қорғаныш үдерістерін оңтайлы басқару, ақпараттық қауіпсіздік саясатын меңгеру.

Қысқаша мазмұны: OSI модельдері деңгейлеріне сәйкес хаттамалар. Қазіргі заманғы желілерде ақпараттық қауіпсіздікті қамтамасыз ету техноло-гиялары. IPSec, PPTP, L2TP, SSL қауіпсіздік хаттамалары. Ауани желілер. Қорғанылған арналармен деректер тасымалдауды ұйымдастыру. Желіаралық экрандардың (брандмауэры, firewall) атқаратын міндеттері, жұмыс істеу қағидаттары, жағымды және жағымсыз жақтары. IDS, WIDS және IPS жүйелерінің атқаратын міндеттері және түрлері. Антивирустық қорғаныш.

Көпфункционалдық қорғаныш құрылғылары. Сымсыз желілердегі деректерді қорғау тетіктері.

Күтілетін нәтижелер: Компьютерлік желі қауіпсіздігін басқару жайында ділімдерді және дағдыларды дамыту.

Постреквизиттер: Ақпараттық қауіпсіздіктің менеджмент жүйелері, Ақпараттық қауіпсіздікті басқару, Электрондық бизнес жүйелерінің қауіпсіздігі.

KMZI 5303, Ақпаратты қорғаудың криптологиялық әдістері мен құралдары, 3кр

Пререквизиттер: Криптографияның математикалық негіздері, Ақпаратты қорғау және параллель есептеулер, Ақпаратты қорғаудағы параллель есептеу әдістері

Оқыту мақсаты: Шифрлау алгоритмдерін, программалау тілінде стандартты криптожүйелерді жүзеге асыра алуды білу, ақпаратты қорғаудың түрлі әдістерін аралас қолдана алуға машықтану.

Қысқаша мазмұны: Заманауи криптография және ақпаратты қорғау мәселелерімен байланысты тапсырмалар. Криптожүйеге формальды анықтама. Классикалық криптожүйелер. Криптоталдаудың негізгі міндеттері. Ағындық шифрлау. Ашық кілтті криптожүйелер. Криптографияда математикалық модельдеуді қолдану. Түрлі жүйелердің артықшылықтары мен кемшіліктері. Эйлер және Ферм теоремалары. Кілттерді басқару. Кілтті беруді қамтымайтын жүйе. Қарапайым көбейткіштерге жіктеу мәселесі. Дискретті логарифмдеу мәселесі. Криптоберіктілік мәселесі. Ақпаратты қорғау жүйелері, электрондық қолтаңба сұлбасы, аутентификация және идентификация хаттамалары.

Күтілетін нәтижелер: Магистрант криптография негіздерін, криптоталдау әдістерін біліп, ақпаратты қорғау тапсырмаларын шешуде криптоталдау әдістері мен математикалық модельдеуді қолдана білуі керек, алынған нәтижелерді сапалы талдай білуге машықтануы керек.

Постреквизиттер: Ақпараттық қауіпсіздіктің менеджмент жүйесі, Экономикалық жүйелердің ақпараттық қауіпсіздігі

AKZI 5303.1, Ақпаратты криптологиялық қорғау алгоритмдері, 3кр

Пререквизиттер: Криптографияның және шифрлаудың математикасы, Ақпаратты қорғау және параллель есептеулер, Ақпаратты қорғаудағы параллель есептеу әдістері

Оқыту мақсаты: Шифрлау алгоритмдерін, программалау тілінде стандартты криптожүйелерді жүзеге асыра алуды білу, ақпаратты қорғаудың түрлі әдістерін аралас қолдана алуға машықтану.

Қысқаша мазмұны: Заманауи криптография және ақпаратты қорғау мәселелерімен байланысты тапсырмалар. Криптожүйеге формальды анықтама. Классикалық криптожүйелер. Криптоталдаудың негізгі міндеттері. Ағындық шифрлау. Ашық кілтті криптожүйелер. Криптографияда математикалық модельдеуді қолдану. Түрлі жүйелердің артықшылықтары мен кемшіліктері. Эйлер және Ферм теоремалары. Кілттерді басқару. Кілтті беруді қамтымайтын жүйе. Қарапайым көбейткіштерге жіктеу мәселесі. Дискретті логарифмдеу мәселесі. Криптоберіктілік мәселесі. Ақпаратты қорғау жүйелері, электрондық қолтаңба сұлбасы, аутентификация және идентификация хаттамалары.

Күтілетін нәтижелер:Магистрант криптография негіздерін, криптоталдау әдістерін біліп, ақпаратты қорғау тапсырмаларын шешуде криптоталдау әдістері мен математикалық модельдеуді қолдана білуі керек, алынған нәтижелерді сапалы талдай білуге машықтануы керек.

Постреквизиттер: Ақпараттық қауіпсіздікті басқару, Электрондық бизнес жүйелерінің қауіпсіздігі

OZBD 5304, ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, 3кр

Пререквизиттер: Дерекқорлардың қауіпсіздігі және сенімділігі, Дерекқорларды жобалау және қорғау, Ақпаратты криптографиялық қорғау әдістері мен құралдары, Ақпарат қорғау жүйелерін ұйымдастыру, Желілік ОЖ-дің қауіпсіздік құралдары, ОЖ -дегі қорғау әдістері және құралдары.

Оқыту мақсаты: Дерекқор қорғауды және қауіпсіздендіруді ұйымдастырудың негізгі қағиғаттарын менгеру.

Қысқаша мазмұны: ДҚ қауіпсіздігінің аспектілері және критерийлері, қауіпсіздік саясаты. Дерекқор қауіпсіздігінің қауіптері. Дерекқорлардың қорғанышы және қауіпсіздігі, деректердің тұтастығы және сенімділігі. Дерекқорды қорғау және қауіпсіздендіру әдістері және құралдары. Қауіпсіз дерекқорды жобалау. Жобалаудың CASE-құралдары. Дерекқордың әкімшелік ету құрал-саймандары. Көрсетімдемелер деректер қауіпсіздігін арттыру құралдары ретінде. Курсорлардың дерекқор қауіпсіздігіне әсері. Транзакцияларды басқару. Сақталатын процедуралар. Триггерлер. ДҚБЖ-де қатынас құруды мандаттық және дискрециондық басқару. Рольдер мен тіркеу жазбалары. ДҚБЖ-ға мониторинг және аудит. Дерекқорды қорғаудың криптографиялық құралдары. Дерекқорды қосалқылау және қалпына келтіру. Жоғарғы дайындықты қолдау құралдары.

Күтілетін нәтижелер: Дерекқорларды қорғауды және қауіпсіздендіруді ұйымдастыру кезінде білімдерді және оларды қолдану дағдыларын дамыту.

Постреквизиттер: Жасанды зерде әдістері, Білімдерді басқару, Экономикалық жүйелердің ақпараттық қауіпсіздігі, Электрондық бизнес жүйелерінің қауіпсіздігі

ASBS 5304.1, ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті, 3кр

Пререквизиттер: Дерекқорлардың қауіпсіздігі және сенімділігі, Дерекқорларды жобалау және қорғау, Ақпаратты криптографиялық қорғау әдістері мен құралдары, Ақпарат қорғау жүйелерін ұйымдастыру, Желілік ОЖ-дің қауіпсіздік құралдары, ОЖ-дегі қорғау әдістері және құралдары.

Оқыту мақсаты: ДҚ серверлерінің қауіпсіздік жүйелері сәулетінің негізгі қағиғаттарын менгеру.

Қысқаша мазмұны: ДҚ серверлері. Дерекқорларды қорғауды жүйелерін жобалаудағы жүйелік келес. Ақпараттық қауіпсіздігі саласындағы стандарттау және сертификаттау. ДҚ қауіпсіздігінің қауіптерін жіктеу. ДҚ қауіпсіздік жүйесінің сәулеті. Деректердің тұтастығы және сенімділігі. Дерекқорды жобалау технологиялары, нормалдау, жобалаудың ER-әдісі, жобалаудың CASE-құралдары. ДҚ қауіпсіздік жүйесіндегі көрсетілімдер және курсорлар. Қауіпсіздік жүйесіндегі транзакциялар және бұғаттаулар. ДҚБЖ-дегі сақталатын процедуралар және триггерлер. SQL-серверлердің қауіпсіздігінің логикалық жүйелері, қатынас құруды басқару, идентификация, аутентификация, авторландыру. Рольдер мен тіркеу жазбалары. ДҚБЖ-дегі тексерімдік бақылау, мониторинг және аудит. ДҚ серверлеріндегі криптография. Қосалқылау стратегиясы. Кластерлеу.

Күтілетін нәтижелер: Серверлердің қауіпсіздік жүйелерінің сәулеті жайындағы білімдерді, сондай-ақ ДҚ қорғауды және қауіпсіздендіруді қамтамасыз ету үшін оларды қолдану дағдыларын дамыту.

Постреквизиттер: Жасанды зерде әдістері, Білімдерді басқару, Экономикалық жүйелердің ақпараттық қауіпсіздігі, Электрондық бизнес жүйелерінің қауіпсіздігі

___2____
(оқу мерзімі)

№	Модуль атауы	Пән циклі	Пән коды	Пән атауы	Кредиттер саны	Семестр
1	Инженерлік-техникалық қорғау модулі	ПД	ASPU 6305	Ақпараттың сыртқа кету арналарын іздеудің және табудың аппараттық құралдары	3	1
1.1		ПД	ITZI 6305.1	Ақпаратты инженерлік-техникалық қорғау	3	1
1.2		ПД	SBIS 6306	Ақпарат қорғаудағы бағдарламаланатын логикалы АШИС	3	1
1.3		ПД	РМК 6306.1	Шағын контроллерді бағдарламалау	3	1
2	Қауіпсіздік модулі	БД	MII 6208	Жасанды зерде әдістері	3	1
2.1		БД	YZ 6208.1	Білімді басқару	3	1
2.2		ПД	SMIB 6307	Ақпараттық қауіпсіздіктің менеджмент жүйесі	3	1

2.3		ПД	YIB 6307.1	Ақпараттық қауіпсіздікті басқару	3	1
2.4		ПД	IBES 6308	Экономикалық жүйелердің ақпараттық қауіпсіздігі	2	1
2.5		ПД	BSEB 6308.1	Электрондық бизнес жүйелерінің қауіпсіздігі	2	1

(көрсетілген курста оқылатын әрбір элективті пәннің сипаттамасы)

ASPU 6305, Ақпараттың сыртқа кету арналарын іздеудің және табудың аппараттық құралдары, 3кр

Пререквизиттер: Ақпараттың ағу арнасын іздеу және табудың аппараттық құралдары пәні Электроника және сұбатехника, Цифрлық және аналогтық электроника және Ақпаратты қорғаудың техникалық құралдары пәндерінен алынған білімдерге негізделген.

Оқыту мақсаты: Ақпараттың активті ағу арнасын іздеу және табудың аппараттық құралдарының жұмыс істеу және пайдалану ерекшеліктерімен танысу; конфиденциалды ақпарат көзіне рұхсатсыз қатынауға тосқауыл қоятын және ақпаратты қорғауды қамтамасыз ететін әртүрлі аппартатық құралдардың техникалық мүмкіншіліктерімен және сипаттамаларымен танысу; әртүрлі обьектердегі және бөлмелердегі ақпараттың ағу арналарын анықтайтын аппараттық құрылғылармен танысу.

Қысқаша мазмұны:Ақпараттың активті ағу арнасын және сымсыз құрылғыларды іздеу және табудың аппараттық құралдары. Ақпаратты рұхсатсыз алатын радиотаратушы құрылғының орналасқан жерін анықтап табатын іздеуші қабылдағыш. Ақпараттың акустикалық ағу арналарының жіктелуі. Радиобақылаудың апараттық құралдары. Мекеме бастығының дыбыстық ақпаратын келушілердің жасырын жазып алуынан қорғау. Дыбыстық ақпараттың оптико-электрондық арна арқылы ағуынан қорғау. Аудио және бейне ақпаратты жасырын тарататын радио арналарын және бейне камераларын іздеу және табу құрылғылары. Цифрлы байланыс арналарындағы ақпаратты рұхсатсыз алатын электрондық құрылғыларды анықтау. Сымды қатынастықтардағы(коммуникациядағы) жоғары жиілікті сигналдарды және электромагниттік шашырауларды(излученияларды) бақылау құрылғылары.

Күтілетін нәтижелер: ақпаратты қорғауды қамтамасыз ететін әртүрлі аппартатық құралдардың техникалық мүмкіншіліктерін және сипаттамаларын білу қажет; ақпаратты қорғайтын аппарттық құрылғылардың жұмыс ерекшеліктерін және қолдану аймақтарын білу қажет; аппаратты құрылғыларды конфиденциалды ақпараттардың активті ағу арналарын іздеуге және табуға тиімді пайдалануды білу қажет.

Постреквизиттер: Ақпараттың ағу арнасын іздеу және табудың аппараттық құралдары пәні бойынша алынған білімдерді магистрлік диссертацияны орындау кезінде

және магистратураны бітіргеннен кейін мамандығы бойынша практикалық қызметте қолдануға болады.

ITZI 6305.1, Ақпаратты инженерлік-техникалық қорғау, 3кр

Пререквизиттер: Ақпаратты инженерлік-техникалық қорғау пәні Электроника және сұбатехника, Цифрлық және аналогтық электроника және Ақпаратты қорғаудың және қауіпсіздігінің аппартатық құралдары пәндерінен алынған білімдерге негізделген.

Оқыту мақсаты: ақпаратты қорғаудың техникалық құралдарының пайдалану ерекшеліктерімен танысу; обьекті қорғаудың физикалық құралдарымен және ақпараттың ағу арналарын іздеуге және табуға қажет аппарттық құралдармен танысу; активті және пассивті техникалық құралдарды пайдаланып ақпаратты қорғауға қажет жүргізілетін іс-шаралармен танысу; ақпаратты қабылдауға және таратуға қажет техникалық құралдармен танысу; «жоғары жиілікті қыстырмалау» (жоғары жиілікті сигналды ақпараттық сигналмен модуляциялау) арқылы ақпараттың техникалық ағу арнасымен танысу.

Қысқаша мазмұны:Ақпаратты инженерлік-техникалық қорғау (ИТҚ). Активті және пассивті техникалық құралдарды пайдаланып ақпаратты қорғауға қажет іс-шараларды жүргізу. Ақпаратты инженерлік-техникалық қорғауға қажет техникалық құралдар, олардың жіктелуі. Обьекті қорғаудың физикалық құралдары. Ақпараттың ағу арналарын іздеуге және табуға қажет аппарттық құралдар. Дыбыстық ақпараттың техникалық ағу арналары. Ақпаратты қабылдауға және таратуға қажет техникалық құралдар. Дыбысты ақпаратты рұқсатсыз алу құрылғысы. Телефондық "құлақ". Электрондық стетоскоп. Лазерлік микрофон. Лазерлік инфрақызыл сәулені терезе шынысына бағыттау арқылы бөлмедегі дыбыстық сигналдарды оптико-электрондық қабылдау. «Жоғары жиілікті қыстырмалау» арқылы ақпараттың техникалық ағу арнасы. Ақпараттың параметрлік техникалық ағу арналары.

Күтілетін нәтижелер: ақпаратты қорғаудың инженерлік-техникалық құралдарының пайдалану ерекшеліктерін білу қажет; ақпаратты қабылдауға және таратуға қажет техникалық құралдардың пайдалану ерекшеліктерін білу қажет; конфиденциалды ақпараттың активті ағу арнасын іздеуге және табуға арналған техникалық құралдарды тиімды пайдалануды білу қажет.

Постреквизиттер: Ақпаратты инженерлік-техникалық қорғау пәні бойынша алынған білімдерді магистрлік диссертацияны орындау кезінде және магистратураны бітіргеннен кейін мамандығы бойынша практикалық қызметте қолдануға болады.

SBIS 6306, Ақпарат қорғаудағы бағдарламаланатын логикалы АҮИС, 3кр

Пререквизиттер: Ақпаратты қорғауға қажет логикасы программаланатын АҮИС пәні Электроника және сұбатехника, Цифрлық және аналогтық электроника және Микроэлектроника пәндерінен алынған білімдерге негізделген

Оқыту мақсаты: программаланатын логикалық матрицалардың, программаланатын матрицалық логиканың және базалық матрицалық кристалдардың сұлбатехникасы және пайдалану енрекшеліктерімен танысу; құрылғылары күрделі прогаммаланатын жәәне қайта программаланатын қазіргі кездегі және келешегі зор АҮИС-термен танысу; логикасы программаланатын АҮИС-ң параметрлерімен, түрлерімен және олардың пішінін өзгерту мәселерімен танысу; программаланатын логикалық ИС-ң микропроцессорлық және есептеу техникасында, байланыс техникасында және ақпаратты қорғау үшін пайдалануымен танысу; программаланатын логикалы ИС-тің программалық қамтамалауды және құрылғыға рұхсатсыз қатынаудан және көшіруден қорғауға пайдалануымен танысу.

Қысқаша мазмұны: Программаланатын логикалық матрицалар. Программаланатын матрицалық логика. Базалық матрицалық кристалдар. Құрылымдары

күрделі программаланатын және қайта программаланатын аса үлкен интегралды сұлбалар (АҮИС). Пайдаланушымен программаланатын вентилді матрицы (FPGA). FPGA және логикасы программаланатын АҮИС-ң пайдалану аймақтары. Күрделі программаланатын логикалық сұлбалар(CPLD) және архитектурасы аралас логикасы программаланатын АҮИС. «Жүйе кристалда» типтес логикасы программаланатын АҮИС. Логикасы программаланатын АҮИС-ң параметрлері, түрлері және олардың пішінін өзгерту (конфигурирование). Программаланатын логикалық ИС-ң микропроцессорлық және есептеу техникасында, байланыс техникасында және ақпаратты қорғау үшін пайдалануы. Программаланатын логикалы ИС-ті программалық қамтамалауды және құрылғыға рұхсатсыз қатынаудан және көшіруден қорғауға пайдалану.

Күтілетін нәтижелер: программаланатын логикалық матрицалардың, программаланатын матрицалық логиканың және базалық матрицалық кристалдардың сұлбатехникасын және пайдалану енрекшеліктерін білу қажет; құрылғылары күрделі прогаммаланатын және қайта программаланатын қазіргі кездегі және келешегі зор АҮИС-тердің ерекшілікерін білу қажет; логикасы программаланатын АҮИС-ң параметрлерін, түрлерін және олардың пішінін өзгерту мәселерін білу қажет; программаланатын логикалық ИС-ң микропроцессорлық және есептеу техникасында, байланыс техникасында және ақпаратты қорғау үшін пайдалануын білу қажет; программаланатын логикалы ИС-тің программалық қамтамалауды және құрылғыға рұхсатсыз қатынаудан және көшіруден қорғауға пайдалануын білу қажет.

Постреквизиттер: Ақпаратты қорғауға қажет логикасы программаланатын АҮИС пәні бойынша алынған білімдерді магистрлік диссертацияны орындау кезінде және магистратураны бітіргеннен кейінгі практикалық қызметте пайдалана алады.

РМК 6306.1, Шағын контроллерді бағдарламалау, 3кр

Пререквизиттер: Есептеу жүйелерінің архитектурасы, Есептеу жүйелерін ұйымдастыру, Жүйелік бағдарламалаудың негіздері, Жүйелік бағдарламалау технологиялары

Оқыту мақсаты: Микробақылаушының қосымшалары қорында жүйенің операцияларын бағдарламалау құралдары және оқыту әдістері.

Қысқаша мазмұны: Микробақылаушының техникалық мінездемесі және бағдарламалық рұқсаталу құралдары. Енгізу/шығару порттарын бағдарламалау. Деректерді арифметикалық өңдеу. Сандарды ұсыну. Сандарды қосу және азайту. Сандарды көбейту және бөлу. Арифметикалық операцияларды бағдарламалау. Микробақылаушының таймері. Тізбектей интерфейсімен деректерді ауыстыру. Параллельді интерфейсімен енгізу/шығаруды ұйымдастыру. Өңдеу мен енгізу/шығаруды синхронды және асинхронды орындау. Аналогты сигналдарды салыстыру. Әмбебап тілдерде бағдарламалау және бағдарламаны тексеру.

Күтілетін нәтижелер: Үдеріс модельдерін құрастыру және микробақылаушының қосымшалары үшін бағдарламалар құру.

Постреквизиттер: магистирлік диссертация, докторантура пәндері

МП 6208, Жасанды зерде әдістері, 3кр

Пререквизиттер: ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, Ақпараттық қауіпсіздіктің жүйесін ұйымдастыру, Ақпаратты криптологиялық қорғау алгоритмдері

Оқыту мақсаты: студенттердің бойында жасанды зерде жүйелерін жобалаудың теориялық негіздері, жасанды зерде жүйелерін жобалау әдістері мен тәсілдері туралы түсінік қалыптастыру; жасанды зрде жүйелерінің көмегімен инновациялық әзірлемелердің тиімділігін көтеру мәселелерін шешуде творчестволық көзқарас қалыптастыру.

Қысқаша мазмұны: Жасанды зерде ғылыми бағыт ретінде. Жасанды зерденің облысы: зияткерлік ақпараттық-ізденіса жүйелері,есептік-логикалық жүйелер, сараптық жүйелер. Білімге негізделген жүйелер. Білімді көрсету модельдері. Жасанды зерделердегі білімді көрсету: Зерделік жүйелердегі білімді қалыптастыру, Формальды-логикалық модельдер, Анық емес логика, Продукциялық модельдер, Желілік модельдер. ЖЗ жүйелері мәселелерінің философиялық аспектілері (қолданылу мүмкіндігі, қауіпсіздік, пайдалалығы). Сараптық жүйелер әзірлеу. Концептуализациялау кезеңдер. Нейрондық желілер. Қателерді кері үлестіруді қамтитын нейрондық желі моделі. Хопфилд және Хэмминг нейрондық желілері. Потенциальды функциялар әдісі.

Күтілетін нәтижелер: Студент сараптыққ жүйелер құру технологиялары туралы жалпы мағлұматтарды, мәселелер шешімін іздеуде білімді пайдалана білу тәсілдерін иемдену керек. Студент білімді алып, қалыптастырып және оны зерделік жүйелерде көрсете білуі керек; күрделі емес сараптық жүйелер әзірлеп, түзетумен қатар, жасанды зерде жүйелерімен жұмыс тәжірибесін иемдену керек.

Постреквизиттер: магистирлік диссертация, докторантура пәндері

YZ 6208.1, Білімді басқару, 3кр

Пререквизиттер: ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, Ақпараттық қауіпсіздіктің жүйесін ұйымдастыру, Ақпаратты криптологиялық қорғау алгоритмдері

Оқыту мақсаты: Білімдер қорын, сараптық жүйелер және жасанды зерде жүйелерін құрудың теориялық негіздерін оқып, тәжірибе жүзінде іске асыруға үйрету, студенттерге жасанды зерде жүйелерін жобалау және экспуатациялауда қажетті оларды құру принциптері, әдістері мен құралдары туралы жүйелі білім беру, тәжірибелік машықтандыру.

Қысқаша мазмұны: Жасанды зерде жүйелерінің теориясына кіріспе; ЖЗЖ жобалау және әзірлеу технологиясы; Білімді алу және құрылымдау; білімді қалыптастыру; Білімге негізделген жүйелер. Білімді көрсету модельдері. Жасанды зерделердегі білімді көрсету: Зерделік жүйелердегі білімді қалыптастыру, Формальды-логикалық модельдер, Анық емес логика, Продукциялық модельдер, Желілік модельдер. ЖЗ жүйелері мәселелерінің философиялық аспектілері (қолданылу мүмкіндігі, қауіпсіздік, пайдалалығы). Сараптық жүйелер әзірлеу. Концептуализациялау кезеңдер. Нейрондық желілер. Қателерді кері үлестіруді қамтитын нейрондық желі моделі. Хопфилд және Хэмминг нейрондық желілері. Потенциальды функциялар әдісі.

Күтілетін нәтижелер: Студент сараптыққ жүйелер құру технологиялары туралы жалпы мағлұматтарды, мәселелер шешімін іздеуде білімді пайдалана білу тәсілдерін иемдену керек. Студент білімді алып, қалыптастырып және оны зерделік жүйелерде көрсете білуі керек; күрделі емес сараптық жүйелер әзірлеп, түзетумен қатар, жасанды зерде жүйелерімен жұмыс тәжірибесін иемдену керек

Постреквизиттер: магистирлік диссертация, докторантура пәндері

SMIB 6307, Ақпараттық қауіпсіздіктің менеджмент жүйесі, 3кр

Пререквизиттер: Желі қауіпсіздігін басқару, Ақпараттық қауіпсіздіктің жүйесін ұйымдастыру, Психо-ақпараттық әсерден қорғау.

Оқыту мақсаты: Ақпараттық қауіпсіздіктің менеджмент жүйесімен танысу; ақпараттық қауіпсіздіктің инциденттерін басқару аймағында негізгі түсініктер және принциптермен танысу; менеджмент жүйесінің құру концепциясы құрылымы және функционалдық ерекшеліктері.

Қысқаша мазмұны: Халықаралық стандарттарға сай ақпараттық қауіпсіздіктің менеджмент жүйесін басқару. Ақпараттық қауіпсіздіктің инциденттерін басқару саласындағы негізгі түсініктер мен принциптері. Ақпараттық қауіпсіздіктің

инциденттерін басқаруда орталықтардың құрылуы мен жұмысы. ISO 27035 және ISO 18044 халықаралық стандарттардың талаптарына сай ақпараттық қауіпсіздіктің инциденттер менеджментінің тиімді кезеңдері. Ақпараттық қауіпсіздіктің инциденттерінің тиімді менеджмент жүйесінің құрылуы, құрылымы және функционалды ерекшеліктері. Ақпараттық қауіпсіздіктің инциденттеріне жауап беру топтарының тиімді жұмыстарының құралдары. Ақпараттық қауіпсіздіктің инциденттерін басқару үрдісін құжаттармен қамтамасызету.

Күтілетін нәтижелер: ақпараттық қауіпсіздіктің инциденттерін басқару ерекшеліктерін білу қажет; ақпараттық қауіпсіздіктің инциденттеріне жауап беру топтарының тиімді жұмыстарының құралдарын басқару білу қажет.

Постреквизиттер: «Ақпараттық қауіпсіздіктің менеджмент жүйесі» пәні бойынша алынған білімдерді магистрлік диссертацияны орындау кезінде және магистратураны бітіргеннен кейінгі практикалық қызметте пайдалана алады.

<u>УІВ 6307.1, Ақпараттық қауіпсіздікті басқару, 3кр</u>

Пререквизиттер: Ақпаратты қорғау жүйелерін жобалау, Ақпаратты аналитикалық өңдеу, Желілердің хаттамалары мен стандарттары және оларды қорғау

Оқыту мақсаты: Халықаралық стандарттар талабымен ақпараттық қауіпсіздіктің менеджмент жүйесімен танысу; Халықаралық стандарттардың талабына сай инцидент-менеджменттің негізгі түсініктері, принциптері және кезеңдерімен танысу; менеджмент жүйесінің функционалдық ерекшеліктері.

Қысқаша мазмұны: халықаралық стандарттардың талаптарына сай ақпараттық қауіпсіздіктің инциденттерін тиімді басқару. Ақпараттық қауіпсіздікті басқару саласындағы базалық терминдер, анықтамалар, түсініктер және принциптер. Ақпараттық қауіпсіздіктің инциденттерін басқару үшін стандарттар мен ұсыныстар. CERT/ CSIRT топтарымен шабуылдарды анықтау және басып кіруді тану. Ақпараттық қауіпсіздіктің инциденттерінің әсерін болдырмау және жою. Бұзушының идентификациясы және ақпараттық қауіпсіздіктің инциденттерінен болған зардапты бағалау. Ақпараттық қауіпсіздіктің инциденттеріне жауап беру топтарының тиімді жұмыстарының құралдары. Ақпараттық қауіпсіздіктің инциденттерін басқару үрдісін құжаттармен қамтамасызету.

Күтілетін нәтижелер: ақпараттық қауіпсіздікті басқару саласындағы негізгі терминдер, түсініктер мен принциптерді білу қажет; ақпараттық қауіпсіздіктің инциденттеріне жауап беру; бұзушыны анықтау

Постреквизиттер: магистирлік диссертация, докторантура пәндері

<u>IBES 6308, Экономикалық жүйелердің ақпараттық қауіпсіздігі, 2кр</u>

Пререквизиттер: Желілік ОЖ-дің қауіпсіздік құралдары, Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Ақпаратты қорғаудың криптологиялық әдістері мен құралдары, ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті.

Оқыту мақсаты: Экономикалық жүйелердің ақпараттық қауіпсіздіктің негізгі теориялық аймақтарында білімдерін жинақтау; ақпаратты қорғауды қамтамасызетудің тәжребиелік білімдерін игеру және экономикалық жүйелерде бағдарламалық құралдарды қауіпсіз қолдану.

Қысқаша мазмұны: Экономикалық ақпарат қауіпсіздік объектісі және тауары ретінде. Интернетте экономикалық әрекеттер. Экономикалық ақпараттық жүйелерінде қауіпсіздік қауіп түрлері. Қауіпсіздік саясаты. Ақпаратқа рұқсатсыз қатынас құрудың негізгі жолдары. Экономикалық жүйелерде қолданатын қорғау құралдары мен әдістері, оларды жіктеу. Ақпаратты қорғаудың аппаратты құралдары. Ақпарат ағу арналарын табу құралдары. Желіаралық экрандар. Шабуылдарды табу жүйелері. DLP-жүйелері. Залал акелетін бағдарламалар. Деректерді қалпына келтіру және қосалқылау жүйелері.

Криптографиялық жүйелері. Дерекқорларды қорғау. Деректердің қауіпсіздігі және бұлттық технологиялар.

Күтілетін нәтижелер: Экономикалық жүйелерінің негізгі түсініктерін игеру, қорғалған экономикалық жүйелердің сәулетін.

Постреквизиттер: магистирлік диссертация, докторантура пәндері

BSEB 6308.1, Электрондық бизнес жүйелерінің қауіпсіздігі, 2кр

Пререквизиттер: ОЖ қорғау әдістері мен құралдары, Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Ақпаратты криптологиялық қорғау алгоритмдері, ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру.

Оқыту мақсаты: электронды бизнес жүйелерінің түсініктерімен танысу, электрондық бизнестегі қауіпсіздік және қатерлер сұрақтары.

Қысқаша мазмұны: Электронды бизнестің түсініктері. Электронды бизнеста қауіпсіздік қауіптерінің түрлері.. Идентификация, аутенфикация және авторландыру. Клиенттің әрекеттерінің шынайлығын растау. Ақпаратты жолай ұстаудан қорғау. Жалған ақпаратты таңуға қарсылық білдіру. Сыртқы шабуылдарды істен шығару. Желіаралық экрандау. Басып кірулерді анықтау жүйелері. Басып кіруді болдырмау жүйелері. Залалды контенттің ішке кірунен қорғау жүйелері. Қорғалатын қорларға дискреционды қ және мандатты қол жеткізуді басқару. Автоматтандырылған банктік жүйелер үшін ақпараттық қауіпсіздікті қамтамасыз ету. Электронды коммерцияның ақпараттық қауіпсіздігі.

Күтілітін нәтижелер: Электронды бизнес жүйелерінің негізгі түсініктерін игеру. Қауіптерге қарсылық білдіретін заманауи құралдарын және әдістерін қолдана білу.

Постреквизиттер: магистирлік диссертация, докторантура пәндері

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И.САТПАЕВА

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН СПЕЦИАЛЬНОСТИ 6М100200 - СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Каталог элективных дисциплин утвержден научно-методическим советом Казахского национального исследовательского технического университета имени К.И. Сатпаева (протокол №5 от «15» июня 2015 г). Алматы, КазНИТУ, 2015.

Каталог включает в себя перечень элективных дисциплин (компонента по выбору) специальности, пререквизиты и постреквизиты дисциплин, цель изучения дисциплины, их краткое содержание, ожидаемые результаты.

ПАМЯТКА ОБУЧАЮЩЕМУСЯ И ЭДВАЙЗЕРУ

Все учебные дисциплины специальности бакалавриата делятся по циклам (ООД, БД, ПД), магистратуры и докторантуры (БД,ПД), модулям, внутри которых они разделяются на обязательные и элективные (по выбору) дисциплины. Перечень обязательных для изучения дисциплин приводится в типовом учебном плане специальности (ТУПл). Перечень элективных дисциплин для каждого курса специальности представляется в каталоге элективных дисциплин (КЭД), который является систематизированным аннотированным перечнем дисциплин по выбору специальности. КЭД должен давать (обеспечивать) обучающимся возможность альтернативного выбора элективных учебных дисциплин в соответствии с выбранной траекторией обучения.

На основании ТУПл и КЭД формируется индивидуальный учебный план (ИУП) обучающегося на учебный год. Помощь бакалаврам и магистрантам при составлении ИУП оказывает эдвайзер, назначенный выпускающей кафедрой. Докторанты ИУП составляют самостоятельно. ИУП определяет индивидуальную образовательную траекторию каждого обучающегося в рамках специальности. В ИУП включаются дисциплины обязательного компонента и виды учебной деятельности (практики, исследовательская работа, государственный (комплексный) экзамен, написание и защита дипломной работы (проекта), диссертации) из ТУПл и дисциплины компонента по выбору из КЭД.

В помощь бакалаврам образовательной траектории, ориентированной на конкретную сферу деятельности с учетом потребностей рынка труда и работодателей, в рамках КЭД должен быть представлен перечень дисциплин, гарантирующий обучающимся целенаправленное освоение намеченной образовательной программы.

При выборе элективных дисциплин необходимо учитывать следующее:

1 В одном семестре студент очной формы обучения должен освоить 18-22 кредита (обязательных и элективных), дистанционной формы – 9-12 кредитов (обязательных и элективных), без учета дополнительных видов обучения (ДВО), которые являются обязательными для изучения.

2 Общее количество кредитов за весь период обучения не должно превышать указанное в ТУПл специальности количество.

3 Элективные дисциплины объединены в группы по выбору с соответствующим номером. Из каждой группы дисциплин можно выбрать только одну элективную учебную дисциплину.

Академическая степень: магистр военных наук

_____1_____
(курс обучения)

№	Наименование модуля	Цикл дисциплины	Код дисциплины	Наименование дисциплины	Кол-во кредитов	Семестр
1	Модуль организации систем безопасности	БД	SBS 5205	Средства безопасности сетевых ОС	3	1
1.1		БД	MSZ 5205.1	Методы и средства защиты в ОС	3	1
2	Модуль высокопроизводительных технологии	БД	APVS 5206	Архитектура параллельных вычислительных систем	3	1
2.1		БД	VTVS 5206.1	Высокопроизводительные технологии в вычислительных системах	3	1
2.2		БД	PaV 5207	Параллельные вычисления и защита информации	3	2
2.3		БД	MPV 5207.1	Методы параллельных вычислений в защите информации	3	2
3	Модуль защиты	ПД	PSSZ 5302	Протоколы и стандарты сетей и их защиты	3	2
3.1		ПД	YBS 5302.1	Управление безопасностью сети	3	2
3.2		ПД	KMZI 5303	Криптологические методы и средства защиты информации	3	2
3.3		ПД	AKZI 5303.1	Алгоритмы криптографической защиты информации	3	2

3.4		ПД	OZBD 5304	Организация защиты и безопасности БД	3	2
3.5		ПД	ASBS 5304.1	Архитектура систем безопасности серверов БД	3	2

(описание каждой элективной дисциплины, изучаемой на указанном курсе)

SBS 5205, Средства безопасности сетевых ОС, 3кр

Пререквизиты: Организация операционных систем, Методы и средства защиты компьютерной информации.

Цель изучения: Знание принципов построения систем защиты информации (СЗИ) в сетевых операционных системах (ОС); средств и методов несанкционированного доступа (НСД) к ресурсам ОС.

Краткое содержание: Основы обеспечения информационной безопасности сетевых ОС. Защита от изменения и контроль целостности программного обеспечения**.** Методы и средства хранения ключевой информации. Принципы многофакторной аутентификации. Технические устройства идентификации и аутентификации. Парольные подсистемы идентификации и аутентификации. Идентификация и аутентификация пользователей с помощью биометрических устройств. Программно-аппаратные средства шифрования. Безопасность сетевых операционных систем. Обеспечение безопасности в системах Windows, Unix. Системы обнаружения вторжений. Основные компоненты архитектуры межсетевых экранов. Современные требования к межсетевым экранам.

Ожидаемые результаты: Оценивать эффективность и надежность защиты сетевых ОС. Умение администрирования современных сетевых ОС. Использование межсетевых экранов и систем обнаружения вторжений.

Постреквизиты: Управление безопасностью сети, магистерская диссертация

MSZ 5205.1, Методы и средства защиты в ОС, 3 кр

Пререквизиты: Организация операционных систем, Методы и средства защиты компьютерной информации

Цель изучения: Изучение принципов построения защиты информации в ОС и анализа надежности защиты ОС. Средства и методы несанкционированного доступа к ресурсам ОС.

Краткое содержание: Основные понятия и положения защиты информации в операционных системах. Угрозы безопасности информации в информационно-вычислительных системах. Угрозы безопасности ОС. Требования к защите ОС. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix, Mac OS. Статистика методов, лежащих в основе атак на современные ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Разграничение доступа к ресурсам в ОС Windws, Unix, Mac OS. Аудит в ОС. Системы защиты программного обеспечения.

Ожидаемые результаты: Знание критериев оценки эффективности и надежности средств защиты ОС. Планирование политики безопасности ОС. Оценивание механизмов защиты ОС.

Постреквизиты: Управление безопасностью сети, магистерская диссертация

APVS5206 Архитектура параллельных вычислительных систем, 3кр

Пререквизиты: Прикладная теория цифровых автоматов, Схематехника ЭВМ, Организация вычислительных машин.

Цель изучения: Изучить методов параллельных обработки и закономерности параллельных вычислении для построения высокопродуктивных вычислительных систем.

Краткое содержание: Уровни параллелизма, метрика параллельных вычислении, закономерности параллельного вычислении. Классификация параллельных вычислительных систем. Организация памяти ВС, топология ВС. Вычислительные системы класса SIMD: векторные, матричные, ассоциативные ВС и ВС на основе и систематических процессоров. ВС класса MIMD. Много процессорные ВС: SMR система, PVP-системы и ВС с неоднородным доступом к памяти. Много компьютерные ВС класса MIMD: MPP- система, кластерные ВС на базе транспортеров.

Ожидаемые результаты: Развитие знаний по методам построении ВС различного класса, а также приобретение навыков их эффективного применения для решения различных задач.

Постреквизиты: Параллельные вычисления и защита информации, Методы параллельных вычислений в защите информации

VTVS5206.1 Высокопроизводительные технологии в вычислительных системах, 3кр

Пререквизиты: Схематехника ЭВМ, Прикладная теория цифровых автоматов, Архитектура вычислительных машин.

Цель изучения: Изучить существующих технологии основанных на параллелизме для разработки высокопроизводительных вычислительных систем.

Краткое описание: технологии вычисления на основе параллелизма законы параллельных вычислении. Классификация высокопроизводительных вычислителей организация памяти ВС. Векторные, матричные, ассоциативные, систематические ВС, на основе мультипроцессоров. Вычислительные системы на основе мультикопьютеров: MPP, кластерные ВС, ВС на базе транспортеров.

Ожидаемые результаты: Развитие знаний в области вычислительных систем, построенных на базе высокопроизводительных технологий, а также приобретение навыков по их изменению для решения различных задач.

Постреквизиты: Параллельные вычисления и защита информации, Методы параллельных вычислений в защите информации

PaV 5207, Параллельные вычисления и защита информации, 3кр

Пререквизиты: Организация операционных систем

Цель изучения: Применение принципов параллельной обработки информации при криптоанализе симметричных и ассиметричных криптосистем.

Краткое содержание: Основные принципы параллельных вычислений. Виды параллелизмов вычислительных задач.Способы параллельных вычислений. Повышение производительности вычислительных средств. Использование принципов распределенных многопроцессорных вычислений(PMB). Современные прикладные программы кластерных вычислительных систем. Анализ симметричных алгоритмов шифрования. Применение интерфейса MPI для создания средств параллельной обработки информации. Применение методов дифференциального анализа для алгоритмов криптозащиты. Проблемы защиты параллельных распределенных вычислений.

Ожидаемые результаты: Использовать принципы параллельной распределенной обработки информации для решения проблем защиты информации.

Постреквизиты: Криптологические методы и средства защиты информации, Алгоритмы криптографической защиты информации

MPV 5207.1, Методы параллельных вычислений в защите информации, 3кр

Пререквизиты: Организация операционных систем

Цель изучения: Применение методов параллельной обработки информации при создании систем защиты информации.

Краткое содержание: Основные методы параллельных вычислений. Виды параллелизмов вычислительных задач.Способы параллельных вычислений. Повышение производительности вычислительных средств. Использование принципов распределенных многопроцессорных вычислений(PMB). Современные прикладные программы кластерных вычислительных систем. Анализ симметричных алгоритмов шифрования. Применение интерфейса MPI для создания средств параллельной обработки информации. Применение методов дифференциального анализа для алгоритмов криптозащиты. Проблемы защиты параллельных распределенных вычислений. Защита распределенных параллельных вычислительных систем.

Ожидаемые результаты: Использовать принципы параллельной распределенной обработки информации для решения проблем защиты информации.

Постреквизиты: Криптологические методы и средства защиты информации, Алгоритмы криптографической защиты информации

PSSZ 5302, Протоколы и стандарты сетей и их защиты, 3кр

Пререквизиты: Средства безопасности сетевых ОС, Методы и средства защиты в ОС, Организация систем информационной безопасности, Криптологические методы и средства защиты информации

Цель изучения: Приобретение знаний в вопросах протоколов, стандартов, архитектуры и принципов работы компьютерных сетей, а также безопасности передачи информации по сети.

Краткое содержание: Современное состояние компьютерных сетей. Протоколы, соответствующие уровням модели OSI. Аппаратные средства сетей. Базовые технологии (архитектуры) локальных сетей. Глобальные сети и технологии глобальных сетей. Структура защищенной корпоративной сети. Протоколы безопасности сетей. Виртуальные сети. Высокоскоростные локальные сети и их будущее. Перспективы беспроводной связи. Технологии беспроводных коммуникаций. Основные концепции и возможности беспроводных ячеистых сетей. Беспроводной Интернет. Безопасность передачи информации по сети. Основные направления развития средств защиты информации в компьютерных сетях.

Ожидаемые результаты: Развитие знаний по протоколам и стандартам компьютерных сетей, защите информации в сетях, а также навыков по их применению.

Постреквизиты: Аппаратные средства поиска и обнаружения каналов утечки информации, Инженерно-техническая защита информации.

YBS 5302.1, Управление безопасностью сети, 3кр

Пререквизиты: Криптологические методы и средства защиты информации, Алгоритмы криптографической защиты информации, Организация защиты и безопасности БД, Архитектура систем безопасности

Цель изучения: Усвоение архитектуры сетевой системы защиты, протоколов безопасности, оптимального управления процессами защиты, политики информационной безопасности.

Краткое содержание: Протоколы, соответствующие уровням модели OSI. Технологии обеспечения информационной безопасности в современных сетях. Протоколы безопасности IPSec, PPTP, L2TP, SSL. Виртуальные сети. Организация передачи данных через защищенные каналы. Назначение, принцип работы, преимущества и недостатки межсетевых экранов (брандмауэры, firewall). Назначение и разновидности систем IDS, WIDS и IPS. Антивирусная защита. Многофункциональные устройства защиты. Механизмы защиты данных в беспроводных сетях

Ожидаемые результаты: Развитие знаний и навыков управления безопасностью компьютерной сети.

Постреквизиты: Системы менеджмента информационной безопасности, Безопасность систем электронного бизнеса.

KMZI 5303, Криптологические методы и средства защиты информации, 3кр

Пререквизиты: Математические основы криптографии, Математика криптографии и шифрования, Методы параллельных вычислений в защите информации, Параллельные вычисления и защита информации

Цель изучения: Знание алгоритмов шифрования, умение реализовывать стандартные криптосистемы на языке программирования, навыки комбинирования различных методов защиты информации.

Краткое содержание: Современная криптография и задачи, связанные с проблемами защиты информации. Формальное определение криптосистемы. Классические криптосистемы. Основные задачи криптоанализа. Поточное шифрование. Криптосистемы с открытым ключом. Применения математического моделирования в криптографии. Достоинства и недостатки различных систем. Теоремы Эйлера и Ферма. Управление ключами, Система без передачи ключа. Проблема разложения на простые множители. Проблема дискретного логарифмирования. Проблема криптостойкости. Системы защиты информации, схемы электронной подписи, протоколы аутентификации и идентификации.

Ожидаемые результаты: Магистрант должен знать основы криптографии, методы криптоанализа, уметь применять методы криптоанализа и математического моделирования при решении задач на защиту информации, иметь навыки качественного анализа полученных результатов.

Постреквизиты: Управление информационной безопасностью, Информационная безопасность экономических систем

AKZI 5303.1, Алгоритмы криптографической защиты информации, 3кр

Пререквизиты: Математические основы криптографии, Математика криптографии и шифрования, Методы параллельных вычислений в защите информации, Параллельные вычисления и защита информации

Цель изучения: Знание алгоритмов шифрования, умение реализовывать стандартные криптосистемы на языке программирования, навыки комбини-рования различных методов защиты информации.

Краткое содержание: Современная криптография и задачи, связанные с проблемами защиты информации. Формальное определение криптосистемы. Классические криптосистемы. Основные задачи криптоанализа. Поточное шифрование. Криптосистемы с открытым ключом. Применения математического моделирования в криптографии. Достоинства и недостатки различных систем. Теоремы Эйлера и Ферма. Управление ключами. Система без передачи ключа. Проблема разложения на простые множители. Проблема дискретного логарифмирования. Проблема криптостойкости.

Системы защиты информации, схемы электронной подписи, протоколы аутентификации и идентификации.

Ожидаемые результаты: Магистрант должен знать основы криптографии, методы криптоанализа, уметь применять методы криптоанализа и математического моделирования при решении задач на защиту информации, иметь навыки качественного анализа полученных результатов.

Постреквизиты: Безопасность систем электронного бизнеса, Информационная безопасность экономических систем

OZBD 5304, Организация защиты и безопасности БД, 3кр

Пререквизиты: Безопасность и надежность баз данных, Проектирование и защита баз данных, Методы и средства криптографической защиты информации, Организация систем защиты информации, Средства безопасности сетевых ОС, Методы и средства защиты в ОС.

Цель изучения: Усвоение базовых принципов организации защиты и обеспечения безопасности баз данных.

Краткое содержание: Аспекты и критерии безопасности БД, политика безопасности. Угрозы безопасности БД. Защита и безопасность БД, целостность и надежность данных. Методы и средства защиты и безопасности БД. Проектирование безопасных баз данных. CASE-средства проектирования. Инструменты администрирования БД. Представления как средства повышения безопасности данных. Влияние курсоров на безопасность БД. Управление транзакциями. Хранимые процедуры. Триггеры. Мандатное и дискреционное управление доступом в СУБД. Роли и учетные записи. Мониторинг и аудит в СУБД. Криптографические средства защиты БД. Резервирование и восстановление БД. Средства поддержания высокой готовности.

Ожидаемые результаты: Развитие знаний и навыков их применения при организации защиты и безопасности баз данных

Постреквизиты: Методы искусственного интеллекта, Управление знаниями, Информационная безопасность экономических систем, Безопасность систем электронного бизнеса

ASBS 5304.1, Архитектура систем безопасности серверов БД, 3кр

Пререквизиты: Безопасность и надежность баз данных, Проектирование и защита баз данных, Методы и средства криптографической защиты информации, Организация систем защиты информации, Средства безопасности сетевых ОС, Методы и средства защиты в ОС.

Цель изучения: Усвоение базовых принципов архитектуры систем безопасности серверов БД.

Краткое содержание: Серверы БД. Системный подход к проектированию систем защиты БД. Стандартизация и сертификация в области информационной безопасности. Классификация угроз безопасности БД. Архитектура системы защиты БД. Целостность и надежность данных. Технологии проектирования баз данных, нормализация, ER-метод проектирования, CASE-средства проектирования. Представления и курсоры в системе безопасности БД. Транзакции и блокировки в системе безопасности. Хранимые процедуры и триггеры в СУБД. Логические системы безопасности SQL-серверов, управление доступом, идентификация, аутентификация, авторизация. Роли и учетные записи. Контрольное слежение в СУБД, мониторинг и аудит. Криптография в серверах БД. Стратегии резервирования. Кластеризация.

Ожидаемые результаты: Развитие знаний по архитектуре систем безопасности серверов и навыков их применения для обеспечения защиты и безопасности баз данных

Постреквизиты: Методы искусственного интеллекта, Управление знаниями, Информационная безопасность экономических систем, Безопасность систем электронного бизнеса

_____2_____
(курс обучения)

№	Наименование модуля	Цикл дисциплины	Код дисциплины	Наименование дисциплины	Кол-во кредитов	Семестр
1	Модуль инженерно-технической защиты	ПД	ASPU 6305	Аппаратные средства поиска и обнаружения каналов утечки информации	3	1
1.1		ПД	ITZI 6305.1	Инженерно-техническая защита информации	3	1
1.2		ПД	SBIS 6306	СБИС программируемой логики в защите информации	3	1
1.3		ПД	PMK 6306.1	Программирование микроконтроллеров	3	1
2	Модуль безопасности	БД	MII 6208	Методы искусственного интеллекта	3	1
2.1		БД	YZ 6208.1	Управления знаниями	3	1
2.2		ПД	SMIB 6307	Системы менеджмента информационной безопасности	3	1

2.3		ПД	YIB 6307.1	Управление информационной безопасностью	3	1
2.4		ПД	IBES 6308	Информационная безопасность экономических систем	2	1
2.5		ПД	BSEB 6308.1	Безопасность систем электронного бизнеса	2	1

(описание каждой элективной дисциплины, изучаемой на указанном курсе)

ASPU 6305, Аппаратные средства поиска и обнаружения каналов утечки информации, 3кр

Пререквизиты: Электроника и схемотехника, Цифровая и аналоговая электроника и Технические средства защиты информации.

Цель изучения: ознакомление с особенностями принципов действия и применения аппаратных средств для поиска и обнаружения активных каналов утечки информации; ознакомление с техническими возможностями и характеристиками различных аппаратных средств, обеспечивающих защиту информации от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации; ознакомление с аппаратными средствами выявления каналов утечки информации на разных объектах и в помещениях.

Краткое содержание: Аппаратные средства поиска и обнаружения активных каналов утечки информации и беспроводных устройств. Поисковый приемник для обнаружения и определения местоположения радиопередающих устройств негласного получения информации. Классификация акустических каналов утечки информации. Аппаратные средства радиоконтроля. Защита речевой информации руководителя организации от скрытой записи посетителем. Защита акустической информации от утечки по оптико-электронному каналу. Устройства поиска и выявления скрытых видеокамер и радиоканалов передачи аудио- и видеоинформации. Аппаратные средства выявления электронных устройств негласного получения информации в каналах цифровой связи. Устройства контроля электромагнитных излучений и высокочастотных сигналов в проводных коммуникациях

Ожидаемые результаты: должны знать технические характеристики и возможности различных аппаратных средств защиты информации; знать особенности работы и области применения аппаратных средств защиты информации; уметь эффективно их использовать для поиска и обнаружения активных каналов утечки конфиденциальной информации.

Постреквизиты: Написание магистрской диссертации, а также после окончания магистратуры на практической работе по специальности.

ITZI 6305.1, Инженерно-техническая защита информации, 3кр

Пререквизиты: Электроника и схемотехника, Цифровая и аналоговая электроника и Аппаратные средства защиты и безопасности информации.

Цель изучения: Ознакомление с особенностями применения технических средства защиты информации; ознакомление с особенностями физических средств защиты объектов и аппаратных средств поиска и выявления каналов утечки информации; ознакомление с техническими мероприятиями по защите информации с применением пассивных и активных технических средств; ознакомление с техническими средствами приема и передачи информации; ознакомление с техническими каналами утечки информации путем «высокочастотного навязывания» (модуляции высокочастотного сигнала информационным).

Краткое содержание: Инженерно-техническая защита (ИТЗ) информации. Мероприятия по защите информации с применением пассивных и активных технических средств. Технические средства ИТЗ информации, классификация. Физические средства защиты объектов. Аппаратные средства поиска и выявление каналов утечки информации. Технические каналы утечки акустической информации. Технические средства приема и передачи информации. Закладные устройства перехвата речевой информации. Телефонное ухо. Электронные стетоскопы. Лазерные микрофоны. Оптико-электронный перехват акустических сигналов путем лазерного зондирования оконных стекол. Технический канал утечки информации путем «высокочастотного навязывания». Параметрические технические каналы утечки информации.

Ожидаемые результаты: должны знать особенности применения инженерно-технических средств защиты информации; знать технические характеристики и возможности различных технических средств приема и передачи информации; уметь эффективно использовать технические средства для поиска и обнаружения активных каналов утечки конфиденциальной информации.

Постреквизиты: Написание магистрской диссертации, а также после окончания магистратуры на практической работе по специальности.

SBIS 6306, СБИС программируемой логики в защите информации, 3кр

Пререквизиты: Электроника и схемотехника, Цифровая и аналоговая электроника и Микроэлектроника.

Цель изучения: ознакомление с особенностями схемотехники и применения программируемых логических матриц, программируемой матричной логики, базовых матричных кристаллов; ознакомление с современными и перспективными СБИС со сложными программируемыми и репрограммируемыми структурами; ознакомление с параметрами, семействами и конфигурированием СБИС программируемой логики; ознакомление с возможностями применения программируемых логических ИС (ПЛИС) в микропроцессорной и вычислительной технике и для защиты информации; изучение возможности применения ПЛИС для защиты программного обеспечения и аппаратуры от несанкционированного доступа и копирования.

Краткое содержание: Программируемые логические матрицы. Программируемая матричная логика. Базовые матричные кристаллы. СБИС со сложными программируемыми и репрограммируемыми структурами. Программируемые пользователем вентильные матрицы (FPGA). Области применения FPGA и СБИС программируемой логики (ПЛ). Сложные программируемые логические схемы (CPLD) и СБИС программируемой логики смешанной архитектуры. СБИС программируемой логики типа «система на кристалле». Параметры, семейства и конфигурирование СБИС программируемой логики. Применение программируемых логических ИС в микропроцессорной и вычислительной технике, технике связи и для защиты информации.

Применение ПЛИС для защиты программного обеспечения и аппаратуры от несанкционированного доступа и копирования.

Ожидаемые результаты: должны знать особенности схемотехники и применения программируемых логических матриц, программируемой матричной логики, базовых матричных кристаллов; знать особенности современных СБИС со сложными программируемыми и репрограммируемыми структурами; знать параметры, семейства и возможности конфигурирования СБИС программируемой логики; знать возможности применения программируемых логических ИС (ПЛИС) в микропроцессорной и вычислительной технике и для защиты информации; знать возможности применения ПЛИС для защиты программного обеспечения и аппаратуры от несанкционированного доступа и копирования.

Постреквизиты: написание магистрской диссертации, а также после окончания магистратуры на практической работе по специальности.

РМК 6306.1, Программирование микроконтроллеров, 3кр

Пререквизиты: Архитектура вычислительных систем, Организация вычислительных систем, Основы системного программирования, Технологии системного программирования

Цель изучения: Изучение методов и средств программирования операций в системах на базе микроконтроллерных приложений.

Краткое содержание: Технические характеристики и программно-доступные средства микроконтроллера. Программирование портов ввода/вывода. Арифметическая обработка данных. Представление чисел. Сложение и вычитание чисел. Умножение и деление чисел. Программирование арифметических операций. Таймеры микроконтроллеров. Обмен данными по последовательному интерфейсу. Организация ввода/вывода по параллельному интерфейсу. Синхронное и асинхронное выполнение ввода/вывода и обработки. Обработка аналоговых сигналов. Аналого-цифровое преобразование. Аналоговое сравнение сигналов. Программирование и отладка программ на универсальных языках

Ожидаемые результаты: Разработка моделей процессов и составления программ для микроконтроллерных приложений.

Постреквизиты: написание магистрской диссертации, дисциплины докторантуры

МІІ 6208, Методы искусственного интеллекта, 3кр

Пререквизиты: Организация защиты и безопасности БД, Организация систем информационной безопасности, Алгоритмы криптографической защиты информации.

Цель изучения: Формирование знаний теоретических основ проектирования систем искусственного интеллекта, формирование у студентов творческого подхода к решению проблем безопасности информации с помощью систем искусственного интеллекта.

Краткое содержание: Искусственный интеллект как научное направление. Системы, основанные на знаниях. Модели представления знаний. Представление знаний в системах искусственного интеллекта. Формализация знаний в интеллектуальных системах. Модели представления знаний. Фреймовые и сетевые модели. Логическое представление знаний и продукционные системы. Правила логического вывода. Поиск решений в пространстве состояний. Нечеткая логика. Экспертные системы, этапы разработки экспертных систем. Системы интеллектуального интерфейса. Системы распознавания и генерации речи. Системы технического зрения и генерации изображений. Нейронные сети.

Ожидаемые результаты Знание основных понятий искусственного интеллекта и форм представления знаний. Умение формализовать знания и представлять их в интеллектуальных системах, разрабатывать несложные экспертные системы.

Постреквизиты: магистерская диссертация, дисциплины докторантуры

YZ 6208.1, Управления знаниями, 3кр

Пререквизиты: Организация систем информационной безопасности, Криптологические методы и средства защиты информации, Архитектура систем безопасности серверов БД.

Цель изучения: Обучение студентов систематизированным знаниям о принципах, методах и средствах построения систем управления знаниями, приобретению практических навыков по созданию систем искусственного интеллекта, экспертных систем.

Краткое содержание: Системы, основанные на знаниях, системы искусственного интеллекта (СИИ). Базы знаний. Формализация знаний, декларативные и процедурные модели представления знаний. Продукционные системы. Правила логического вывода. Поиск решений в пространстве состояний. Представление и использование нечетких знаний. Экспертные системы, этапы разработки экспертных систем. Инженерия знаний и технология разработки ЭС. Методы извлечения знаний. Инструментальные средства систем управления знаний. Системы интеллектуального интерфейса. Системы распознавания и генерации речи. Системы технического зрения и генерации изображений. Искусственные нейронные сети.

Ожидаемые результаты: Знание основных понятий управления знаниями и форм представления знаний. Умение формализации и представления знаний, разработки простых экспертных систем.

Постреквизиты: магистерская диссертация, дисциплины докторантуры

SMIB 6307, Системы менеджмента информационной безопасности, 3кр

Пререквизиты: Управление безопасностью сети, Организация систем защиты информации, Защита от психо-информационного воздействия.

Цель изучения: ознаокмление с системой менеджмента информационной безопасности; с основными понятиями и принципами в сфере управления инциндентами ИБ; с концепциями построения, структурой и функциональными особенностями системы менеджмента.

Краткое содержание: Управление системой менеджмента информационной безопасности по требованиям международных стандартов. Основные понятия и принципы в сфере управления инцидентами информационной безопасности. Создание и функционирование центров управления инцидентами информационной безопасности. Этапы эффективного менеджмента инцидентов информационной безопасности по требованиям международных стандартов ISO 27035 и ISO 18044. Концепция построения, структура и функциональные особенности эффективной системы менеджмента инцидентов ИБ. Инструментарий для эффективного функционирования групп реагирования на инциденты ИБ. Документационное обеспечение процесса управления инцидентами ИБ.

Ожидаемые результаты: Должны знать особенности управления инциндентами информационной безопасности; управлять инструментариями для эффективного функционирования групп реагирования на инцинденты ИБ.

Постреквизиты: теоретические знания, полученные при изучении дисциплины «Системы менеджмента информационной безопасности» могут быть полезны при написании магистрской диссертации, а также после окончания магистратуры на практической работе по специальности.

YIB 6307.1, Управление информационной безопасностью, 3кр

Пререквизиты: Проектирование системы защиты и безопасности информации, Аналитическая обработка информации, Протоколы и стандарты сетей и их защиты

Цель изучения: ознаокмление с системой менеджмента информационной безопасности по требованиям международных стандартов; ознакомление с сновными понятиями, принципами и этапами инцидент-менеджмента согласно требованиям международного стандарта; с функциональными особенностями системы менеджмента.

Краткое содержание: Эффективное управление инцидентами информационной безопасности по требованиям международных стандартов. Базовые термины, определения, понятия и принципы в сфере управления информационной безопасности. Стандарты, рекомендации по управлению инцидентами информационной безопасности. Обнаружение атак и распознавание вторжений группами CERT/ CSIRT. Локализация и устранение последствий инцидентов информационной безопасности. Идентификация нарушителей и оценка ущерба от инцидентов информационной безопасности. Устранение негативных последствий инцидентов и возобновление работы информационных систем. Документационное обеспечение процесса управления инцидентами ИБ. Деятельность групп реагирования на инциденты ИБ.

Ожидаемые результаты: знать основные термины, понятия и принципы в сфере управления информационной безопасностью; уметь реагировать на инциндеты ИБ; идентифицировать нарушителей.

Постреквизиты: магистерская диссертация, дисциплины докторантуры

IBES 6308, Информационная безопасность экономических систем, 2кр

Пререквизиты: Средства безопасности сетевых ОС, Организация систем информационной безопасности, Криптологические методы и средства защиты информации, Архитектура систем безопасности серверов БД.

Цель изучения: Формирование знаний в области теоретических основ информационной безопасности экономических систем; навыков практического обеспечения защиты информации и безопасного использования программных средств в экономических системах.

Краткое содержание: Экономическая информация как товар и объект безопасности. Экономическая деятельность в Интернет. Виды угроз безопасности в экономических информационных системах. Политика безопасности. Основные пути несанкционированного доступа к информации. Методы и средства защиты, используемые в экономических системах, их классификация. Аппаратные средства защиты информации. Средства обнаружения каналов утечки информации. Межсетевые экраны. Системы обнаружения атак. DLP-системы. Вредоносные программы. Системы резервного копирования и восстановления данных. Криптографические средства. Защита баз данных. Облачные технологии и безопасность данных

Ожидаемые результаты: Знание основных понятий информационной безопасности в экономических системах, архитектуры защищённых экономических систем. Умение обеспечения защиты и безопасности экономических систем.

Постреквизиты: магистерская диссертация, дисциплины докторантуры

BSEB 6308.1, Безопасность систем электронного бизнеса, 2кр

Пререквизиты: Методы и средства защиты в ОС, Организация систем информационной безопасности, Алгоритмы криптографической защиты информации, Организация защиты и безопасности БД.

Цель изучения: Ознакомление с понятиями системы электронного бизнеса, практического обеспечения безопасности электронного бизнеса.

Краткое содержание: Понятие электронного бизнеса. Виды угроз безопасности в электронном бизнесе. Идентификация, аутентификация, авторизация. Подтверждение подлинности действий клиента. Защита от перехвата информации. Противодействия навязыванию ложной информации. Нейтрализация внешних атак. Межсетевое экранирование. Системы обнаружения вторжений. Системы предотвращения вторжений. Системы защиты от проникновения вредоносного контента. Дискреционное и мандатное управление доступом к защищаемым ресурсам. Обеспечение информационной безопасности автоматизированных банковских систем. Информационная безопасность электронной коммерции (ЭК).

Ожидаемые результаты: Знание основных понятий системы электронного бизнеса. Применение современных методов и средств противодействия угрозам.

Постреквизиты: магистерская диссертация, дисциплины докторантуры