ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF KAZAKHSTAN

Қ.И.СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ЗЕРТТЕУ ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И.САТПАЕВА

KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY named after K. I. Satpaev

6М100200 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ МАМАНДЫҒЫНЫҢ ЭЛЕКТИВТІ ПӘНДЕР КАТАЛОГЫ

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН СПЕЦИАЛЬНОСТИ 6М100200 СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ELECTIVE DISCIPLINES CATALOG OF SPECIALITY 5B100200 OF SYSTEM FOR INFORMATION SAFETY

Алматы 2016

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И.СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ЗЕРТТЕУ ТЕХНИКАЛЫҚ УНИВЕРСИТЕТІ

6М100200 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ МАМАНДЫҒЫНЫҢ ЭЛЕКТИВТІ ПӘНДЕР КАТАЛОГЫ

БІЛІМ АЛУШЫ МЕН ЭДВАЙЗЕРГЕ АРНАЛҒАН ЖАДНАМА

Мамандықтың барлық пәндері модульдер мен циклдер (бакалавриатта ЖБП, БП, КП; магистратура мен докторантурада БП, КП) 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.

_____2_____
(оқу мерзімі)

№	Модуль атауы	Пән циклі	Пән коды	Пән атауы	Кредиттер саны	Семестр
1	Қауіпсіздік модулі	БП	MII 6208	Жасанды зерде әдістері	3	1
1.1		БП	YZ 6208.1	Білімді басқару	3	1
2		КП	SMIB 6307	Ақпараттық қауіпсіздіктің менеджмент жүйесі	3	1
2.1		КП	YIB 6307.1	Ақпараттық қауіпсіздікті басқару	3	1
3		КП	IBES 6308	Экономикалық жүйелердің ақпараттық қауіпсіздігі	2	1
3.1		КП	BSEB 6308.1	Электрондық бизнес жүйелерінің қауіпсіздігі	2	1
4	Инженерлік-техникалық қорғау модулі	КП	ASPU6305	Ақпараттың сыртқа кету арналарын іздеудің және табудың аппараттық құралдары	3	1
4.1		КП	TZI6305.1	Ақпаратты инженерлік-техникалық қорғау	3	1
5		КП	SBIS 6306	Ақпарат қорғаудағы бағдарламаланатын логикалы АШИС	3	1
5.1		КП	PMK 6306.1	Шағын контроллерді бағдарламалау	3	1

(көрсетілген курста оқылатын әрбір элективті пәннің сипаттамасы)

MII 6208, Жасанды зерде әдістері, 3 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерінің ұйымдастырылуы, ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, Ақпаратты қорғаудың криптологиялық әдістері мен құралдары

Оқыту мақсаты: студенттердің бойында жасанды зерде жүйелерінің жобалаудың теориялық негіздері туралы түсінік қалыптастыру, жасанды зерде жүйелерінің көмегімен ақпараттық қауіпсіздік проблемаларын шешуде творчестволық көзқарас қалыптастыру.

Қысқаша мазмұны: Жасанды зерде ғылыми бағыт ретінде. Білімдерге негізделген жүйелер. Жасанды зерделердегі білімді көрсету. Зерделік жүйелердегі білімді қалыптастыру. Білімді көрсету үлгілері. Фреймдық және желілік үлгілер. Білімдерді логикалық көрсету және продукционды жүйелер. Логикалық қорытындау ережелері. Күйлер кеңістігінде шешімдерді іздеу. Анық емес логика. Сараптық жүйелер, сараптық жүйелерді құру кезеңдері. Зерделік интерфейс жүйелері. Тілді генерациялау және тану жүйелері. Бейнелерді генерациялау және техникалық көру жүйелері. Нейронды желілер.

Күтілетін нәтижелер: Жасанды зерденің негізгі түсініктерін және білімдерді көрсету түрлерін білу. Зерде жүйелерінде білімдерді қалыптастыру және оларды көрсету, күрделі емес сараптық жүйелерді құру қабілеттігі.

Постреквизиттер: магистерлік диссертация

YZ 6208.1, Білімді басқару, 3 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерінің ұйымдастырылуы, ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті, Ақпаратты криптографиялық қорғау алгоритмдері.

Оқыту мақсаты: Білім беру жүйелерін құру принциптері, әдістері мен құралдары туралы жүйелі білім беруді қалыптастыру, сараптық жүйелер және жасанды зерде жүйелерін құрудың тәжірибелік дағдыларын алу.

Қысқаша мазмұны: Білімдерге негізделген жүйелер. Жасанды зерде жүйелері. Білімдер қорлары. Білімдерді қалыптастыру, білімдерді көрсетудің декларативті және процедуралық үлгілері. Продукционды жүйелер. Логикалық қорытындау ережелері. Күйлер кеңістігінде шешімдерді іздеу. Сараптық жүйелер, сараптық жүйелерді құру кезеңдері. Білім инженериясы және сараптық жүйелерді құру технологиясы. Білімдерді іріктеу әдістері. Білімдерді басқару жүйелерінің аспаптық құралдары. Зерделік интерфейс жүйелері. Тілді генерациялау және тану жүйелері. Бейнелерді генерациялау және техникалық көру жүйелері. Жасанды нейронды желілер.

Күтілетін нәтижелер: Жасанды зерденің негізгі түсініктерін және білімдерді көрсету түрлерін білу. Зерде жүйелерінде білімдерді қалыптастыру және оларды көрсету, күрделі емес сараптық жүйелерді құру қабілеттігі.

Постреквизиттер: магистерлік диссертация

SMIB 6307, Ақпараттық қауіпсіздіктің менеджмент жүйесі, 3 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Желі қауіпсіздігін басқару

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 инциндентерін басқару ерекшеліктерін білу қажет; ақпараттық қауіпсіздіктің инциндентеріне 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.

УІВ 6307.1, Ақпараттық қауіпсіздікті басқару, 3 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, 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 инциндентерін басқару үшін стандарттар мен ұсыныстар. CERT/CSIRT топтарымен шабуылдарды анықтау және басып кіруді тану. Ақпараттық қауіпсіздіктің инциндентерінің әсерін болдырмау және жою. Бұзушының идентификациясы және ақпараттық қауіпсіздіктің инциндентерінен болған зардапты бағалау. Ақпараттық қауіпсіздіктің инциндентеріне жауап беру топтарының тиімді жұмыстарының құралдары. Ақпараттық қауіпсіздіктің инциндентерін 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

IBES 6308, Экономикалық жүйелердің ақпараттық қауіпсіздігі, 2 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, Желілік ОЖ-дің қауіпсіздік құралдары, ДҚ қорғауды және қауіпсіздендіруді ұйымдастыру, Ақпаратты қорғаудың криптологиялық әдістері мен құралдары.

Оқу 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: магистерлік диссертация

BSEB 6308.1, Электрондық бизнес жүйелерінің қауіпсіздігі, 2 кр

Пререквизиттер: Ақпараттық қауіпсіздік жүйелерін ұйымдастыру, ОЖ қорғау әдістері мен құралдары, ДҚ серверлерінің қауіпсіздік жүйелерінің сәулеті, Ақпаратты криптографиялық қорғау алгоритмдері.

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 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: магистерлік диссертация

ASPU6305 Ақпараттың ағу арнасын іздеу және табудың аппараттық құралдары, 3 кр

Пререквизиттері: Электроника және сұбатехника, Цифрлық және аналогтық электроника, Ақпаратты қорғаудың техникалық құралдары

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. Байланыс арналарындағы ақпаратты рұхсатсыз алатын электрондық құрылғыларды анықтау. Сымды қатынастықтардағы(коммуникациядағы) жоғары жиілікті сигналдарды және электромагниттік шашырауларды(излученияларды) бақылау құрылғылары.

Күтілітін 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.

Постреквизиттері: «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, 3 кр

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, 3 кр

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 ұйымдастырылуы, Микроконтроллерлер

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: магистерлік диссертация

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И.САТПАЕВА

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН СПЕЦИАЛЬНОСТИ 6М100200 СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

_____2_____
(курс обучения)

№	Наименование модуля	Цикл дисциплины	Код дисциплины	Наименование дисциплины	Кол-во кредитов	Семестр
1	Модуль безопасности	БД	MII 6208	Методы искусственного интеллекта	3	1
1.1		БД	YZ 6208.1	Управление знаниями	3	1
2		ПД	SMIB 6307	Системы менеджмента информационной безопасности	3	1
2.1		ПД	YIB 6307.1	Управление информационной безопасностью	3	1
3		ПД	IBES 6308	Информационная безопасность экономических систем	2	1
3.1		ПД	BSEB 6308.1	Безопасность систем электронного бизнеса	2	1
4	Модуль инженерно-технической защиты	ПД	ASPU6305	Аппаратные средства поиска и обнаружения каналов утечки информации	3	1
4.1		ПД	TZI6305.1	Инжененнрно-техническая защита информации	3	1
5		ПД	SBIS 6306	СБИС программируемой логики в защите информации	3	1
5.1		ПД	PMK 6306.1	Программирование микроконтроллеров	3	1

(описание каждой элективной дисциплины, изучаемой на указанном курсе)

MII 6208, Методы искусственного интеллекта, 3 кр

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

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

Краткое содержание: Искусственный интеллект как научное направление. Системы, основанные на знаниях. 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. Способность формализовать знания и представлять их в интеллектуальных системах, разрабатывать несложные экспертные системы.

Постреквизиты: магистерская диссертация

YZ 6208.1, Управление знаниями, 3 кр

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

Цель изучения: Формирование систематизированных знаний о принципах, методах и средствах построения систем управления знаниями, приобретение практических навыков по созданию систем искусственного интеллекта и экспертных систем.

Краткое содержание: Системы, основанные на знаниях. Системы искусственного интеллекта. 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. Способность формализации и представления знаний, разработки простых экспертных систем.

Постреквизиты: магистерская диссертация

SMIB 6307, Системы менеджмента информационной безопасности, 3 кр

Пререквизиты: Организация систем информационной безопасности, Управление безопасностью сети

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, 3 кр

Пререквизиты: Организация систем информационной безопасности, Протоколы и стандарты сетей и их защиты

Цель изучения: ознакомление с системой менеджмента информационной безопасности по требованиям международных стандартов; с основными 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.

IBES 6308, Информационная безопасность экономических систем, 2 кр

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

Цель изучения: Формирование знаний в области теоретических основ информационной безопасности экономических систем. Формирование навыков практического обеспечения защиты информации 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. Способность обеспечения защиты и безопасности экономических систем.

Постреквизиты: магистерская диссертация

BSEB 6308.1, Безопасность систем электронного бизнеса, 2 кр

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

Цель изучения: Ознакомление с понятиями системы электронного бизнеса и 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.

Ожидаемые результаты: Знание основных понятий системы электронного бизнеса. Способность применения современных методов и средств противодействия угрозам в системах электронного бизнеса.

Постреквизиты: магистерская диссертация

ASPU6305 Аппаратные средства поиска и обнаружения каналов утечки информации, 3 кр

Пререквизиты: Электроника и схемотехника, Цифровая и аналоговая электроника, 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 связи. Устройства контроля электромагнитных излучений и высокочастотных сигналов в проводных коммуникациях.

Ожидаемые результаты: 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: написании магистрской диссертации, на практической работе по специальности.

TZI6305.1 Инженерно-техническая защита информации, 3 кр

Пререквизиты: Электроника и схемотехника, Цифровая и аналоговая электроника, 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: написании магистрской диссертации, на практической работе по специальности.

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

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, 3 кр

Пререквизиты: Организация вычислительных систем, Микроконтроллеры

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: магистрская диссертация

MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

KAZAKH NATIONAL RESEARCH
TECHNICAL UNIVERSITY named after K. I. Satpaev

ELECTIVE DISCIPLINES CATALOG OF SPECIALITY 6M100200 OF SYSTEM FOR INFORMATION SAFETY

AIDE-MEMOIRE TO STUDENTS AND CURATOR

All disciplines by specialty undergraduate are divided by cycles (GED, GS, PS), Master's and Doctoral (GS, PS), modules, within which they are divided into compulsory and elective (optional) subjects. The list of mandatory subjects for study is represented at the model curriculum of the specialty (MC).

The list of elective courses for each specialty course is represented in the directory of elective disciplines (DED), which is the list of systematized and annotated of subjects for choosing a specialty.

DED should give (provide) students the possibility of an alternative choice of elective subject matters according with the chosen trajectory of learning.

Based at the model curriculum of the specialty and DED formed individual educational plan (IEP) of student for the academic year.

The curator appointed by letting out of chair assists to bachelors and masters in the preparation of IEP. Candidates of doctoral make up IEP by yourself.

IEP defines individual educational trajectory of each student within the specialty. The IEP includes a mandatory component disciplines and types of training activities (practice, research, state (complex) exam, writing and protection of degree work (project), dissertation) of the model curriculum and components of disciplines of choice from DED.

The educational path, is oriented to a specific field of activity taking into account needs of labor market and employers. Within DED has to be submitted the list of disciplines guaranteeing to students purposeful of mastering of a scheduled educational program .

At the choice of elective disciplines it is necessary to consider the following:

1 In one semester the student of full-time courses has to master 18-22 credits (obligatory and elective), a form of remote – 9-12 credits (obligatory and elective), without the additional types of training (ATT) which are obligatory for studying.

2 The total of the credits for the entire period of training shouldn't exceed the quantity specified at MC of specialty .

3 Elective disciplines are united in groups on the choice with the corresponding number. It is possible to choose only one elective subject matter from each group of disciplines.

Academic degree: Bachelor of military affairs and security

_____2_____
(Course of Study)

№	Name of the module	Cycle of Discipline	Discipline Code	Name of Discipline	Number of credits	Semester
1	Safety module	GS	MII 6208	Methods of artificial intelligence	3	1
1.1		GS	YZ 6208.1	Management by Knowledge	3	1
2		PS	SMIB 6307	Systems of management of information security	3	1
2.1		PS	YIB 6307.1	Information security management	3	1
3		PS	IBES 6308	Information security of economic systems	2	1
3.1		PS	BSEB 6308.1	Security of systems of electronic business	2	1
4	Module of engineering and technical protection	PS	ASPU6305	Vehicle query and finding out the channels of loss of information facilities	3	1
4.1		PS	TZI6305.1	Technical defence of information	3	1
5		PS	SBIS 6306	VLSI programmable logic in defence of information	3	2
5.1		PS	PMK 6306.1	Programming of microcontrollers	3	2

(the description of each of elective subject wich have studing on the specified course)

MII 6208, Methods of artificial intelligence, 3 cr

Prerequisites: Organization of systems of information safety, Organization of protection and safety of a database, Methods of cryptology and means of information protection.

The purpose of the study: Formation of knowledge of the theoretical foundations for the design of artificial intelligence systems, the formation of creative approach to solving information security problems by using artificial intelligence systems.

Summary: Artificial intelligence as a scientific discipline. Systems based on knowledge. Knowledge representation in artificial intelligence systems. The formalization of knowledge in intelligent systems. Models of knowledge representation. Framed and network models. The logical representation of knowledge and production systems. Logical inference rules. Finding

solutions in state space. Fuzzy logic. Expert systems, stages of engineering of expert systems. Intelligent interface systems. Systems of recognition and speech generation. Vision systems and image generation. Neural networks.

The expected results: Knowledge of the basic concepts of artificial intelligence and of knowledge representation. Ability is formalize knowledge and to represent them in intelligent systems and develop simple expert systems

Postrequisites: Master's dissertation

YZ 6208.1, Management by Knowledge, 3 cr

Prerequisites: Organization of systems of information safety, Architecture of systems of safety of the DB servers Algorithms of cryptographic protection of information

The purpose of the study: Formation of systematic knowledge of the principles, methods and means of building knowledge management systems, formation of practical skills in the creation of artificial intelligence and expert systems.

Summary: Knowledge-based systems. Artificial intelligence systems. Knowledge base, the formalization of knowledge. The declarative and procedural knowledge representation model. Production system. Logical inference rules. Finding solutions in state space. Presentation and use of fuzzy knowledge. Expert systems, stages of engineering of expert systems. Knowledge engineering and technology of expert systems development. Methods of extraction of knowledge. The tools of knowledge management systems. Intelligent interface systems. Systems of recognition and speech generation. Vision systems and image generation. Artificial neural networks.

The expected results: Knowledge of the basic concepts of knowledge management and of the forms of knowledge representation. Ability to formalization and to representation of knowledge to engineering of simple expert systems.

Postrequisites: Master's dissertation

SMIB 6307, Systems of management of information security, 3 cr

Prerequisites: Organization of systems of information safety, Security management of a network

The purpose of the study: acquaintance with system of management of information security; with the basic concepts and the principles in the sphere of control of incidents of IB; with concepts of creation, of structure and functional features of system of management.

Summary: System management of management of information security according to requirements of the international standards. The basic concepts and the principles in the sphere of incident management of information security. Creation and functioning of command centers incidents of information security. Stages of effective management of incidents of information security according to requirements of the international ISO 27035 and ISO 18044 standards. Concept of creation, structure and the functional features of effective system of management of incidents of IB. Tools for effective functioning of groups of response to incidents of IB. Documentation of support of administrative process with incidents of IB.

The expected results: You should know the features of management of information security incidents occurred; to control tools for the effective functioning of the first responders to incidents of information security.

Postrequisites: Master's dissertation

YIB 6307.1, Information security management, 3 cr

Prerequisites: Organization of information security systems, Protocols and standards of networks and their protection

The purpose of the study: acquaintance with system of management of information security according to requirements of the international standards; with the basic concepts, principles and phases of incident management in accordance with the requirements of the international standard; with the functional features of the management system.

Summary: Effective management of incidents of information security according to requirements of the international standards. Basic terms, determination, concepts and the principles in the sphere of control of information security. Standards, recommendations about incident management of information security. Detection of attacks and recognition of invasions by CERT/CSIRT groups. Localization and elimination of consequences of incidents of information security. Identification of violators and an assessment of damage from incidents of information security. Elimination of negative consequences of incidents and resumption of work of information systems. Documentation of support of administrative process with incidents of IS. Activities of groups of response to incidents of IS.

The expected results: to know the main terms, concepts and the principles in the sphere of information security management; to be able to react to IS intsindeta; to identify violators.

Postrequisites: Master's dissertation

IBES 6308, Information security of economic systems, 2 cr

Prerequisites: Organization of systems of information safety, Means of security of network of operating systems, Organization of protection and safety of a database, Methods of cryptology and means of information protection.

The purpose of the study: Formation of knowledge of the theoretical foundations of information security of economic systems. Formation of skills of practical providing information security in economic systems.

Summary: Economic information as a commodity and a object of security. Economic activity in the Internet. Types of security threats in the economic information systems. Security policy. The main ways of unauthorized access to information. Methods and means of protection used in economic systems, their classification. Hardware of data protection. Means of detection of information leakage channels. Firewalls. Intrusion detection systems. DLP-system. Malicious programs. Backup systems and data recovery. Cryptographic tools. Database protection. Cloud technology and data security.

The expected results: Knowledge of the basic concepts of information security to the economic systems, architecture of protected economic systems. The ability to ensure the protection and security of economic systems.

Postrequisites: Master's dissertation

BSEB 6308.1, Security of systems of electronic business, 2 cr

Prerequisites: Organization of systems of information safety, Methods and means of protection in operating systems, Architecture of systems of safety of the DB servers, Algorithms of cryptographic protection of information.

The purpose of the study: Introduction to the concepts of e-business systems and of providing practical security e-business.

Summary: The concept of e-business. Types of security threats in e-business. Identification, authentication, authorization. Confirm the authenticity of the client's actions. Protection against interception. Countering obtrusions of false information. Neutralization of external attacks. Firewall. Intrusion Detection Systems. Intrusion Prevention Systems. Systems of protection against malicious content. Discretionary and mandatory access control to protected resources. Providing of information safety of the automated banking system. Information security e-commerce.

The expected results: Knowledge of the basic concepts of e-business systems. Ability of using of modern methods and means of countering threats in e-business.

Postrequisites: Master's dissertation

ASPU6305, Vehicle query and finding out the channels of loss of information facilities, 3 cr

Prerequisites: Electronics and circuit technology, Digital and analog electronics, Technical equipments of defence of information".

The purpose of the study: acquaintance with the features of principles of action and application of vehicle facilities for a search and finding out the active channels of loss of information; acquaintance with economic feasibilities and descriptions of different vehicle facilities, providing protecting of information from a loss and counteraction to the unauthorized division to the confidential information generators; acquaintance with vehicle facilities of exposure of channels of loss of information on different objects and in apartments.

Summary: Vehicle query and finding out the active channels of loss of information and off-wire devices facilities. Searching receiver for a discovery and position-fix of radiotransmitter devices of secret receipt of information. Classification of acoustic channels of loss of information. Vehicle facilities of radiomonitoring. Protecting of speech information of leader of organization from the hidden record a visitor. Protecting of acoustic information from a loss on an optical-electronic channel. Devices of search and exposure of the hidden video cameras and radio channels of transmission of аудио-и video information. Vehicle facilities of exposure of electronic devices of secret receipt of information are in communication channels. Devices of control of electromagnetic radiations and high-frequency signals are in wire communications.

The expected results: must know technical descriptions and possibilities of different vehicle facilities of defence of information; to know the features of work and application of vehicle facilities of defence of information domain; able effectively to use them for a search and finding out the active channels of loss of confidential information.

Postrequisites: Master's dissertation, at practical work on speciality.

TZI6305.1, Technical defence of information, 3 cr

Prerequisites: Electronics and circuit technology, Digital and analog electronics

The purpose of the study: acquaintance with the features of application technical facilities of defence of information; acquaintance with the features of physical facilities of defence of objects and vehicle query and exposure of channels of loss of information facilities; acquaintance with technical events on defence of information with the use of passive and active technical equipments; acquaintance with the technical equipments of reception and information transfer; acquaintance with the technical channels of loss of information by the «high-frequency imposing» (modulations of high-frequency signal informative).

Summary: Technical defence (ИТЗ) of information. Events on defence of information with the use of passive and active technical equipments. Technical equipments of ИТЗ of information, classification. Physical facilities of defence of objects. Vehicle query facilities and exposure of channels of loss of information. Technical channels of loss of acoustic information. Technical equipments of reception and information transfer. Mortgaged devices of intercept of speech information. Telephone ear. Electronic стетоскопы. Laser microphones. Оптико-электронный intercept of acoustic signals by the laser sounding of window-panes. Technical channel of loss of information by the «high-frequency imposing». Self-reactance technical channels of loss of information.

The expected results: must know the features of application of technical facilities of defence of information; to know technical descriptions and possibilities of different technical equipments of reception and information transfer; able effectively to use technical equipments for a search and finding out the active channels of loss of confidential information.

Postrequisites:can be useful at writing of магистрской dissertation, at practical work on speciality.

SBIS6306, VLSI programmable logic in defence of information, 3 cr

Prerequisites: Electronics and circuit technology, Digital and analog electronics, Microelectronics

The purpose of the study: acquaintance with the features of circuit technology and application of programmable logical matrices, programmable matrix logic, matrix masterslices; acquaintance with modern and perspective VLSI with difficult programmable and by reprogrammable structures; acquaintance with parameters, families and configuring VLSI programmable logic; acquaintance with possibilities of application programmable logical IS (PLIS) in a microprocessor-based and calculable technique and for defence of information; study of possibility of application PLIS for the protection of software and apparatus fetch and printing-down.

Summary: the Programmable logical matrices. Programmable matrix logic. Matrix masterslices. VLSI with difficult programmable and by reprogrammable structures. User-programmable gate arrays (FPGA). Application of FPGA domains and VLSI programmable logic (PL). Difficult programmable logical charts (CPLD) and VLSI programmable logic of the mixed architecture. VLSI programmable logic of type «system on a crystal». Parameters, families and configuring VLSI programmable logic. Application programmable logical IS in a microprocessor-based and calculable technique, to the technique of connection and for defence of information. Application PLIS for the protection of software and apparatus fetch and printing-down.

The expected results: must know the features of circuit technology and application of programmable logical matrices, programmable matrix logic, matrix masterslices; to know features modern VLSI with difficult programmable and by reprogrammable structures; to know parameters, families and possibilities of configuring VLSI programmable logic; to know possibilities of application programmable logical IS (PLIS) in a microprocessor-based and calculable technique and for defence of information; to know to possibility of application PLIS for the protection of software and apparatus fetch and printing-down.

Postrequisites:can be useful at writing of магистрской dissertation, at practical work on speciality.

PMK 6306.1, Programming of microcontrollers, 3 cr

Prerequisites: Organization of computing systems, Microcontrollers

The purpose of the study: Study of methods and means of programming aids of operations in systems on the basis of applications microcontroller

Summary: Technical characteristics and program and available means of the microcontroller. Programming of input/output ports. Arithmetical data handling. Representation of numbers. Addition and subtraction of numbers. Multiplication and division of numbers. Programming of arithmetical operations. Timers of microcontrollers. A data interchange on the serial interface. Organization of input-output for the parallel interface. The synchronous and asynchronous of execution of input-output and processing. Analog signals processing. Analog digital conversion. Analog comparing of signals. Programming and debugging of programs in the universal languages

The expected results: Development of models of processes and compilation of programs for applications of microcontroller.

Postrequisites: Master's dissertation