«ҚАЗАҚ ҰЛТТЫҚ АГРАРЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ»
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

«Су ресурстары және IT-технологиялар» факультеті

ЭЛЕКТИВТІК ПӘНДЕР КАТАЛОГЫ

7М06301 – «Ақпараттық қауіпсіздіктің интеллектуалды жүйелері»

2026-2028 оқу жылына арналған

АЛМАТЫ, 2026

Элективті пәндер каталогы Қазақ ұлттық аграрлық зерттеу университеті оқу-әдістемелік кеңесінің (хаттама №___ «___»_____2026 ж.) және Ғылыми кеңесінің (хаттама №___,
«___»_____2026 ж.) шешімдерімен мақұлданған

Құрастырғандар: Медетбаева С.А.

Алғы сөз

Элективті пәндер каталогы (ЭПК) Қазақстан Республикасы Ғылым және жоғары білім министрінің 2022 жылғы 20 шілдедегі №2 бұйрығы бекітілген Жоғары білім берудің мемлекеттік жалпыға міндетті стандарты негізінде Қазақ ұлттық аграрлық зерттеу университетінің оқу-әдістемелік жұмыстар бөлімімен құрастырылды.

ЭПК білім алушыларға жеке білім траекториясын құру үшін элективті оқу пәндерін және ПОҚ таңдау мүмкіндігімен қамтамасыз етеді. Білім беру бағдарламаларының және ЭПК негізінде білім алушылар эдвайзерлердің көмегімен жеке оқу жоспарын әзірлейді.

Каталог кестесінде магистратураның базалық пәндер (БП) және бейіндеуші пәндер (БеП) циклдерінің жоғары оқу орны компоненті мен таңдау компоненті пәндері, практикалар, магистранттың ғылыми-зерттеу жұмысы және қорытынды аттестаттау, сондай-ақ пәндердің формулярлары келтіріледі. ЭПК формулярында пәндердің атаулары, пәннің қысқаша мазмұны, пререквизиттері мен постреквизиттері, ПОҚ аты-жөні, кредит саны мен курсты оқу семестрі көрсетілген.

БІЛІМ БЕРУ БАҒДАРЛАМАСЫ: 7М06301 – «АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕЛЕРІ»

Берілетін дәреже: 7М06301 – «Ақпараттық қауіпсіздіктің интеллектуалды жүйелері» білім беру бағдарламасы бойынша техника ғылымдарының магистрі

1 КУРС

Цикл	Код	Пәндер	Академ. кредиттер
1 семестр – 30 академиялық кредит			
Жоғары оқу орны компоненті – 13 кр.			
БП	IFN 5204	Ғылым тарихы мен философиясы	5
БП	IYaP 5202	Шет тілі (кәсіби)	3
БП	PVSH 5203	Жоғары мектептің педагогикасы	5
Таңдау компоненті – 15 кр.			
БП	ABOS 5207	Операциялық жүйелердің қауіпсіздігін талдау	5
	KIS 5206	Ақпараттық жүйелердің киберқауіпсіздігі	
БП	ASB 5209	Желілік қауіпсіздікті талдау	5
	AISB 5208	Қауіпсіздіктің аналитикалық ақпараттық жүйелері	
БП	KMSZI 5211	Ақпаратты қорғаудың криптографиялық әдістері мен құралдары	5
	PPKP 5210	Криптографиялық хаттамаларды құру қағидалары	
Магистранттың ғылыми-зерттеу жұмысы – 2 кр.			
ҒЗЖ	NIRM 5501	Магистранттың ғылыми-зерттеу жұмысы	2
2 семестр – 30 академиялық кредит			
Жоғары оқу орны компоненті – 28 кр.			
БП	PU 5205	Басқару психологиясы	3
БП	PP 5201	Педагогикалық практика	4
БеП	MIK 5313	Киберқауіпсіздіктегі зерттеу әдістері	6
БеП	UPK 5314	Киберқауіпсіздік жобаларын басқару	5
БеП	AIB 5312	Ақпараттық қауіпсіздік аудиті	5
БеП	IP 5309	Зерттеу практикасы	5
Магистранттың ғылыми-зерттеу жұмысы – 2 кр.			
ҒЗЖ	NIRM 5502	Магистранттың ғылыми-зерттеу жұмысы	2

Пәнді сипаттау формуляры

Пәннің коды мен атауы	**IFN 5204 Ғылым тарихы мен философиясы**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Философия (бакалавриат деңгейінде)
Пәннің постреквизиттері	Киберқауіпсіздіктегі зерттеу әдістері, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Магистранттарда ғылымды әлеуметтік-мәдени құбылыс ретінде, ғылыми білімнің тарихи динамикасы және ақпараттық қауіпсіздік саласындағы зерттеулерді жоспарлау мен жүргізуге қажетті ғылыми зерттеудің әдіснамалық негіздері туралы тұтас түсінік қалыптастыру.
Пән мазмұны	Ғылым философиясының пәні. Ғылым білім жүйесі, қызмет түрі және әлеуметтік институт ретінде. Ғылымның генезисі: антика, орта ғасырлар, Жаңа заман. Классикалық, классикалық емес және постклассикалық ғылым. Ғылымның даму тұжырымдамалары (К. Поппер, Т. Кун, И. Лакатос, П. Фейерабенд). Ғылыми білімнің құрылымы: эмпирикалық және теориялық деңгейлер. Ғылыми таным әдістері. Әлемнің ғылыми бейнесі. Техника, информатика және кибернетиканың философиялық мәселелері. Ақпараттық қоғам және цифрлық этика. Ғылым этикасы және академиялық адалдық. Қазақстандағы ғылымның дамуы.
Пәннің құзіреттілігі	- - біледі: ғылымның тарихи дамуының негізгі кезеңдерін, даму тұжырымдамаларын және ғылыми білімнің құрылымын; - - түсінеді: ғылыми зерттеудің философиялық және әдіснамалық негіздерін, ақпараттық қоғамның дамуындағы ғылымның рөлін; - - қолдана алады: ақпараттық қауіпсіздік саласындағы зерттеу міндеттерін қою мен негіздеуде ғылыми таным әдістерін; - - құзыретті: ғылыми этика мен академиялық адалдық қағидаттарын сақтай отырып, ғылыми нәтижелерді дәлелді бағалауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 1. 1. Степин В.С. История и философия науки: учебник для аспирантов и соискателей. – М.: Академический проект, 2011. – 423 с. 2. 2. Лебедев С.А. Философия науки: учебное пособие для магистров. – М.: Юрайт, 2014. – 288 с. 3. 3. Кохановский В.П., Лешкевич Т.Г., Матяш Т.П., Фатхи

	Т.Б. Основы философии науки. – Ростов н/Д: Феникс, 2010. – 603 с. 4. 4. Кун Т. Структура научных революций. – М.: АСТ, 2020. – 320 с. **Қосымша:** 5. 5. Поппер К. Логика научного исследования. – М.: Республика, 2004. – 447 с. 6. 6. Лакатос И. Фальсификация и методология научно-исследовательских программ. – М.: Медиум, 1995. – 236 с. 7. 7. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Пәннің коды мен атауы	**IYaP 5202 Шет тілі (кәсіби)**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7M06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	3
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Шет тілі (бакалавриат деңгейінде)
Пәннің постреквизиттері	Киберқауіпсіздіктегі зерттеу әдістері, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Магистрантқа ақпараттық қауіпсіздік бойынша шетелдік дереккөздерді оқуға және талдауға, академиялық мәтіндер мен презентациялар дайындауға және халықаралық ғылыми пікірталастарға қатысуға мүмкіндік беретін шет тіліндегі кәсіби және ғылыми коммуникативтік құзыреттілікті дамыту.
Пән мазмұны	Ақпараттық қауіпсіздік және жасанды интеллект саласындағы кәсіби лексика мен терминология. Ғылыми мақалаларды оқу және рефферреттеу. Ғылыми мақаланың құрылымы (IMRaD). Академиялық жазылым: аннотация, кіріспе, әдебиеттерге шолу, нәтижелерді талқылау. Дәйексөз келтіру және сілтемелерді рәсімдеу (APA, IEEE). Ғылыми презентацияны дайындау және өткізу. Пікірталасқа, конференцияға, вебинарға қатысу. Іскерлік хат алмасу және зерттеушінің түйіндемесі. Кәсіби бағдарлы мәтіндерді аудару.
Пәннің құзіреттілігі	- - біледі: кәсіби терминологияны және шет тіліндегі ғылыми дискурстың жанрлық ерекшеліктерін; - - түсінеді: ақпараттық қауіпсіздік бойынша шетелдік ғылыми жарияланымдар мен техникалық құжаттаманың мазмұнын; - - қолдана алады: аннотацияларды, ғылыми мақалаларды және зерттеу нәтижелерінің презентацияларын дайындау үшін шет тілін; - - құзыретті: халықаралық ғылыми ортада ауызша және жазбаша кәсіби коммуникацияда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)

Әдебиеттер тізімі	**Негізгі:** 8. 1. Swales J.M., Feak C.B. Academic Writing for Graduate Students: Essential Tasks and Skills. – 3rd ed. – Ann Arbor: University of Michigan Press, 2012. – 418 p. 9. 2. Wallwork A. English for Writing Research Papers. – 2nd ed. – Cham: Springer, 2016. – 368 p. 10. 3. Wallwork A. English for Presentations at International Conferences. – 2nd ed. – Cham: Springer, 2016. – 222 p. 11. 4. Murphy R. English Grammar in Use. – 5th ed. – Cambridge: Cambridge University Press, 2019. – 394 p. **Қосымша:** 12. 5. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Harlow: Pearson, 2020. – 832 p. 13. 6. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Пәннің коды мен атауы	**PVSH 5203 Жоғары мектептің педагогикасы**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7M06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Психология, педагогика негіздері (бакалавриат деңгейінде)
Пәннің постреквизиттері	Басқару психологиясы, Педагогикалық практика
Пәнді оқу мақсаты	Білім беру процесін жобалауға, заманауи педагогикалық технологияларды қолдануға және бағалауға, тиімді педагогикалық коммуникацияны қамтамасыз етуге қабілетті болашақ жоғары оқу орны оқытушысының психологиялық-педагогикалық құзыреттілігін қалыптастыру.
Пән мазмұны	Жоғары мектеп педагогикасы ғылым ретінде. Болон процесі және Қазақстан Республикасында жоғары білім берудің дамуы. Жоғары білім берудің нормативтік базасы (МЖМБС, академиялық саясат). Жоғары мектеп дидактикасы: оқыту қағидаттары, нысандары мен әдістері. Кредиттік технология және білім алушыға бағдарланған оқыту. Оқыту нәтижелері мен силлабусты жобалау. Белсенді және интерактивті әдістер, аралас және қашықтықтан оқыту. Оқыту нәтижелерін бағалау. Тәрбие жұмысы және кураторлық. Педагогикалық қарым-қатынас және оқытушының кәсіби этикасы.
Пәннің құзіреттілігі	- - біледі: жоғары мектепте білім беру процесін ұйымдастырудың заңдылықтарын, қағидаттарын және нормативтік негіздерін; - - түсінеді: кредиттік технологияның және оқытудағы білім алушыға бағдарланған тәсілдің мәнін; - - қолдана алады: заманауи педагогикалық технологияларды, белсенді оқыту және оқыту нәтижелерін бағалау әдістерін; - - құзыретті: оқу сабақтары мен силлабустарды жобалауда,

	педагогикалық коммуникацияда және кәсіби этиканы сақтауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 14. 1. Громкова М.Т. Педагогика высшей школы: учебное пособие. – М.: ЮНИТИ-ДАНА, 2012. – 447 с. 15. 2. Пидкасистый П.И. Педагогика: учебник для бакалавров. – М.: Юрайт, 2014. – 511 с. 16. 3. Мынбаева А.К., Садвакасова З.М. Инновационные методы обучения, или Как интересно преподавать: учебное пособие. – Алматы, 2010. – 344 с. 17. 4. Biggs J., Tang C. Teaching for Quality Learning at University. – 4th ed. – Maidenhead: Open University Press, 2011. – 389 p. **Қосымша:** 18. 5. Государственный общеобязательный стандарт высшего и послевузовского образования. Приказ Министра науки и высшего образования РК от 20 июля 2022 года № 2. 19. 6. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Пәннің коды мен атауы	**ABOS 5207 Операциялық жүйелердің қауіпсіздігін талдау**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Операциялық жүйелер, Ақпараттық қауіпсіздік негіздері, Компьютерлік желілер (бакалавриат деңгейінде)
Пәннің постреквизиттері	Ақпараттық қауіпсіздік аудиті, Киберқауіпсіздік жобаларын басқару, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі, Ақпараттық қауіпсіздікті басқару технологиялары, Киберқауіпсіздіктегі генеративті жасанды интеллект
Пәнді оқу мақсаты	Заманауи операциялық жүйелердің архитектурасы мен кірістірілген қауіпсіздік механизмдері туралы тереңдетілген білімді, ОЖ қорғалуын кешенді талдау, осалдықтарды анықтау және жіктеу, жүйелерді нығайту шараларын негіздеу біліктерін қалыптастыру.
Пән мазмұны	Заманауи ОЖ архитектурасы және қауіптер моделі. DAC, MAC, RBAC қолжетімділікті шектеу модельдері және олардың Windows пен Linux-та іске асырылуы (ACL, SELinux, AppArmor). Сәйкестендіру, аутентификация, есептік жазбалар мен артықшылықтарды басқару. Процестер мен жадты оқшаулау, виртуализация және контейнерлеу. ОЖ осалдықтарын жіктеу (CVE, CWE, CVSS), ядро осалдықтары және артықшылықтарды арттыру. Қауіпсіздік оқиғаларының аудиті және журналдау (Windows Event Log, auditd, syslog). ОЖ қорғалуын нығайту: CIS Benchmarks, STIG. Зиянды БҚ мен руткиттерді анықтау, ОЖ-ны

	криминалистикалық талдау негіздері. Мобильді және кірістірілген ОЖ қауіпсіздігі.
Пәннің құзіреттілігі	- - біледі: заманауи ОЖ архитектурасын, қолжетімділікті шектеу модельдерін және кірістірілген қауіпсіздік механизмдерін; - - түсінеді: ОЖ осалдықтарының табиғатын және CVE, CWE, CVSS негізінде олардың сыни деңгейін бағалау әдістемесін; - - қолдана алады: рұқсатсыз қол жеткізу әрекеттерін анықтау үшін конфигурациялар аудиті мен оқиғалар журналдарын талдау құралдарын; - - құзыретті: салалық стандарттарға сәйкес ОЖ қорғалуын нығайту шаралар кешенін жобалауда және негіздеуде.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 20. 1. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 21. 2. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов. . - М: Юрайт, 2022. - 104 с. - (Высшее образование). - ISBN 978-5-534-14590-8. http://rmebrk.kz/book/1179658 22. 3. Мартынов, А.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / А.П. Мартынов, И.А. Мартынова, А.А. Русаков.- 2-е изд.- М: Ай Пи Ар Медиа, 2024.- 130 с. 23. 4. Прохорова, О.В. Информационная безопасность и защита информации. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. http://rmebrk.kz/book/1183813 24. 5. Усенова, А.Ж. Операциялық жүйелер, орталар және қабықшалар [Мәтін]: оқу-әдістемелік құралы / А.Ж. Усенова.- Алматы: Эверо, 2020.- 348 б. **Қосымша:** 25. 6. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 26. 7. Ешпанов, А. Разработка концепции информационной безопасности: мировой опыт и Казахстан. // Саясат Policy. — 2019. — №9. — С. 33–36. 27. 8. IEEE Computer Society. Operating System Security Models and Access Control. — IEEE Xplore Digital Library, 2022–2024. https://ieeexplore.ieee.org/ 28. 9. Stallings W. Operating Systems: Internals and Design Principles. — 9th ed. — Harlow : Pearson Education Limited, 2018. — 1128 p. — ISBN 978-1292214290 https://api.pageplace.de/preview/DT0400.9781292214306_A37747502/preview-9781292214306_A37747502.pdf?utm_source=chatgpt.com

Пәннің коды мен атауы	**KIS 5206 Ақпараттық жүйелердің киберқауіпсіздігі**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5

Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Ақпараттық қауіпсіздік негіздері, Деректер қоры, Ақпараттық жүйелер архитектурасы (бакалавриат деңгейінде)
Пәннің постреквизиттері	Ақпараттық қауіпсіздік аудиті, Киберқауіпсіздік жобаларын басқару, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі, Ақпараттық қауіпсіздікті басқару технологиялары, Киберқауіпсіздіктегі генеративті жасанды интеллект
Пәнді оқу мақсаты	Өмірлік циклдің барлық кезеңдерінде ақпараттық жүйелердің киберқауіпсіздігін қамтамасыз етуге жүйелі тәсілді, АЖ қорғалу деңгейін бағалау, өзекті қауіптерді модельдеу және кешенді қорғау шешімдерін жобалау қабілетін қалыптастыру.
Пән мазмұны	АЖ қорғау объектісі ретінде, Security by Design қағидаты. Қауіптер мен бұзушыны модельдеу: STRIDE, PASTA, MITRE ATT&CK. Веб-қосымшалар қауіпсіздігі: OWASP Top 10. Деректер қорының қауіпсіздігі, инъекциялардан қорғау, деректерді шифрлау. Сәйкестендіру мен қолжетімділікті басқару (IAM), көпфакторлы аутентификация, Zero Trust архитектурасы. БҚ-ны қауіпсіз әзірлеу: SAST, DAST, DevSecOps. Енуге тестілеу әдіснамасы. Инциденттерді мониторингтеу және оларға әрекет ету: SIEM, SOC. АЖ үздіксіздігі және қалпына келтіру: резервтік көшіру, DRP.
Пәннің құзіреттілігі	- - біледі: қауіптер мен бұзушы модельдерін, қосымшаларды, деректер қорлары мен сервистерді қорғау талаптары мен механизмдерін; - - түсінеді: Security by Design, Zero Trust және бағдарламалық жасақтаманы қауіпсіз әзірлеу қағидаттарын; - - қолдана алады: АЖ қорғалуын бағалау үшін қауіптерді модельдеу, осалдықтарды анықтау және енуге тестілеу әдістерін; - - құзыретті: АЖ-ны қорғау архитектурасын жобалауда және инциденттерді мониторингтеу мен оларға әрекет етуді ұйымдастыруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 29. 1. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 30. 2. Бабаш, А.В. и др. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. – М.: РИОР: ИНФРА-М, 2020. - 236с. - (Высшее образование). -ISBN 978-5-369-01788-3 . https://rmebrk.kz/book/1176322 31. 3. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems

	and computing. Volume 657). 32. 4. Бирюков, А.А. Информационная безопасность: защита и нападение. — М.: ДМК Пресс, 2023. — 440 с. https://rmebrk.kz/book/1183819 33. 5. Медеуова, А.Б. WEB-программирование [Текст]: учеб. пособие / А.Б. Медеуова, В.Н. Казагачев, Ж. Жумагулова.- Алматы: Эверо, 2025.- 232 с. **Қосымша:** 34. 6. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 35. 7. Ешпанов, А. Разработка концепции информационной безопасности: мировой опыт и Казахстан. // Саясат Policy. — 2019. — №9. — С. 33–36. 36. 8. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2024 (18)2. – P. 70–83. https://rmebrk.kz/magazine/6475# 37. 9. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2022. — 30 p. https://www.iso.org/standard/27001

Пәннің коды мен атауы	**ASB 5209 Желілік қауіпсіздікті талдау**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Компьютерлік желілер, Желілік хаттамалар мен технологиялар, Ақпараттық қауіпсіздік негіздері (бакалавриат деңгейінде)
Пәннің постреквизиттері	Киберқауіпсіздіктегі зерттеу әдістері, Ақпараттық қауіпсіздік аудиті, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі, Ақпараттық қауіпсіздіктегі интеллектуалдық модельдер мен әдістер, Ақпараттық қауіпсіздіктің интеллектуалды жүйелеріндегі жүйелік талдау және модельдеу, Қауіптерді талдаудағы жасанды интеллект, Киберқауіпсіздіктегі генеративті жасанды интеллект
Пәнді оқу мақсаты	Желілік инфрақұрылымның қорғалуын талдау, трафик бойынша желілік шабуылдарды анықтау, желілік қорғау құралдарын баптау және бағалау, қорғалған желілік архитектураны жобалау дағдыларын қалыптастыру.

Пән мазмұны	Желілік инфрақұрылым қауіптерінің моделі және желілік шабуылдардың жіктелуі. ARP, IP, TCP, UDP, DNS хаттамаларының осалдықтары. Желілік трафикті ұстау және талдау (Wireshark). Желілік барлау, сканерлеу және қорғалуды бағалау (Nmap). Желіаралық экрандар мен NGFW, сүзгілеу саясаттарын жобалау. Шабуылдарды анықтау және алдын алу жүйелері (Suricata, Snort). Желіні сегменттеу, VLAN, микросегменттеу, VPN және IPsec. Сымсыз желілер (WPA3) мен IoT желілерінің қауіпсіздігі. DDoS-шабуылдардан қорғау, желіні мониторингтеу (NetFlow, SIEM).
Пәннің құзіреттілігі	- - біледі: желілік хаттамалардың осалдықтарын, желілік шабуылдардың жіктелуін және желілік қорғау технологияларын; - - түсінеді: желіаралық экрандардың, IDS/IPS, VPN жұмыс істеу және желіні сегменттеу қағидаттарын; - - қолдана алады: шабуылдарды анықтау және желі қорғалуын бағалау үшін трафикті талдау мен сканерлеу құралдарын; - - құзыретті: қорғалған желілік архитектураны жобалауда және желілік ағындарды басқаруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 38. 1. Якубов, Б.М., Мекебаева, А.К. Телекоммуникациялық жүйелердегі ақпараттар қауіпсіздігі: оқу құралы. — Алматы: Альманах, 2018. — 75 б. 39. 2. Басыня, Е.А. Сетевая информационная безопасность: учебник. — М.: НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. https://rmebrk.kz/book/1184075 40. 3. Даушеева, Н.Н. Стандарты сетевых технологий [Текст]: учеб. пособие / Н.Н. Даушеева.- Алматы: Эпиграф, 2023.- 160 с. 41. 4. Воробъев С.П., Широбокова С.Н., Литвяк Р.К. Компьютерные сети и сетевая безопасность: учебное пособие /Южно-Российский государственный политехнический университет (НПИ) им. М.И.Платова + Новочеркасск: ЮРГПУ (НПИ), 2022. -216с. https://kaznaru.elib.kz/ru/search/read_book/11390/ 42. 5. Усенова, А.Ж. Желілік технологиялар [Мәтін]: пәні бойынша дәрістер жинағы / А.Ж. Усенова, Ж.Д. Изтаев.- Алматы: Эпиграф, 2023.- 172 б. **Қосымша:** 43. 6. Усенова, А.Ж. Желілік технологиялар [Мәтін]: пәні бойынша дәрістер жинағы / А.Ж. Усенова, Ж.Д. Изтаев.- Алматы: Эпиграф, 2023.- 172 б. 44. 7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета. // Вестник КазГУ. - 2016. - №4. - С. 80–88. 45. 8. IEEE Computer Society. Intrusion Detection Systems and Network Security: Research Articles. — IEEE Xplore Digital

	Library, 2022–2024. https://ieeexplore.ieee.org/ 46. 9. Kikissagbe, B. R., & Adda, M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Electronics, 2024, 13(18), 3601. https://doi.org/10.3390/electronics13183601

Пәннің коды мен атауы	**AISB 5208 Қауіпсіздіктің аналитикалық ақпараттық жүйелері**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Деректер қоры, Ақпараттық қауіпсіздік негіздері, Ықтималдықтар теориясы және математикалық статистика (бакалавриат деңгейінде)
Пәннің постреквизиттері	Киберқауіпсіздіктегі зерттеу әдістері, Ақпараттық қауіпсіздік аудиті, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі, Ақпараттық қауіпсіздіктегі интеллектуалдық модельдер мен әдістер, Ақпараттық қауіпсіздіктің интеллектуалды жүйелеріндегі жүйелік талдау және модельдеу, Қауіптерді талдаудағы жасанды интеллект, Киберқауіпсіздіктегі генеративті жасанды интеллект
Пәнді оқу мақсаты	Аномалияларды анықтау және шешім қабылдауды қолдау үшін қауіпсіздік оқиғалары туралы деректерді жинау, корреляциялау және интеллектуалдық өңдеудің аналитикалық жүйелерін құру және қолдану дағдыларын қалыптастыру.
Пән мазмұны	АҚ-дағы деректер аналитикасы: деректер көздері, міндеттер, аналитикалық жүйелер архитектурасы. Оқиғалар журналдарын жинау, қалыпқа келтіру және сақтау (Syslog, CEF, JSON). SIEM жүйелері: архитектурасы, корреляция ережелері, анықтау сценарийлері. UEBA — мінез-құлықтық аналитика. Threat Intelligence: компрометация индикаторлары, STIX/TAXII, MISP. SOAR: әрекет етуді автоматтандыру және плейбуктер. Аномалияларды анықтауға арналған статистикалық әдістер мен Data Mining. Қауіпсіздік деректерін визуализациялау, SOC метрикалары мен KPI. Қауіпсіздіктің аналитикалық жүйесін жобалау (ELK/OpenSearch, Wazuh).
Пәннің құзіреттілігі	- - біледі: SIEM, SOAR, UEBA және Threat Intelligence платформаларының архитектурасы мен функцияларын; - - түсінеді: оқиғаларды қалыпқа келтіру және корреляциялау әдістерін, аномалияларды анықтаудың статистикалық негіздерін; - - қолдана алады: корреляция ережелері мен қауіптерді анықтау сценарийлерін әзірлеу үшін аналитикалық

	платформаларды; - - құзыретті: қауіпсіздік деректерін талдауда және интерпретациялауда, ұйымның аналитикалық жүйесін жобалауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 47. 1. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems and computing. Volume 657). 48. 2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 49. 3. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 50. 4. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с. https://baraev.elib.kz/ru/search/read_book/3586/ 51. 5. Мартынов, А.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / А.П. Мартынов, И.А. Мартынова, А.А. Русаков.- 2-е изд.- Москва: Ай Пи Ар Медиа, 2024.- 130 с. **Қосымша:** 52. 6. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 53. 7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета. // Вестник КазГУ. - 2016. - №4. - С. 80–88. 54. 8. Кайбасова Д.Ж. Автоматтандырылған ақпараттық жүйелерді жобалауда деректер қорын қолдану тәсілдері: Монография /Д.Ж. Кайбасова, Б.О. Мухаметжанова, Э.К. Сейпишева; Қарағанды мемлекеттік техникалық университеті. – Алматы: Эверо, 2020. - 186 б. https://baraev.elib.kz/ru/search/read_book/3992/ 55. 9. Patel, S. J., Raj, P., Visconti, A. (Eds.) Security, Privacy and Data Analytics. — Singapore: Springer Nature, 2022. — 400+ p. Available at: https://link.springer.com/book/10.1007/978-981-16-9089-1

Пәннің коды мен атауы	**KMSZI 5211 Ақпаратты қорғаудың криптографиялық әдістері мен құралдары**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК

Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Дискретті математика, Криптография негіздері, Ақпараттық қауіпсіздік негіздері (бакалавриат деңгейінде)
Пәннің постреквизиттері	Ақпараттық қауіпсіздік аудиті, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі
Пәнді оқу мақсаты	Криптографиялық қорғаудың математикалық негіздері мен заманауи әдістері туралы тереңдетілген білімді, ақпараттың құпиялылығын, тұтастығын және түпнұсқалығын қамтамасыз ету үшін криптографиялық алгоритмдерді негізді таңдау, талдау және қолдану біліктерін қалыптастыру.
Пән мазмұны	Криптографияның математикалық негіздері: сандар теориясы, ақырлы өрістер, есептеу күрделілігі. Симметриялық блоктық және ағындық шифрлар, шифрлау режимдері. Хэш-функциялар және хабарламаларды аутентификациялау кодтары (SHA-2/3, HMAC). Асимметриялық криптожүйелер: RSA, Диффи–Хеллман, эллиптикалық қисықтар. Электрондық цифрлық қолтаңба және ашық кілттер инфрақұрылымы (PKI), ҚР ҰКО. Кілттерді басқару және HSM. Криптографиялық қорғаудың бағдарламалық-аппараттық құралдары, талаптар және сертификаттау. Криптоталдау және жанама арналар арқылы шабуылдар. Постквантық криптография (ML-KEM, ML-DSA).
Пәннің құзіреттілігі	- - біледі: криптографияның математикалық негіздерін, криптожүйелер кластарын және криптографиялық қорғау стандарттарын; - - түсінеді: алгоритмдердің беріктік қасиеттерін және PKI мен кілттерді басқару жүйелерін құру қағидаттарын; - - қолдана алады: құпиялылықты, тұтастықты және түпнұсқалықты қамтамасыз ету үшін симметриялық және асимметриялық алгоритмдерді, хэш-функцияларды және ЭЦҚ-ны; - - құзыретті: криптографиялық қорғау құралдарын, соның ішінде постквантық шешімдерді салыстырмалы талдауда және негізді таңдауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 56. 1. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости [Текст]: учеб. пособие / А.В. Черемушкин.- М.: Академия, 2009.- 272с. 57. 2. Кожомбердиева, Г.И., Глухарев, М.Л. Криптографическая защита информации и управление доступом на платформе Java. — СПб., 2016. — 87 с. https://rmebrk.kz/book/1189323 58. 3. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems – Криптографические системы : Textbook. . - Almaty: Bastau,

	2021. - 320- ISBN 978-601-7660-08-6. https://rmebrk.kz/book/1176885 59. 4. Абдикаликов, К.А. Анализ каналов уязвимости криптографической системы RSA. — 2012. https://rmebrk.kz/book/54167 60. 5. Айтхожаева, Е.Ж., Тынымбаев, С. Аспекты аппаратного приведения по модулю в асимметричной криптографии. — 2014. https://rmebrk.kz/book/1026852 **Қосымша:** 61. 6. Фомичев, В.М. Криптография - наука о тайнописи [Текст]: учеб. пособие / В.М. Фомичев; Фин. ун-т при Правительстве РФ.- М.: Прометей, 2020.- 66 с. 62. 7. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б. 63. 8. Тынымбаев, С.Т., Айтхожаева, Е.Ж. Аппаратное ускорение приведения по модулю для асимметричной криптографии. — 2016. — С.158–160. https://rmebrk.kz/book/1151931 64. 9. Renner, R., & Wolf, R. (2022). Quantum advantage in cryptography. arXiv. https://arxiv.org/abs/2206.04078

Пәннің коды мен атауы	**PPKP 5210 Криптографиялық хаттамаларды құру қағидалары**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7M06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	1
Пәннің пререквизиттері	Дискретті математика, Криптография негіздері, Компьютерлік желілер (бакалавриат деңгейінде)
Пәннің постреквизиттері	Ақпараттық қауіпсіздік аудиті, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі
Пәнді оқу мақсаты	Берілген қауіпсіздік қасиеттері бар криптографиялық хаттамаларды жобалау, олардағы осалдықтарды анықтау және формальды әдістер көмегімен олардың қасиеттерін верификациялау қабілетін қалыптастыру.
Пән мазмұны	Криптографиялық примитивтер хаттамалардың негізі ретінде, қауіпсіздік модельдері. Долев–Яо бұзушы моделі, хаттамаларға шабуылдар (қайталау, шағылдыру, «ортадағы адам»). Аутентификация хаттамалары: парольдік, «сұрау–жауап», Kerberos, FIDO2. Кілттерді тарату және келісу хаттамалары. Қорғалған арналар хаттамалары: TLS 1.3, IPsec, SSH. Формальды талдау: BAN-логика, ProVerif, Tamarin.

	Нөлдік жариялау хаттамалары және қауіпсіз көпжақты есептеулер. Электрондық қолтаңба хаттамалары, блокчейн және смарт-келісімшарттар. Хаттамалардың постквантық миграциясы.
Пәннің құзіреттілігі	- - біледі: криптографиялық хаттамалардың кластарын, бұзушы модельдерін және хаттамаларға типтік шабуылдарды; - - түсінеді: аутентификация, кілттерді тарату және қорғалған арналар хаттамаларын құру қағидаттарын; - - қолдана алады: хаттамалардың қауіпсіздік қасиеттерін талдау үшін формальды әдістер мен верификация құралдарын; - - құзыретті: хаттамаларды жобалауда және нақты АЖ үшін қорғалған алмасу хаттамаларын таңдау мен конфигурациялауды негіздеуде.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 65. 1. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости [Текст]: учеб. пособие / А.В. Черемушкин.- М.: Академия, 2009.- 272с.- (Высшее профессиональное образование). 66. 2. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 67. 3. Сидельников, В.М. Криптография и теория кодирования. - М.: МГУ, 2006. - 22 с. https://rmebrk.kz/book/1010922 68. 4. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems – Криптографические системы : Textbook. . - Almaty: Bastau, 2021. - 320- ISBN 978-601-7660-08-6. https://rmebrk.kz/book/1176885 **Қосымша:** 69. 5. Фомичев, В.М. Криптография - наука о тайнописи [Текст]: учеб. пособие / В.М. Фомичев; Фин. ун-т при Правительстве РФ.- М.: Прометей, 2020.- 66 с. 70. 6. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б. 71. 7. Тынымбаев, С.Т., Айтхожаева, Е.Ж. Аппаратное ускорение приведения по модулю для асимметричной криптографии. — 2016. — С.158–160. https://rmebrk.kz/book/1151931 72. 8. IEEE Computer Society. Cryptographic Systems and Security. — IEEE Xplore Digital Library, 2022–2024. https://ieeexplore.ieee.org/

Пәннің коды мен атауы	**PU 5205 Басқару психологиясы**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ:

	_____
Пән циклі	БП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	3
Оқыту формасы	Күндізгі
Семестр	2
Пәннің пререквизиттері	Жоғары мектептің педагогикасы
Пәннің постреквизиттері	Ақпараттық қауіпсіздікті басқару технологиялары, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Магистранттарда басқару қызметінің психологиялық заңдылықтары туралы білімді және оларды кәсіби ортада жағдайларды талдау, негізделген шешімдер қабылдау, командалар мен жобаларды басқару үшін қолдану біліктерін қалыптастыру.
Пән мазмұны	Басқару психологиясының пәні мен міндеттері. Басшының тұлғасы және басшылық стильдері. Көшбасшылық теориялары. Персоналды ынталандыру психологиясы. Шағын топтар психологиясы және команданы қалыптастыру. Белгісіздік пен тәуекел жағдайында басқарушылық шешімдер қабылдау психологиясы. Басқарудағы коммуникациялар, іскерлік келіссөздер. Ұйымдағы жанжалдар және оларды шешу әдістері. Стресс-менеджмент және кәсіби күйзелістің алдын алу. Ұйымдық мәдениет және өзгерістерді басқару. Ақпараттық қауіпсіздікті қамтамасыз етудегі адам факторы.
Пәннің құзіреттілігі	- - біледі: басқару қызметінің психологиялық заңдылықтарын, көшбасшылық пен ынталандыру теорияларын; - - түсінеді: басқаруда және ақпараттық қауіпсіздікті қамтамасыз етуде адам факторының, ұйымдық мәдениет пен коммуникациялардың рөлін; - - қолдана алады: жағдайларды психологиялық талдау, жанжалдарды басқару және команданы қалыптастыру әдістерін; - - құзыретті: кәсіби ортада негізделген басқарушылық шешімдер қабылдауда және ұжымды басқаруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 73. 1. Кабаченко Т.С. Психология управления: учебник. – 4-е изд. – М.: Юрайт, 2019. – 409 с. 74. 2. Урбанович А.А. Психология управления: учебное пособие. – Минск: Харвест, 2003. – 640 с. 75. 3. Robbins S.P., Judge T.A. Organizational Behavior. – 18th ed. – Harlow: Pearson, 2019. – 744 p. **Қосымша:** 76. 4. Hadnagy C. Social Engineering: The Science of Human Hacking. – 2nd ed. – Indianapolis: Wiley, 2018. – 320 p. 77. 5. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Пәннің коды мен атауы	**MIK 5313 Киберқауіпсіздіктегі зерттеу әдістері**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	6
Оқыту формасы	Күндізгі
Семестр	2
Пәннің пререквизиттері	Ғылым тарихы мен философиясы, Шет тілі (кәсіби), Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері
Пәннің постреквизиттері	Зерттеу практикасы, Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары, Магистранттың ғылыми-зерттеу жұмысы
Пәнді оқу мақсаты	Магистранттарда киберқауіпсіздік саласындағы ғылыми зерттеудің әдіснамалық мәдениетін қалыптастыру: экспериментті жоспарлау және жүргізу, деректерді өңдеу және интерпретациялау, нәтижелердің дұрыстығын бағалау және оларды ғылыми жарияланым түрінде ұсыну біліктері.
Пән мазмұны	Киберқауіпсіздіктегі ғылыми зерттеудің әдіснамасы. Зерттеу мәселесін, мақсатын, гипотезасын және міндеттерін қою. Ғылыми ақпаратты іздеу және талдау: Scopus, Web of Science, IEEE Xplore; әдебиеттерге жүйелі шолу (PRISMA). Сандық, сапалық және аралас әдістер. Экспериментті жоспарлау, сынақ стендтері мен киберполигондар. АҚ зерттеулеріне арналған деректер жиындары және олардың шектеулері. Нәтижелерді статистикалық өңдеу, гипотезаларды тексеру, қайталанымдылық. Қауіптерді модельдеу және тәуекелдерді бағалау зерттеу әдістері ретінде. АҚ-дағы зерттеулер этикасы, осалдықтарды жауапты ашу. Ғылыми мақала мен магистрлік диссертацияны дайындау.
Пәннің құзіреттілігі	- - біледі: киберқауіпсіздік саласындағы ғылыми зерттеудің әдіснамасын, әдістері мен кезеңдерін; - - түсінеді: экспериментті жоспарлау қағидаттарын, деректерге қойылатын талаптарды және нәтижелердің дұрыстық өлшемдерін; - - қолдана алады: ғылыми ақпаратты іздеу мен талдаудың, эксперименттік деректерді статистикалық өңдеу мен интерпретациялаудың әдістерін; - - құзыретті: этикалық талаптарды сақтай отырып, зерттеу нәтижелерін ғылыми жарияланым түрінде дайындауда және ұсынуда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 78. 1. Боуш, Г.Д., Разумов, В.И. Методология научного исследования (в кандидатских и докторских диссертациях): учебник. — М.: ИНФРА-М, 2025. — 227 с. 79. 2. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет

	ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ 80. 3. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems and computing. Volume 657). 81. 4. Creswell, J. W., Creswell, J. D. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. — 5th ed. — Thousand Oaks: SAGE Publications, 2018. — 304 p. — ISBN 978-1506386706. https://us.sagepub.com/en-us/nam/research-design/book255675 82. 5. Федотова, Е.Л. Информационные технологии в науке и образовании [Текст]: учеб. пособие / Е.Л. Федотова, А.А. Федотов.- Москва: "ФОРУМ"; ИНФРА-М, 2024.- 335 с.- (Высшее образование). **Қосымша:** 83. 6. Автоматизация физических исследований и эксперимента компьютерные измерения и виртуальные приборы на основе Lagvlew [Текст]: 30 лекций / П.А.Бутырин, Т.А.Васьковская, В.В.Каратаев [и др.].- 2- изд.,.- М.: ДМК Пресс, 2011.- 265 с. 84. 7. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с. 85. 8. Oroni, C. Z., Xianping, F., Ndunguru, D. D., Ani, A. Enhancing cyber safety in e-learning environment through cybersecurity awareness and policy compliance. — Computers & Security, Elsevier, 2025. https://doi.org/10.1016/j.cose.2024.104276 86. 9. Czaja, P., Gdowski, B., Niemiec, M., et al. Cybersecurity challenges and opportunities of machine learning-based AI. — Neural Computing and Applications, Springer, 2025. https://link.springer.com/article/10.1007/s00521-025-11604-9

Пәннің коды мен атауы	**UPK 5314 Киберқауіпсіздік жобаларын басқару**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	2
Пәннің пререквизиттері	Ақпараттық жүйелердің киберқауіпсіздігі / Операциялық жүйелердің қауіпсіздігін талдау
Пәннің постреквизиттері	Ақпараттық қауіпсіздікті басқару технологиялары, Ақпараттық қауіпсіздіктің интеллектуалды жүйелеріндегі жүйелік талдау және модельдеу, Магистранттың ғылыми-зерттеу жұмысы
Пәнді оқу мақсаты	Магистранттарда тәуекелдерді, ресурстарды және стандарттар талаптарын ескере отырып, ақпараттық қауіпсіздікті қамтамасыз

	ету жүйелерін құру және дамыту жобаларын бастау, жоспарлау, іске асыру және бақылау саласындағы құзыреттерді қалыптастыру.
Пән мазмұны	АҚ саласындағы жоба және жобалық қызмет. Жобаларды басқару стандарттары: PMBOK, ISO 21500, PRINCE2. Ақпаратты қорғау жүйесін құру жобасының өмірлік циклі. Жобаны бастау: негіздеме, жарғы, мүдделі тараптар. Мазмұнды, мерзімдерді, құнды және ресурстарды жоспарлау (WBS, Гант диаграммасы, критикалық жол әдісі). Жоба тәуекелдерін басқару. Икемді әдіснамалар (Scrum, Kanban) және DevSecOps жобалары. Команда мен коммуникацияларды басқару. Ақпаратты қорғау құралдарын сатып алу, техникалық тапсырма. Орындалуын бақылау, метрикалар және жобаны жабу.
Пәннің құзіреттілігі	- - біледі: жобаларды басқару стандарттары мен әдіснамаларын, АҚ саласындағы жобаның өмірлік циклін; - - түсінеді: ақпаратты қорғау жобасының мазмұны, мерзімдері, құны, сапасы және тәуекелдері арасындағы өзара байланысты; - - қолдана алады: жобаны жоспарлау, тәуекелдерді басқару және орындалуын бақылау құралдарын; - - құзыретті: жобалық құжаттаманы, техникалық тапсырманы әзірлеуде және жобалық команданы басқаруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 87. 1. Ахметов, К.А. Моделирование бизнес-решений [Текст]: учебник для вузов / К.А. Ахметов.- Алматы: Эверо, 2022.- 444 с. 88. 2. Емелина Н.К. Методы принятия оптимальных решений: учебно-практическое пособие / Н.К. Емелина.– Алматы: Эверо, 2020.- 216 с. https://baraev.elib.kz/ru/search/read_book/1170/ 89. 3. Ахметов, К.А. Моделирование бизнес-решений [Текст]: учебник для вузов / К.А. Ахметов.- Алматы: EDP Hub (Идипи Хаб); Ай Пи Ар Медиа, 2024.- 558 с. 90. 4. Kirgizbayeva, B.Zh. Modeling of business decisions [Текст]: manual for master degree students studying in all educational programs of the university / B.Zh. Kirgizbayeva, K.A. Akhmetov, Zh.Zh. Kozhamkulova; KazNAU.- Almaty: Aytumar, 2021.- 104 p. **Қосымша:** 91. 5. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 92. 6. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2022. — 30 p. https://www.iso.org/standard/27001 93. 7. Senft, S., Gallegos, F., Davis, A. Information Technology Control and Audit. — Elsevier, 2016. https://www.sciencedirect.com/book/9780128024379 94. 8. Behl, A. et al. Cybersecurity compliance and auditing mechanisms. — Elsevier, 2023. https://www.sciencedirect.com/science/article/pii/S0268401223004567

Пәннің коды мен атауы	**AIB 5312 Ақпараттық қауіпсіздік аудиті**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	5
Оқыту формасы	Күндізгі
Семестр	2
Пәннің пререквизиттері	Ақпараттық жүйелердің киберқауіпсіздігі / Операциялық жүйелердің қауіпсіздігін талдау, Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Ақпаратты қорғаудың криптографиялық әдістері мен құралдары / Криптографиялық хаттамаларды құру қағидалары
Пәннің постреквизиттері	Ақпараттық қауіпсіздікті басқару технологиялары, Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы
Пәнді оқу мақсаты	Магистранттарда ақпараттық қауіпсіздік аудитін жоспарлау және жүргізу, ақпараттық жүйелердің тәуекелдері мен қорғалу деңгейін бағалау, ұлттық және халықаралық стандарттар талаптарына сәйкестікті талдау және аудиторлық қорытынды дайындау бойынша құзыреттерді қалыптастыру.
Пән мазмұны	АҚ аудитінің ұғымы, түрлері және мақсаттары. Нормативтік база: ҚР «Ақпараттандыру туралы» Заңы, АКТ және АҚ-ны қамтамасыз ету саласындағы бірыңғай талаптар, ISO/IEC 27001, ISO/IEC 27007, ISO 19011. Аудитті жоспарлау: көлемі, бағдарламасы, ресурстары, аудиторлық топ. Аудиторлық дәлелдемелерді жинау: құжаттаманы талдау, сұхбат жүргізу, техникалық тексерулер. Периметр мен ішкі инфрақұрылымның қорғалуын талдау, осалдықтарды сканерлеу. ОЖ, ДҚБЖ және желілік жабдық конфигурацияларының аудиті. Аудит шеңберінде бастапқы кодты талдау және енуге тестілеу. Тәуекелдерді бағалау және сәйкессіздіктерді анықтау. Есеп пен аудиторлық қорытынды дайындау, түзету іс-шараларының жоспары.
Пәннің құзіреттілігі	- - біледі: ақпараттық қауіпсіздік аудитінің түрлерін, кезеңдерін және нормативтік базасын; - - түсінеді: аудиторлық дәлелдемелерді жинау, тәуекелдерді бағалау және аудит объектілерінің қорғалуын талдау әдістерін; - - қолдана алады: қорғалуды талдаудың аспаптық құралдарын және стандарттар талаптарына сәйкестікті тексеру әдістемелерін; - - құзыретті: аудитті жоспарлауда, оның нәтижелерін құжаттауда және аудиторлық қорытынды дайындауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 95. 1. Прохорова, О.В. Информационная безопасность и защита информации. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. http://rmebrk.kz/book/1183813 96. 2. Зенков, А.В. Информационная безопасность и защита

	информации : учебное пособие для вузов. . - М: Юрайт, 2022. - 104 с. - (Высшее образование). - ISBN 978-5-534-14590-8. http://rmebrk.kz/book/1179658 97. 3. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 98. 4. Жангисина, Г.Д. Теория и методика компьютерного моделирования для задач базы данных и глобальной сети [Текст]: учеб. пособие / Г.Д. Жангисина, Т. Хакимова.- Алматы: Ғылым, 2007.- 94с. https://lib.kaznaru.edu.kz/res/Injenerlik/Hakimova%20T.7.index.pdf **Қосымша:** 99. 5. Peltier, T. R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. — Springer, 2020. https://link.springer.com/book/10.1007/978-3-030-58290-6 100.6. ISO/IEC 27001:2022 Information security management systems — Requirements. — ISO, 2022 https://www.iso.org/standard/27001 101.7. Senft, S., Gallegos, F., Davis, A. Information Technology Control and Audit. — Elsevier, 2016. https://www.sciencedirect.com/book/9780128024379

БІЛІМ БЕРУ БАҒДАРЛАМАСЫ: 7М06301 – «АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕЛЕРІ»

Берілетін дәреже: 7М06301 – «Ақпараттық қауіпсіздіктің интеллектуалды жүйелері» білім беру бағдарламасы бойынша техника ғылымдарының магистрі

2 КУРС

Цикл	Код	Пәндер	Академ. кредиттер
3 семестр – 30 академиялық кредит			
Жоғары оқу орны компоненті – 7 кр.			
БеП	ITAZI 6310	Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары	7
Таңдау компоненті – 20 кр.			
БеП	BBDOI 6315	Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі	7
	TUIB 6316	Ақпараттық қауіпсіздікті басқару технологиялары	
БеП	IMMIB 6317	Ақпараттық қауіпсіздіктегі интеллектуалдық модельдер мен әдістер	7
	SAMISIB 6318	Ақпараттық қауіпсіздіктің интеллектуалды жүйелеріндегі жүйелік талдау және модельдеу	
БеП	IIAU 6319	Қауіптерді талдаудағы жасанды интеллект	6
	GIIK 6320	Киберқауіпсіздіктегі генеративті жасанды интеллект	
Магистранттың ғылыми-зерттеу жұмысы – 3 кр.			
ҒЗЖ	NIRM 6503	Магистранттың ғылыми-зерттеу жұмысы	3
4 семестр – 30 академиялық кредит			
Жоғары оқу орны компоненті – 5 кр.			
БеП	IP 6311	Зерттеу практикасы	5
Магистранттың ғылыми-зерттеу жұмысы – 17 кр.			
ҒЗЖ	NIRM 6504	Магистранттың ғылыми-зерттеу жұмысы	17
Қорытынды аттестаттау – 8 кр.			
ҚА	—	Магистрлік диссертацияны рәсімдеу және қорғау (МДРҚ)	8

Пәнді сипаттау формуляры

Пәннің коды мен атауы	**ITAZI 6310 Ақпаратты талдау және қорғаудың интеллектуалдық технологиялары**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ЖК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	7
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Киберқауіпсіздіктегі зерттеу әдістері, Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Ақпаратты қорғаудың криптографиялық әдістері мен құралдары / Криптографиялық хаттамаларды құру қағидалары
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Магистранттарда қауіпсіздік деректерін талдау, аномалияларды анықтау, киберқауіптерді анықтау және болжау үшін Data Mining, машиналық оқыту және жасанды интеллект әдістерін қолдану және әзірлеу бойынша құзыреттерді қалыптастыру.
Пән мазмұны	Ақпаратты қорғау жүйелеріндегі интеллектуалдық технологиялар. Қауіпсіздік деректерінің көздері мен түрлері. Деректерді алдын ала өңдеу, белгілерді жасау және іріктеу. Data Mining әдістері: жіктеу, кластерлеу, ассоциативтік ережелер. Аномалиялар мен шабуылдарды анықтау. АҚ міндеттеріндегі нейрондық желілер және терең оқыту. Мәтіндер мен оқиғалар журналдарын талдау (NLP). SOC-тағы шешім қабылдауды қолдаудың интеллектуалдық жүйелері. Модельдердің сапасын бағалау және түсіндірілуі (XAI). Интеллектуалдық жүйелердің өз қауіпсіздігі: жарыспалы шабуылдар, деректерді улау. Python тілінде интеллектуалдық қорғау жүйесінің прототипін әзірлеу.
Пәннің құзіреттілігі	- - біледі: ақпаратты талдау және қорғау үшін қолданылатын Data Mining, машиналық оқыту және жасанды интеллект әдістерін; - - түсінеді: қауіпсіздік деректерінің ерекшеліктерін және интеллектуалдық модельдердің шектеулерін, соның ішінде олардың жарыспалы шабуылдарға осалдығын; - - қолдана алады: аномалияларды анықтау, қауіптерді жіктеу және оқиғалар журналдарын талдау үшін интеллектуалдық әдістерді; - - құзыретті: деректерді өңдеу және қауіптерді болжау модельдерін әзірлеуде, бағалауда және оңтайландыруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 102.1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы

	искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 103.2. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 104.3. Яворский, В.В. Процессы формирования и развития информационных систем [Текст]: учеб. пособие / В.В. Яворский, Т.О. Перемитина.- Алматы: Эпиграф, 2022.- 108 с. 105.4. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 106.5. Партыка, Т.Л. Информационная безопасность [Текст]: учеб. пособие / Т.Л. Партыка, И.И. Попов.- 5-е изд., перераб. и доп.- М.: Форум; ИНФРА-М, 2014.- 432 с **Қосымша:** 107.6. Абдиев К.С. Информационные технологии производства статистических данных [Текст] / Абдиев К.С.- Алматы: Агенства РК по статистике, 2006.- 280 с. 108.7. Черикбаева, Л.Ш. Деректерді талдаудың топтық шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 109.8. Остроух, А.В. Введение в искусственный интеллект: монография. — Красноярск: Научно-инновационный центр, 2020. — 250 с. — ISBN 978-5-907208-26-1. — DOI: 10.12731/978-5-907208-26-1. https://rmebrk.kz/book/1188729 110.9. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с.

Пәннің коды мен атауы	**BBDOI 6315 Үлкен деректер мен бұлттық инфрақұрылымдардың қауіпсіздігі**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	7
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Операциялық жүйелердің қауіпсіздігін талдау / Ақпараттық жүйелердің киберқауіпсіздігі, Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Ақпаратты қорғаудың криптографиялық әдістері мен құралдары / Криптографиялық хаттамаларды құру қағидалары
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Үлкен деректерді өңдеудің қорғалған конвейерлері мен

	бұлттық орталарды жобалау, қауіпсіздік деректерін ауқымды талдау, аномалияларды анықтау және дербес деректерді қорғау мен құпиялылықты қамтамасыз ету қабілетін қалыптастыру.
Пән мазмұны	Үлкен деректер архитектуралары (Hadoop, Spark, Kafka) және қауіптер модельдері. IaaS, PaaS, SaaS бұлттық қызмет модельдері және бөлінген жауапкершілік моделі. Бұлттағы қолжетімділікті басқару, деректерді сақтау және беру кезінде шифрлау. Контейнерлер мен Kubernetes қауіпсіздігі, Infrastructure as Code тексеру. Бөлінген қоймалар мен NoSQL қорғау. Құпиялылық: анонимдеу, бүркеншіктеу, дифференциалды құпиялылық, гомоморфты шифрлау. Үлкен деректер платформаларында журналдардың ағындық аналитикасы және аномалияларды анықтау. Бұлттық қауіпсіздікті мониторингтеу: CSPM, CWPP, бұлттық SIEM. ISO/IEC 27017/27018, дербес деректер туралы ҚР заңнамасы.
Пәннің құзіреттілігі	- - біледі: үлкен деректер платформалары мен бұлттық орталардың архитектураларын, олардың қауіптер модельдерін және қорғау механизмдерін; - - түсінеді: бөлінген жауапкершілік моделін және деректер құпиялылығын қамтамасыз ету әдістерін; - - қолдана алады: қауіпсіздік оқиғаларын талдау және аномалияларды анықтау үшін үлкен деректерді өңдеу технологияларын; - - құзыретті: дербес деректерді қорғау талаптарын ескере отырып, қорғалған бұлттық орталар мен деректер конвейерлерін жобалауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 111.1. Бимұрат, Ж. Big Data технологияларының негіздері [Мәтін]: оқу құралы / Ж. Бимұрат; Ғ.Дәукеев атын. Алматы энергетика және байланыс ун-ті КЕАҚ.- Алматы:Альманахъ,2023.-131б. 112.2. Bart Baesens Analytics in a Big Data World: The Essential Guide to Data Science and its Applications. : Wiley, 2014. - 243- ISBN 978-1-118-89270-1. https://rmebrk.kz/book/1178447 113.3. Цехановский, В.В. Управление данными [Текст]: учебник / В.В. Цехановский, В.Д. Чертовской.- СПб.: Лань, 2015.- 432 с 114.4. Mukasheva, A.K. et al. Big Data analytics : Textbook (for students of all specialties). / A.K. Mukasheva, T.F. Umarov, I.A. Zimin. - Almaty: Lantar books LLC, 2022. - 116- ISBN 978-601-7659-94-3. https://rmebrk.kz/book/1177465 115.5. Силен, Д. Основы Data Science и Big Data. Python и наука о данных [Текст] / Д. Силен, А. Мейсман, М. Али.- СПб.: Питер, 2020.- 336 с.- (Б-ка программиста). **Қосымша:** 116.6. Казагачев, В.Н. Цифровизация производства (по отраслям) [Текст]: учеб.-метод. пособие / В.Н. Казагачев, А.А. Мусина.- Алматы: Эпиграф, 2023.- 204 с. 117.7. Черикбаева, Л.Ш. Деректерді талдаудың топтық

	шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 118.8. Кайбасова Д.Ж. Автоматтандырылған ақпараттық жүйелерді жобалауда деректер қорын қолдану тәсілдері: Монография /Д.Ж. Кайбасова, Б.О. Мухаметжанова, Э.К. Сейпишева; Қарағанды мемлекеттік техникалық университеті. – Алматы: Эверо, 2020. - 186 б. https://baraev.elib.kz/ru/search/read_book/3992/ 119.9. García, L., Parra, L., Jimenez, J. M., Lloret, J. IoT and Big Data Analytics for Smart Agriculture. — Springer Nature, 2020. https://link.springer.com/book/10.1007/978-3-030-35389-6

Пәннің коды мен атауы	**TUIB 6316 Ақпараттық қауіпсіздікті басқару технологиялары**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	7
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Операциялық жүйелердің қауіпсіздігін талдау / Ақпараттық жүйелердің киберқауіпсіздігі, Ақпараттық қауіпсіздік аудиті, Киберқауіпсіздік жобаларын басқару
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Ұйымның ақпараттық қауіпсіздік менеджменті жүйесін жобалау, енгізу және жетілдіру, тәуекелдерді өңдеу бойынша шешімдерді негіздеу және АҚ-ны басқару процестерінің тиімділігін бағалау қабілетін қалыптастыру.
Пән мазмұны	ҚР-дағы АҚ нормативтік-құқықтық базасы: «Ақпараттандыру туралы» Заң, АКТ және АҚ-ны қамтамасыз ету саласындағы бірыңғай талаптар. Стандарттар мен фреймворктер: ISO/IEC 27000, NIST CSF 2.0, COBIT. АҚМЖ құру, PDCA циклі. ISO/IEC 27005 бойынша АҚ тәуекелдерін басқару. Саясаттарды, регламенттерді және нормативтік құжаттаманы әзірлеу. Инциденттерді басқару (ISO/IEC 27035) және АҚ жедел орталықтарымен өзара әрекеттесу. Бизнестің үздіксіздігін басқару (ISO 22301). АҚМЖ метрикалары және тиімділігін бағалау (ISO/IEC 27004), сертификаттауға дайындық. GRC платформалары.
Пәннің құзіреттілігі	- - біледі: АҚ-ны басқару саласындағы ұлттық нормативтік базаны және халықаралық стандарттарды; - - түсінеді: АҚМЖ құруға процестік тәсілді және тәуекелдерді бағалау мен өңдеу әдістерін; - - қолдана алады: саясаттарды, регламенттерді және бизнес үздіксіздігін қамтамасыз ету жоспарларын әзірлеу әдістемелерін; - - құзыретті: АҚМЖ тиімділігін бағалауда және ұйымды

	аудит пен сертификаттауға дайындауда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 120.1. Борух, О.А. Облачные вычисления [Текст]: учеб. пособие / О.А. Борух.- Алматы: Alem book, 2024.- 200 с. 121.2. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 122.3. Гумерова, Г.И. Электронное правительство [Текст]: учебник для вузов / Г.И. Гумерова, Э.Ш. Шаймиева.- 5-е изд., испр. и доп.- М.: Юрайт, 2023.- 227 с. 123.4. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems. — Almaty: Bastau, 2021. — 320 p. https://rmebrk.kz/book/1176885 124.5. Жатканбаева, А.Е. Информационное право (Общая часть) [Текст]: учеб. пособие / А.Е. Жатканбаева; КазНУ им. аль-Фараби.- Алматы: Қазақ университеті, 2020.- 150 с. **Қосымша:** 125.6. Мазалов, В.В. Математическая теория игр и приложения [Текст]: учеб. пособие / В.В. Мазалов.- СПб.: Лань, 2010.- 448 с. 126.7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета // Вестник КазГУ. — 2016. — № 4. — С. 80–88. 127.8. Тлеккабылова, Д.Ж., Иксебаева, Ж.С. Информационная безопасность как элемент информационной культуры. - 2014. - С.103-104. https://rmebrk.kz/book/1144347 128.9. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б.

Пәннің коды мен атауы	**IMMIB 6317 Ақпараттық қауіпсіздіктегі интеллектуалдық модельдер мен әдістер**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	7
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Киберқауіпсіздіктегі зерттеу әдістері
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Белгісіздік пен деректердің толық болмауы жағдайында

	шабуылдарды анықтау, зиянды БҚ-ны жіктеу және тәуекелдерді бағалау міндеттері үшін интеллектуалдық модельдерді әзірлеу, оқыту, бағалау және оңтайландыру қабілетін қалыптастыру.
Пән мазмұны	АҚ-дағы интеллектуалдық жүйелер: міндеттер кластары және әдістерге шолу. Қауіпсіздік деректерін дайындау, эталондық жиындар (CIC-IDS, UNSW-NB15). Шабуылдар мен зиянды БҚ-ны анықтауға арналған машиналық оқытудың классикалық әдістері. Нейрожелілік модельдер және терең оқыту. Тәуекелдерді бағалау үшін анық емес логика және анық емес шығару. Байес желілері және қауіптердің ықтималдық модельдері. Қорғау жүйелерін оңтайландырудың эволюциялық және үйірлік алгоритмдері. Модельдердің сапа метрикалары, валидациясы және түсіндірілуі (XAI). Жарыспалы машиналық оқыту және модельдердің тұрақтылығы.
Пәннің құзіреттілігі	- - біледі: ақпараттық қауіпсіздік міндеттерінде қолданылатын интеллектуалдық модельдер мен әдістердің кластарын; - - түсінеді: модельдердің шектеулерін, олардың сапа метрикаларын және жарыспалы шабуылдарға тұрақтылық мәселелерін; - - қолдана алады: қауіптерді анықтау және тәуекелдерді бағалау үшін машиналық оқыту, анық емес логика және ықтималдық шығару әдістерін; - - құзыретті: белгісіздік жағдайында интеллектуалдық модельдерді әзірлеуде, валидациялауда және оңтайландыруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 129.1. Андрейчиков, А.В., Андрейчикова, О.Н., 2024. — 530 с. 130.2. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 131.3. Шукаев, Д.Н. Прикладные методы оптимизации [Текст]: учебник / Д.Н. Шукаев; МОН РК.- Алматы: Эверо, 2020.- 220 с. 132.4. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 133.5. Силен, Д. Основы Data Science и Big Data. Python и наука о данных [Текст] / Д. Силен, А. Мейсман, М. Али.- СПб.: Питер, 2020.- 336 с.- (Б-ка программиста). **Қосымша:** 134.6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 135.7. Бурибаев, Ж.А. Нысанды тану мен жіктеу жүйесіне арналған машиналық оқытудың тиімді алгоритмдерін әзірлеу

	[Мәтін]: монография / Ж.А. Бурибаев; әл-Фараби атын. ҚазҰУ.- Алматы: Дарын, 2022.- 126 б. 136.8. Остроух, А.В. Введение в искусственный интеллект: монография. — Красноярск: Научно-инновационный центр, 2020. — 250 с. — ISBN 978-5-907208-26-1. — DOI: 10.12731/978-5-907208-26-1. https://rmebrk.kz/book/1188729 137.9. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с.

Пәннің коды мен атауы	**SAMISIB 6318 Ақпараттық қауіпсіздіктің интеллектуалды жүйелеріндегі жүйелік талдау және модельдеу**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	7
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Киберқауіпсіздіктегі зерттеу әдістері, Киберқауіпсіздік жобаларын басқару
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Күрделі ақпараттық және әлеуметтік-техникалық жүйелерді жүйелік талдау мен модельдеу әдіснамасын, қорғау жүйелерінің модельдерін құру, олардың тиімділігі мен сенімділігін бағалау және белгісіздік жағдайында қауіпсіздікті арттыру шешімдерін оңтайландыру біліктерін қалыптастыру.
Пән мазмұны	Жүйелік талдау негіздері: жүйе, құрылым, қасиеттер; АҚ интеллектуалдық жүйесі күрделі жүйе ретінде. Құрылымдық модельдеу: IDEF0, UML/SysML, декомпозиция. Шабуылдар графтары мен ағаштары, қауіптердің таралу модельдері. Марков модельдері және қорғау жүйелерінің сенімділік модельдері. «Шабуылдаушы — қорғаушы» ойындар теориясы модельдері. АҚ процестерін имитациялық модельдеу: дискретті-оқиғалық және агенттік тәсілдер. Көпкритерийлі талдау және шешім қабылдау әдістері (ИТӘ, TOPSIS). Шектеулі ресурстар кезінде қорғау жүйелерін оңтайландыру. Тиімділікті және киберорнықтылықты бағалау.
Пәннің құзіреттілігі	- - біледі: жүйелік талдау, құрылымдық, ықтималдық және имитациялық модельдеу әдістерін; - - түсінеді: күрделі ақпараттық және әлеуметтік-техникалық жүйелердің қасиеттерін және олардың тиімділігі мен сенімділігінің критерийлерін; - - қолдана алады: АҚ процестерін зерттеу үшін шабуылдар графтарын, Марков, ойындар теориясы және имитациялық модельдерін; - - құзыретті: белгісіздік жағдайында жүйелердің

	қауіпсіздігін арттыру шешімдерін негіздеуде және оңтайландыруда.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 138.1. Андрейчиков, А.В., Андрейчикова, О.Н., 2024. — 530 с. 139.2. Емелина Н.К. Методы принятия оптимальных решений: учебно-практическое пособие / Н.К. Емелина.– Алматы: Эверо, 2020.- 216 с. https://baraev.elib.kz/ru/search/read_book/1170/ 140.3. Боуш, Г.Д. Методология научного исследования (в кандидатских и докторских диссертациях) [Текст]: учебник / Г.Д. Боуш, В.И. Разумов.- М.: ИНФРА-М, 2025.- 227 с.- (Высшее образование). 141.4. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ 142.5. Федотова, Е.Л. Информационные технологии в науке и образовании [Текст]: учеб. пособие / Е.Л. Федотова, А.А. Федотов.- Москва: "ФОРУМ"; ИНФРА-М, 2024.- 335 с.- (Высшее образование). **Қосымша:** 143.6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 144.7. Черикбаева, Л.Ш. Деректерді талдаудың топтық шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 145.8. Методы и модели исследования сложных систем и обработки больших данных : монография. / И.Ю. Парамонов, В.А. Смагин, Н.Е. Косых, А.Д. Хомоненко; под ред. В.А. Смагина, А.Д. Хомоненко. - Санкт-Петербург: Лань, 2020. - 236 с. - ISBN 978-5-8114-4006-1. https://rmebrk.kz/book/1179911 146.9. Mitchell, M. Complexity: A Guided Tour. — Oxford University Press / Springer access, 2009. https://link.springer.com/book/10.1007/978-3-030-27672-0

Пәннің коды мен атауы	**IIAU 6319 Қауіптерді талдаудағы жасанды интеллект**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	6
Оқыту формасы	Күндізгі
Семестр	3

Пәннің пререквизиттері	Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Киберқауіпсіздіктегі зерттеу әдістері
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Киберқауіптерді анықтау, жіктеу және болжау, олардың нәтижелерін интерпретациялау және АҚ мониторинг орталығының процестеріне біріктіру үшін жасанды интеллект негізіндегі шешімдерді әзірлеу және енгізу дағдыларын қалыптастыру.
Пән мазмұны	Қауіптерді талдаудың өмірлік циклі және ЖИ рөлі, MITRE ATT&CK матрицасы. Қауіптер туралы деректерді жинау және дайындау, белгілерді жасау. Машиналық және терең оқыту әдістерімен желілік шабуылдарды анықтау. Статикалық және динамикалық талдау деректері бойынша зиянды БҚ-ны жіктеу және кластерлеу. NLP әдістерімен фишингті анықтау. Мінез-құлықтық аналитика және аномалияларды анықтау (UEBA, автокодтауыштар). Қауіптерді болжау және уақыттық қатарларды талдау. Threat Intelligence және Threat Hunting-тегі ЖИ, SIEM/SOAR-мен біріктіру. АҚ-да ЖИ қолданудың этикалық және құқықтық аспектілері.
Пәннің құзіреттілігі	- - біледі: киберқауіптерді талдау, жіктеу және болжау үшін қолданылатын жасанды интеллект әдістерін; - - түсінеді: қауіптерді талдаудың өмірлік циклін және мониторинг пен әрекет ету процестеріндегі ЖИ шешімдерінің орнын; - - қолдана алады: нақты қауіп деректеріне машиналық және терең оқыту, NLP және уақыттық қатарларды талдау әдістерін; - - құзыретті: этикалық талаптарды ескере отырып, ЖИ модельдерінің нәтижелерін интерпретациялауда және оларды SOC процестеріне біріктіруде.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 147.1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 148.2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 149.3. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 150.4. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 151.5. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с.

	https://baraev.elib.kz/ru/search/read_book/3586/ **Қосымша:** 152.6. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с. 153.7. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – P. 70–83. https://rmebrk.kz/magazine/6475# 154.8. Amanzholova, S., Mutanov, G., Mukhanov, S., Ussatova, O., & Razaque, A. AI-powered system for network activity monitoring and detection of SQL injection attacks using Zabbix and Grafana // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – Is. 3. – P. 61–83. https://rmebrk.kz/magazine/6475#

Пәннің коды мен атауы	**GIIK 6320 Киберқауіпсіздіктегі генеративті жасанды интеллект**
Пәннің ПОҚ	IT-технологиялар кафедрасының ПОҚ: _____
Пән циклі	БеП/ТК
Оқу деңгейі	Магистратура (ғылыми-педагогикалық бағыт)
Білім беру бағдарламасы	7М06301 – Ақпараттық қауіпсіздіктің интеллектуалды жүйелері
Академиялық кредит	6
Оқыту формасы	Күндізгі
Семестр	3
Пәннің пререквизиттері	Операциялық жүйелердің қауіпсіздігін талдау / Ақпараттық жүйелердің киберқауіпсіздігі, Желілік қауіпсіздікті талдау / Қауіпсіздіктің аналитикалық ақпараттық жүйелері, Киберқауіпсіздіктегі зерттеу әдістері
Пәннің постреквизиттері	Зерттеу практикасы, Магистранттың ғылыми-зерттеу жұмысы, Магистрлік диссертацияны рәсімдеу және қорғау
Пәнді оқу мақсаты	Киберқауіпсіздік міндеттері үшін генеративті ЖИ негізіндегі инновациялық шешімдерді жобалау, зерттеу және енгізу, сондай-ақ этикалық және құқықтық талаптарды ескере отырып, генеративті модельдермен байланысты қауіптерді анықтау және бейтараптандыру қабілетін қалыптастыру.
Пән мазмұны	Генеративті модельдер: трансформерлер, GAN, VAE, диффузиялық модельдер. АҚ мониторинг орталығындағы LLM: журналдарды талдау, инциденттерді қорытындылау, талдаушы көмекшілері. Кодты талдау мен қауіпсіз әзірлеудегі генеративті ЖИ. Анықтау жүйелерін оқыту үшін синтетикалық деректерді генерациялау. LLM қауіпсіздігіне қатерлер: промпт-инъекциялар, деректердің ағуы, улау; OWASP Top 10 for LLM Applications. Дипфейктер және ЖИ көмегімен әлеуметтік инженерия, анықтау әдістері. Генеративті модельдерді қорғау: red teaming, қорғаныс механизмдері, RAG архитектуралары. ЖИ-ді реттеу және этикасы: NIST AI RMF, ISO/IEC 42001. Зерттеу шағын

	жобасы.
Пәннің құзіреттілігі	- - біледі: генеративті модельдердің архитектураларын және олардың киберқауіпсіздікте қолданылу салаларын; - - түсінеді: генеративті ЖИ-мен байланысты қауіптерді және ЖИ-ді жауапкершілікпен пайдалану қағидаттарын; - - қолдана алады: журналдарды, кодты талдау және синтетикалық деректерді генерациялау үшін генеративті модельдерді, сондай-ақ LLM жүйелерін қорғау шараларын; - - құзыретті: тиімділігін бағалай және этикалық талаптарды сақтай отырып, генеративті ЖИ негізіндегі инновациялық шешімдерді жобалауда және зерттеуде.
Қорытынды бақылау нысаны	Емтихан
Пәннің оқытылу мерзімі	1 академиялық кезең (20 апта)
Әдебиеттер тізімі	**Негізгі:** 155.1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 156.2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 157.3. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 158.4. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с. https://baraev.elib.kz/ru/search/read_book/3586/ 159.5. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ **Қосымша:** 160.6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 161.7. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с. 162.8. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – P. 70–83. https://rmebrk.kz/magazine/6475# 163.9. Amanzholova, S., Mutanov, G., Mukhanov, S., Ussatova, O., & Razaque, A. AI-powered system for network activity monitoring and detection of SQL injection attacks using Zabbix

	and Grafana // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – Is. 3. – P. 61–83. https://rmebrk.kz/magazine/6475#

НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ АГРАРНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
Факультет «Водные ресурсы и IT-технологии»

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН

7М06301 – «Интеллектуальные системы информационной безопасности»

на 2026-2028 учебный год

АЛМАТЫ, 2026

Каталог элективных дисциплин одобрен решением учебно-методического совета КазНАИУ (протокол №___ от «___»_____2026 г.) и Ученым Советом КазНАИУ (протокол №___ от «___»_____2026 г.).

Составители: Медетбаева С.А.

Предисловие

Каталог элективных дисциплин (КЭД) сформирован отделом учебно-методической работы Казахского национального аграрного исследовательского университета в соответствии с утвержденным Государственный общеобязательный стандарт высшего образования. Приказ Министра науки и высшего образования Республики Казахстан от 20 июля 2022 года № 2

КЭД обеспечивает обучающимся возможность в выборе элективных учебных дисциплин и ППС для формирования индивидуальной образовательной траектории. На основании Образовательной программы и КЭД обучающимися с помощью эдвайзеров разрабатываются ИУПы

В таблице каталога приводятся дисциплины вузовского компонента и компонента по выбору циклов базовых дисциплин (БД) и профилирующих дисциплин (ПД) магистратуры, практики, научно-исследовательская работа магистранта и итоговая аттестация, а также формуляры дисциплин. В формуляре КЭД указаны названия дисциплин с кратким описанием курса, пререквизиты, постреквизиты, Ф.И.О. ППС, количество кредитов и семестр изучения.

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА: 7М06301 – «ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Присуждаемая степень: магистр технических наук по образовательной программе 7М06301 – «Интеллектуальные системы информационной безопасности»

1 КУРС

Цикл	Код	Дисциплины	Академ. кредиты
1 семестр – 30 академических кредитов			
Вузовский компонент – 13 кр.			
БД	IFN 5204	История и философия науки	5
БД	IYaP 5202	Иностранный язык (профессиональный)	3
БД	PVSH 5203	Педагогика высшей школы	5
Компонент по выбору – 15 кр.			
БД	ABOS 5207	Анализ безопасности операционных систем	5
	KIS 5206	Кибербезопасность информационных систем	
БД	ASB 5209	Анализ сетевой безопасности	5
	AISB 5208	Аналитические информационные системы безопасности	
БД	KMSZI 5211	Криптографические методы и средства защиты информации	5
	PPKP 5210	Принципы построения криптографических протоколов	
Научно-исследовательская работа магистранта – 2 кр.			
НИРМ	NIRM 5501	Научно-исследовательская работа магистранта	2
2 семестр – 30 академических кредитов			
Вузовский компонент – 28 кр.			
БД	PU 5205	Психология управления	3
БД	PP 5201	Педагогическая практика	4
ПД	MIK 5313	Методы исследований в кибербезопасности	6
ПД	UPK 5314	Управление проектами кибербезопасности	5
ПД	AIB 5312	Аудит информационной безопасности	5
ПД	IP 5309	Исследовательская практика	5
Научно-исследовательская работа магистранта – 2 кр.			
НИРМ	NIRM 5502	Научно-исследовательская работа магистранта	2

Формуляр для описания дисциплины

Код и название дисциплины	**IFN 5204 История и философия науки**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Философия (бакалавриат деңгейінде)
Постреквизиты дисциплины	Методы исследований в кибербезопасности, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование у магистрантов целостного представления о науке как социокультурном феномене, об исторической динамике научного знания и методологических основах научного исследования, необходимых для планирования и проведения исследований в области информационной безопасности.
Содержание дисциплины	Предмет философии науки. Наука как система знания, деятельность и социальный институт. Генезис науки: античность, средневековье, Новое время. Классическая, неклассическая и постнеклассическая наука. Концепции развития науки (К. Поппер, Т. Кун, И. Лакатос, П. Фейерабенд). Структура научного знания: эмпирический и теоретический уровни. Методы научного познания. Научная картина мира. Философские проблемы техники, информатики и кибернетики. Информационное общество и цифровая этика. Этика науки и академическая честность. Развитие науки в Казахстане.
Компетенции дисциплины	-знать основные этапы исторического развития науки, концепции её развития и структуру научного знания; -понимать философские и методологические основания научного исследования и роль науки в развитии информационного общества; -применять методы научного познания при постановке и обосновании исследовательских задач в области информационной безопасности; -быть компетентным в аргументированной оценке научных результатов с соблюдением принципов научной этики и академической честности.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Степин В.С. История и философия науки: учебник для аспирантов и соискателей. – М.: Академический проект, 2011. – 423 с. 2. Лебедев С.А. Философия науки: учебное пособие для магистров. – М.: Юрайт, 2014. – 288 с.

	3. Кохановский В.П., Лешкевич Т.Г., Матяш Т.П., Фатхи Т.Б. Основы философии науки. – Ростов н/Д: Феникс, 2010. – 603 с. 4. Кун Т. Структура научных революций. – М.: АСТ, 2020. – 320 с. **Дополнительная** 5. Поппер К. Логика научного исследования. – М.: Республика, 2004. – 447 с. 6. Лакатос И. Фальсификация и методология научно-исследовательских программ. – М.: Медиум, 1995. – 236 с. 7. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Код и название дисциплины	**IYaP 5202 Иностранный язык (профессиональный)**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	3
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Иностранный язык (бакалавриат деңгейінде)
Постреквизиты дисциплины	Методы исследований в кибербезопасности, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Развитие иноязычной профессиональной и научной коммуникативной компетенции, позволяющей магистранту читать и анализировать зарубежные источники по информационной безопасности, готовить академические тексты и презентации и участвовать в международных научных дискуссиях.
Содержание дисциплины	Профессиональная лексика и терминология в области информационной безопасности и ИИ. Чтение и реферирование научных статей. Структура научной статьи (IMRaD). Академическое письмо: аннотация, введение, обзор литературы, обсуждение результатов. Цитирование и оформление ссылок (APA, IEEE). Подготовка и проведение научной презентации. Участие в дискуссии, конференции, вебинаре. Деловая переписка и CV исследователя. Перевод профессионально ориентированных текстов.
Компетенции дисциплины	-знать профессиональную терминологию и жанровые особенности научного дискурса на иностранном языке; -понимать содержание зарубежных научных публикаций и технической документации по информационной безопасности; -применять иностранный язык для подготовки аннотаций, научных статей и презентаций результатов исследования; -быть компетентным в устной и письменной профессиональной коммуникации в международной научной среде.

Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Swales J.M., Feak C.B. Academic Writing for Graduate Students: Essential Tasks and Skills. – 3rd ed. – Ann Arbor: University of Michigan Press, 2012. – 418 p. 2. Wallwork A. English for Writing Research Papers. – 2nd ed. – Cham: Springer, 2016. – 368 p. 3. Wallwork A. English for Presentations at International Conferences. – 2nd ed. – Cham: Springer, 2016. – 222 p. 4. Murphy R. English Grammar in Use. – 5th ed. – Cambridge: Cambridge University Press, 2019. – 394 p. **Дополнительная** 5. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Harlow: Pearson, 2020. – 832 p. 6. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Код и название дисциплины	**PVSH 5203 Педагогика высшей школы**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Психология, основы педагогики (бакалавриат деңгейінде)
Постреквизиты дисциплины	Психология управления, Педагогическая практика
Цель изучения дисциплины	Формирование психолого-педагогической компетентности будущего преподавателя вуза, способного проектировать образовательный процесс, применять и оценивать современные педагогические технологии и обеспечивать эффективную педагогическую коммуникацию.
Содержание дисциплины	Педагогика высшей школы как наука. Болонский процесс и развитие высшего образования в Республике Казахстан. Нормативная база высшего образования (ГОСО, академическая политика). Дидактика высшей школы: принципы, формы и методы обучения. Кредитная технология и студентоцентрированное обучение. Проектирование результатов обучения и силлабуса. Активные и интерактивные методы, смешанное и дистанционное обучение. Оценивание результатов обучения. Воспитательная работа и кураторство. Педагогическое общение и профессиональная этика преподавателя.
Компетенции дисциплины	-знать закономерности, принципы и нормативные основы организации образовательного процесса в высшей школе; -понимать сущность кредитной технологии и студентоцентрированного подхода к обучению;

	-применять современные педагогические технологии, методы активного обучения и оценивания результатов обучения; -быть компетентным в проектировании учебных занятий и силлабусов, в педагогической коммуникации и соблюдении профессиональной этики.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Громкова М.Т. Педагогика высшей школы: учебное пособие. – М.: ЮНИТИ-ДАНА, 2012. – 447 с. 2. Пидкасистый П.И. Педагогика: учебник для бакалавров. – М.: Юрайт, 2014. – 511 с. 3. Мынбаева А.К., Садвакасова З.М. Инновационные методы обучения, или Как интересно преподавать: учебное пособие. – Алматы, 2010. – 344 с. 4. Biggs J., Tang C. Teaching for Quality Learning at University. – 4th ed. – Maidenhead: Open University Press, 2011. – 389 p. **Дополнительная** 5. Государственный общеобязательный стандарт высшего и послевузовского образования. Приказ Министра науки и высшего образования РК от 20 июля 2022 года № 2. 6. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Код и название дисциплины	**ABOS 5207 Анализ безопасности операционных систем**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Операционные системы, Основы информационной безопасности, Компьютерные сети (бакалавриат деңгейінде)
Постреквизиты дисциплины	Аудит информационной безопасности, Управление проектами кибербезопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур, Технологии управления информационной безопасностью, Генеративный искусственный интеллект в кибербезопасности
Цель изучения дисциплины	Формирование углублённых знаний об архитектуре современных операционных систем и встроенных механизмах безопасности, умений проводить комплексный анализ защищённости ОС, выявлять и классифицировать уязвимости и обосновывать меры по укреплению систем.
Содержание дисциплины	Архитектура современных ОС и модель угроз. Модели

	разграничения доступа DAC, MAC, RBAC и их реализация в Windows и Linux (ACL, SELinux, AppArmor). Идентификация, аутентификация, управление учётными записями и привилегиями. Изоляция процессов и памяти, виртуализация и контейнеризация. Классификация уязвимостей ОС (CVE, CWE, CVSS), уязвимости ядра и повышение привилегий. Аудит и журналирование событий безопасности (Windows Event Log, auditd, syslog). Укрепление защищённости ОС: CIS Benchmarks, STIG. Обнаружение вредоносного ПО и руткитов, основы криминалистического анализа ОС. Безопасность мобильных и встраиваемых ОС.
Компетенции дисциплины	-знать архитектуру современных ОС, модели разграничения доступа и встроенные механизмы безопасности; -понимать природу уязвимостей ОС и методику оценки их критичности на основе CVE, CWE и CVSS; -применять средства аудита конфигураций и анализа журналов событий для выявления попыток несанкционированного доступа; -быть компетентным в проектировании и обосновании комплекса мер по укреплению защищённости ОС в соответствии с отраслевыми стандартами.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 2. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов. . - М: Юрайт, 2022. - 104 с. - (Высшее образование). - ISBN 978-5-534-14590-8. http://rmebrk.kz/book/1179658 3. Мартынов, А.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / А.П. Мартынов, И.А. Мартынова, А.А. Русаков.- 2-е изд.- М: Ай Пи Ар Медиа, 2024.- 130 с. 4. Прохорова, О.В. Информационная безопасность и защита информации. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. http://rmebrk.kz/book/1183813 5. Усенова, А.Ж. Операциялық жүйелер, орталар және қабықшалар [Мәтін]: оқу-әдістемелік құралы / А.Ж. Усенова.- Алматы: Эверо, 2020.- 348 б. **Дополнительная** 6. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 7. Ешпанов, А. Разработка концепции информационной безопасности: мировой опыт и Казахстан. // Саясат Policy.

	— 2019. — №9. — С. 33–36. 8. IEEE Computer Society. Operating System Security Models and Access Control. — IEEE Xplore Digital Library, 2022–2024. https://ieeexplore.ieee.org/ 9. Stallings W. Operating Systems: Internals and Design Principles. — 9th ed. — Harlow : Pearson Education Limited, 2018. — 1128 p. — ISBN 978-1292214290 https://api.pageplace.de/preview/DT0400.9781292214306_A37747502/preview-9781292214306_A37747502.pdf?utm_source=chatgpt.com

Код и название дисциплины	**KIS 5206 Кибербезопасность информационных систем**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Основы информационной безопасности, Базы данных, Архитектура информационных систем (бакалавриат деңгейінде)
Постреквизиты дисциплины	Аудит информационной безопасности, Управление проектами кибербезопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур, Технологии управления информационной безопасностью, Генеративный искусственный интеллект в кибербезопасности
Цель изучения дисциплины	Формирование системного подхода к обеспечению кибербезопасности информационных систем на всех этапах жизненного цикла, способности оценивать уровень защищённости ИС, моделировать актуальные угрозы и проектировать комплексные решения по защите.
Содержание дисциплины	ИС как объект защиты, принцип Security by Design. Моделирование угроз и нарушителя: STRIDE, PASTA, MITRE ATT&CK. Безопасность веб-приложений: OWASP Top 10. Безопасность баз данных, защита от инъекций, шифрование данных. Управление идентификацией и доступом (IAM), многофакторная аутентификация, архитектура Zero Trust. Безопасная разработка ПО: SAST, DAST, DevSecOps. Методология тестирования на проникновение. Мониторинг и реагирование на инциденты: SIEM, SOC. Непрерывность и восстановление ИС: резервное копирование, DRP.
Компетенции дисциплины	-знать модели угроз и нарушителя, требования и механизмы защиты приложений, баз данных и сервисов; -понимать принципы Security by Design, Zero Trust и безопасной разработки программного обеспечения; -применять методы моделирования угроз, выявления уязвимостей и тестирования на проникновение для

	оценки защищённости ИС; -быть компетентным в проектировании архитектуры защиты ИС и организации мониторинга и реагирования на инциденты.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 2. Бабаш, А.В. и др. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. – М.: РИОР: ИНФРА-М, 2020. - 236с. - (Высшее образование). -ISBN 978-5-369-01788-3 . https://rmebrk.kz/book/1176322 3. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems and computing. Volume 657). 4. Бирюков, А.А. Информационная безопасность: защита и нападение. — М.: ДМК Пресс, 2023. — 440 с. https://rmebrk.kz/book/1183819 5. Медеуова, А.Б. WEB-программирование [Текст]: учеб. пособие / А.Б. Медеуова, В.Н. Казагачев, Ж. Жумагулова.- Алматы: Эверо, 2025.- 232 с. **Дополнительная** 6. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 7. Ешпанов, А. Разработка концепции информационной безопасности: мировой опыт и Казахстан. // Саясат Policy. — 2019. — №9. — С. 33–36. 8. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2024 (18)2. – P. 70–83. https://rmebrk.kz/magazine/6475# 9. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2022. — 30 p. https://www.iso.org/standard/27001

Код и название дисциплины	**ASB 5209 Анализ сетевой безопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ

Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Компьютерные сети, Сетевые протоколы и технологии, Основы информационной безопасности (бакалавриат деңгейінде)
Постреквизиты дисциплины	Методы исследований в кибербезопасности, Аудит информационной безопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур, Интеллектуальные модели и методы в информационной безопасности, Системный анализ и моделирование в интеллектуальных системах информационной безопасности, Искусственный интеллект в анализе угроз, Генеративный искусственный интеллект в кибербезопасности
Цель изучения дисциплины	Формирование навыков анализа защищённости сетевой инфраструктуры, выявления сетевых атак по трафику, настройки и оценки средств сетевой защиты и проектирования защищённой сетевой архитектуры.
Содержание дисциплины	Модель угроз сетевой инфраструктуры и классификация сетевых атак. Уязвимости протоколов ARP, IP, TCP, UDP, DNS. Захват и анализ сетевого трафика (Wireshark). Сетевая разведка, сканирование и оценка защищённости (Nmap). Межсетевые экраны и NGFW, проектирование политик фильтрации. Системы обнаружения и предотвращения вторжений (Suricata, Snort). Сегментация сети, VLAN, микросегментация, VPN и IPsec. Безопасность беспроводных сетей (WPA3) и сетей IoT. Защита от DDoS-атак, мониторинг сети (NetFlow, SIEM).
Компетенции дисциплины	-знать уязвимости сетевых протоколов, классификацию сетевых атак и технологии сетевой защиты; -понимать принципы работы межсетевых экранов, IDS/IPS, VPN и сегментации сети; -применять средства анализа трафика и сканирования для выявления атак и оценки защищённости сети; -быть компетентным в проектировании защищённой сетевой архитектуры и управлении сетевыми потоками.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Якубов, Б.М., Мекебаева, А.К. Телекоммуникациялық жүйелердегі ақпараттар қауіпсіздігі: оқу құралы. — Алматы: Альманах, 2018. — 75 б. 2. Басыня, Е.А. Сетевая информационная безопасность: учебник. — М.: НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. https://rmebrk.kz/book/1184075 3. Даушеева, Н.Н. Стандарты сетевых технологий [Текст]:

	учеб. пособие / Н.Н. Даушеева.- Алматы: Эпиграф, 2023.- 160 с. 4. Воробъев С.П., Широбокова С.Н., Литвяк Р.К. Компьютерные сети и сетевая безопасность: учебное пособие /Южно-Российский государственный политехнический университет (НПИ) им. М.И.Платова + Новочеркасск: ЮРГПУ (НПИ), 2022. -216с. https://kaznaru.elib.kz/ru/search/read_book/11390/ 5. Усенова, А.Ж. Желілік технологиялар [Мәтін]: пәні бойынша дәрістер жинағы / А.Ж. Усенова, Ж.Д. Изтаев.- Алматы: Эпиграф, 2023.- 172 б. **Дополнительная** 6. Усенова, А.Ж. Желілік технологиялар [Мәтін]: пәні бойынша дәрістер жинағы / А.Ж. Усенова, Ж.Д. Изтаев.- Алматы: Эпиграф, 2023.- 172 б. 7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета. // Вестник КазГУ. - 2016. - №4. - С. 80–88. 8. IEEE Computer Society. Intrusion Detection Systems and Network Security: Research Articles. — IEEE Xplore Digital Library, 2022–2024. https://ieeexplore.ieee.org/ 9. Kikissagbe, B. R., & Adda, M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Electronics, 2024, 13(18), 3601. https://doi.org/10.3390/electronics13183601

Код и название дисциплины	**AISB 5208 Аналитические информационные системы безопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Базы данных, Основы информационной безопасности, Теория вероятностей и математическая статистика (бакалавриат деңгейінде)
Постреквизиты дисциплины	Методы исследований в кибербезопасности, Аудит информационной безопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур, Интеллектуальные модели и методы в информационной безопасности, Системный анализ и моделирование в интеллектуальных системах информационной безопасности, Искусственный интеллект в анализе угроз, Генеративный искусственный интеллект в кибербезопасности
Цель изучения дисциплины	Формирование навыков построения и применения аналитических систем сбора, корреляции и

	интеллектуальной обработки данных о событиях безопасности для обнаружения аномалий и поддержки принятия решений.
Содержание дисциплины	Аналитика данных в ИБ: источники данных, задачи, архитектура аналитических систем. Сбор, нормализация и хранение журналов событий (Syslog, CEF, JSON). SIEM-системы: архитектура, правила корреляции, сценарии обнаружения. UEBA — поведенческая аналитика. Threat Intelligence: индикаторы компрометации, STIX/TAXII, MISP. SOAR: автоматизация реагирования и плейбуки. Статистические методы и Data Mining для обнаружения аномалий. Визуализация данных безопасности, метрики и KPI SOC. Проектирование аналитической системы безопасности (ELK/OpenSearch, Wazuh).
Компетенции дисциплины	-знать архитектуру и функции SIEM, SOAR, UEBA и платформ Threat Intelligence; -понимать методы нормализации и корреляции событий, статистические основы обнаружения аномалий; -применять аналитические платформы для разработки правил корреляции и сценариев обнаружения угроз; -быть компетентным в анализе и интерпретации данных безопасности и проектировании аналитической системы организации.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems and computing. Volume 657). 2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 3. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 4. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с. https://baraev.elib.kz/ru/search/read_book/3586/ 5. Мартынов, А.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / А.П. Мартынов, И.А. Мартынова, А.А. Русаков.- 2-е изд.- Москва: Ай Пи Ар Медиа, 2024.- 130 с. **Дополнительная** 6. Казагачев, В.Н. Вычислительные системы и сети

	[Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета. // Вестник КазГУ. - 2016. - №4. - С. 80–88. 8. Кайбасова Д.Ж. Автоматтандырылған ақпараттық жүйелерді жобалауда деректер қорын қолдану тәсілдері: Монография /Д.Ж. Кайбасова, Б.О. Мухаметжанова, Э.К. Сейпишева; Қарағанды мемлекеттік техникалық университеті. – Алматы: Эверо, 2020. - 186 б. https://baraev.elib.kz/ru/search/read_book/3992/ 9. Patel, S. J., Raj, P., Visconti, A. (Eds.) Security, Privacy and Data Analytics. — Singapore: Springer Nature, 2022. — 400+ p. Available at: https://link.springer.com/book/10.1007/978-981-16-9089-1

Код и название дисциплины	**KMSZI 5211 Криптографические методы и средства защиты информации**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Дискретная математика, Основы криптографии, Основы информационной безопасности (бакалавриат деңгейінде)
Постреквизиты дисциплины	Аудит информационной безопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур
Цель изучения дисциплины	Формирование углублённых знаний о математических основах и современных методах криптографической защиты, умений обоснованно выбирать, анализировать и применять криптографические алгоритмы для обеспечения конфиденциальности, целостности и подлинности информации.
Содержание дисциплины	Математические основы криптографии: теория чисел, конечные поля, вычислительная сложность. Симметричные блочные и поточные шифры, режимы шифрования. Хеш-функции и коды аутентификации сообщений (SHA-2/3, HMAC). Асимметричные криптосистемы: RSA, Диффи–Хеллман, эллиптические кривые. Электронная цифровая подпись и инфраструктура открытых ключей (PKI), НУЦ РК. Управление ключами и HSM. Программно-аппаратные средства криптографической защиты, требования и сертификация. Криптоанализ и атаки по побочным каналам. Постквантовая криптография (ML-KEM, ML-DSA).
Компетенции дисциплины	-знать математические основы криптографии, классы

	криптосистем и стандарты криптографической защиты; -понимать свойства стойкости алгоритмов и принципы построения PKI и систем управления ключами; -применять симметричные и асимметричные алгоритмы, хеш-функции и ЭЦП для обеспечения конфиденциальности, целостности и подлинности; -быть компетентным в сравнительном анализе и обоснованном выборе средств криптографической защиты, включая постквантовые решения.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости [Текст]: учеб. пособие / А.В. Черемушкин.- М.: Академия, 2009.- 272с. 2. Кожомбердиева, Г.И., Глухарев, М.Л. Криптографическая защита информации и управление доступом на платформе Java. — СПб., 2016. — 87 с. https://rmebrk.kz/book/1189323 3. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems – Криптографические системы : Textbook. . - Almaty: Bastau, 2021. - 320- ISBN 978-601-7660-08-6. https://rmebrk.kz/book/1176885 4. Абдикаликов, К.А. Анализ каналов уязвимости криптографической системы RSA. — 2012. https://rmebrk.kz/book/54167 5. Айтхожаева, Е.Ж., Тынымбаев, С. Аспекты аппаратного приведения по модулю в асимметричной криптографии. — 2014. https://rmebrk.kz/book/1026852 **Дополнительная** 6. Фомичев, В.М. Криптография - наука о тайнописи [Текст]: учеб. пособие / В.М. Фомичев; Фин. ун-т при Правительстве РФ.- М.: Прометей, 2020.- 66 с. 7. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б. 8. Тынымбаев, С.Т., Айтхожаева, Е.Ж. Аппаратное ускорение приведения по модулю для асимметричной криптографии. — 2016. — С.158–160. https://rmebrk.kz/book/1151931 9. Renner, R., & Wolf, R. (2022). Quantum advantage in cryptography. arXiv. https://arxiv.org/abs/2206.04078

Код и название дисциплины	**PPKP 5210 Принципы построения криптографических протоколов**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)

Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	1
Пререквизиты дисциплины	Дискретная математика, Основы криптографии, Компьютерные сети (бакалавриат деңгейінде)
Постреквизиты дисциплины	Аудит информационной безопасности, Интеллектуальные технологии анализа и защиты информации, Безопасность больших данных и облачных инфраструктур
Цель изучения дисциплины	Формирование способности проектировать криптографические протоколы с заданными свойствами безопасности, выявлять в них уязвимости и верифицировать их свойства с помощью формальных методов.
Содержание дисциплины	Криптографические примитивы как основа протоколов, модели безопасности. Модель нарушителя Долева–Яо, атаки на протоколы (повтор, отражение, «человек посередине»). Протоколы аутентификации: парольные, «запрос–ответ», Kerberos, FIDO2. Протоколы распределения и согласования ключей. Протоколы защищённых каналов: TLS 1.3, IPsec, SSH. Формальный анализ: BAN-логика, ProVerif, Tamarin. Протоколы с нулевым разглашением и безопасные многосторонние вычисления. Протоколы электронной подписи, блокчейн и смарт-контракты. Постквантовая миграция протоколов.
Компетенции дисциплины	-знать классы криптографических протоколов, модели нарушителя и типовые атаки на протоколы; -понимать принципы построения протоколов аутентификации, распределения ключей и защищённых каналов; -применять формальные методы и средства верификации для анализа свойств безопасности протоколов; -быть компетентным в проектировании протоколов и обосновании выбора и конфигурации протоколов защищённого обмена для реальных ИС.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости [Текст]: учеб. пособие / А.В. Черемушкин.- М.: Академия, 2009.- 272с.- (Высшее профессиональное образование). 2. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 3. Сидельников, В.М. Криптография и теория кодирования. - М.: МГУ, 2006. - 22 с. https://rmebrk.kz/book/1010922 4. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems –

	Криптографические системы : Textbook. . - Almaty: Bastau, 2021. - 320- ISBN 978-601-7660-08-6. https://rmebrk.kz/book/1176885 **Дополнительная** 5. Фомичев, В.М. Криптография - наука о тайнописи [Текст]: учеб. пособие / В.М. Фомичев; Фин. ун-т при Правительстве РФ.- М.: Прометей, 2020.- 66 с. 6. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б. 7. Тынымбаев, С.Т., Айтхожаева, Е.Ж. Аппаратное ускорение приведения по модулю для асимметричной криптографии. — 2016. — С.158–160. https://rmebrk.kz/book/1151931 8. IEEE Computer Society. Cryptographic Systems and Security. — IEEE Xplore Digital Library, 2022–2024. https://ieeexplore.ieee.org/

Код и название дисциплины	**PU 5205 Психология управления**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	БД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	3
Форма обучения	очная
Семестр	2
Пререквизиты дисциплины	Педагогика высшей школы
Постреквизиты дисциплины	Технологии управления информационной безопасностью, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование у магистрантов знаний о психологических закономерностях управленческой деятельности и умений применять их для анализа ситуаций, принятия обоснованных решений, руководства командами и проектами в профессиональной среде.
Содержание дисциплины	Предмет и задачи психологии управления. Личность руководителя и стили руководства. Теории лидерства. Психология мотивации персонала. Психология малых групп и формирование команды. Психология принятия управленческих решений в условиях неопределённости и риска. Коммуникации в управлении, деловые переговоры. Конфликты в организации и методы их разрешения. Стресс-менеджмент и профилактика профессионального выгорания. Организационная культура и управление изменениями. Человеческий фактор в обеспечении информационной безопасности.
Компетенции дисциплины	-знать психологические закономерности управленческой деятельности, теории лидерства и мотивации;

	-понимать роль человеческого фактора, организационной культуры и коммуникаций в управлении и обеспечении информационной безопасности; -применять методы психологического анализа ситуаций, управления конфликтами и формирования команды; -быть компетентным в принятии обоснованных управленческих решений и руководстве коллективом в профессиональной среде.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Кабаченко Т.С. Психология управления: учебник. – 4-е изд. – М.: Юрайт, 2019. – 409 с. 2. Урбанович А.А. Психология управления: учебное пособие. – Минск: Харвест, 2003. – 640 с. 3. Robbins S.P., Judge T.A. Organizational Behavior. – 18th ed. – Harlow: Pearson, 2019. – 744 p. **Дополнительная** 4. Hadnagy C. Social Engineering: The Science of Human Hacking. – 2nd ed. – Indianapolis: Wiley, 2018. – 320 p. 5. Интернет-ресурс: http://library.kaznau.kz/new/?lang=ru

Код и название дисциплины	**MIK 5313 Методы исследований в кибербезопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	6
Форма обучения	очная
Семестр	2
Пререквизиты дисциплины	История и философия науки, Иностранный язык (профессиональный), Анализ сетевой безопасности / Аналитические информационные системы безопасности
Постреквизиты дисциплины	Исследовательская практика, Интеллектуальные технологии анализа и защиты информации, Научно-исследовательская работа магистранта
Цель изучения дисциплины	Формирование у магистрантов методологической культуры научного исследования в области кибербезопасности: умений планировать и проводить эксперимент, обрабатывать и интерпретировать данные, оценивать достоверность результатов и представлять их в виде научной публикации.
Содержание дисциплины	Методология научного исследования в кибербезопасности. Постановка проблемы, цели, гипотезы и задачи исследования. Поиск и анализ научной информации: Scopus, Web of Science, IEEE Xplore; систематический обзор литературы (PRISMA). Количественные, качественные и смешанные методы. Планирование эксперимента, испытательные стенды и киберполигоны. Наборы данных для исследований в ИБ и

	их ограничения. Статистическая обработка результатов, проверка гипотез, воспроизводимость. Моделирование угроз и оценка рисков как исследовательские методы. Этика исследований в ИБ, ответственное раскрытие уязвимостей. Подготовка научной статьи и магистерской диссертации.
Компетенции дисциплины	-знать методологию, методы и этапы научного исследования в области кибербезопасности; -понимать принципы планирования эксперимента, требования к данным и критерии достоверности результатов; -применять методы поиска и анализа научной информации, статистической обработки и интерпретации экспериментальных данных; -быть компетентным в подготовке и представлении результатов исследования в виде научной публикации с соблюдением этических требований.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Боуш, Г.Д., Разумов, В.И. Методология научного исследования (в кандидатских и докторских диссертациях): учебник. — М.: ИНФРА-М, 2025. — 227 с. 2. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ 3. Wilimowska, Z. Information systems architecture and technology: proceedings of 38th international conference on information systems architrcture and trchnology - ISAT 2017 [Текст]: part 3 / Z. Wilimowska, L. Borzemski, J. Swiatek.- Poland: Springer, 2018.- 390 p.- (Advances in intelligent systems and computing. Volume 657). 4. Creswell, J. W., Creswell, J. D. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. — 5th ed. — Thousand Oaks: SAGE Publications, 2018. — 304 p. — ISBN 978-1506386706. https://us.sagepub.com/en-us/nam/research-design/book255675 5. Федотова, Е.Л. Информационные технологии в науке и образовании [Текст]: учеб. пособие / Е.Л. Федотова, А.А. Федотов.- Москва: "ФОРУМ"; ИНФРА-М, 2024.- 335 с.- (Высшее образование). **Дополнительная** 6. Автоматизация физических исследований и эксперимента компьютерные измерения и виртуальные приборы на основе Lagvlew [Текст]: 30 лекций / П.А.Бутырин, Т.А.Васьковская, В.В.Каратаев [и др.].- 2-изд.,.- М.: ДМК Пресс, 2011.- 265 с. 7. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.-

	Алматы: Эверо, 2025.- 176 с. 8. Oroni, C. Z., Xianping, F., Ndunguru, D. D., Ani, A. Enhancing cyber safety in e-learning environment through cybersecurity awareness and policy compliance. — Computers & Security, Elsevier, 2025. https://doi.org/10.1016/j.cose.2024.104276 9. Czaja, P., Gdowski, B., Niemiec, M., et al. Cybersecurity challenges and opportunities of machine learning-based AI. — Neural Computing and Applications, Springer, 2025. https://link.springer.com/article/10.1007/s00521-025-11604-9

Код и название дисциплины	**UPK 5314 Управление проектами кибербезопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7M06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	2
Пререквизиты дисциплины	Кибербезопасность информационных систем / Анализ безопасности операционных систем
Постреквизиты дисциплины	Технологии управления информационной безопасностью, Системный анализ и моделирование в интеллектуальных системах информационной безопасности, Научно-исследовательская работа магистранта
Цель изучения дисциплины	Формирование у магистрантов компетенций в области инициации, планирования, реализации и контроля проектов по созданию и развитию систем обеспечения информационной безопасности с учётом рисков, ресурсов и требований стандартов.
Содержание дисциплины	Проект и проектная деятельность в сфере ИБ. Стандарты управления проектами: PMBOK, ISO 21500, PRINCE2. Жизненный цикл проекта по созданию системы защиты информации. Инициация проекта: обоснование, устав, заинтересованные стороны. Планирование содержания, сроков, стоимости и ресурсов (WBS, диаграмма Ганта, метод критического пути). Управление рисками проекта. Гибкие методологии (Scrum, Kanban) и DevSecOps-проекты. Управление командой и коммуникациями. Закупки средств защиты информации, техническое задание. Контроль исполнения, метрики и закрытие проекта.
Компетенции дисциплины	-знать стандарты и методологии управления проектами, жизненный цикл проекта в сфере ИБ; -понимать взаимосвязь содержания, сроков, стоимости, качества и рисков проекта по защите информации; -применять инструменты планирования, управления рисками и контроля исполнения проекта; -быть компетентным в разработке проектной документации, технического задания и руководстве проектной командой.

Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Ахметов, К.А. Моделирование бизнес-решений [Текст]: учебник для вузов / К.А. Ахметов.- Алматы: Эверо, 2022.- 444 с. 2. Емелина Н.К. Методы принятия оптимальных решений: учебно-практическое пособие / Н.К. Емелина.– Алматы: Эверо, 2020.- 216 с. https://baraev.elib.kz/ru/search/read_book/1170/ 3. Ахметов, К.А. Моделирование бизнес-решений [Текст]: учебник для вузов / К.А. Ахметов.- Алматы: EDP Hub (Идипи Хаб); Ай Пи Ар Медиа, 2024.- 558 с. 4. Kirgizbayeva, B.Zh. Modeling of business decisions [Текст]: manual for master degree students studying in all educational programs of the university / B.Zh. Kirgizbayeva, K.A. Akhmetov, Zh.Zh. Kozhamkulova; KazNAU.- Almaty: Aytumar, 2021.- 104 p. **Дополнительная** 5. Казагачев, В.Н. Вычислительные системы и сети [Текст]: учеб. пособие / В.Н. Казагачев.- Алматы: Эпиграф, 2022.- 240 с. 6. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2022. — 30 p. https://www.iso.org/standard/27001 7. Senft, S., Gallegos, F., Davis, A. Information Technology Control and Audit. — Elsevier, 2016. https://www.sciencedirect.com/book/9780128024379 8. Behl, A. et al. Cybersecurity compliance and auditing mechanisms. — Elsevier, 2023. https://www.sciencedirect.com/science/article/pii/S0268401223004567

Код и название дисциплины	**AIB 5312 Аудит информационной безопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	5
Форма обучения	очная
Семестр	2
Пререквизиты дисциплины	Кибербезопасность информационных систем / Анализ безопасности операционных систем, Анализ сетевой безопасности / Аналитические информационные системы безопасности, Криптографические методы и средства защиты информации / Принципы построения криптографических протоколов

Постреквизиты дисциплины	Технологии управления информационной безопасностью, Исследовательская практика, Научно-исследовательская работа магистранта
Цель изучения дисциплины	Формирование у магистрантов компетенций по планированию и проведению аудита информационной безопасности, оценке рисков и уровня защищённости информационных систем, анализу соответствия требованиям национальных и международных стандартов и подготовке аудиторского заключения.
Содержание дисциплины	Понятие, виды и цели аудита ИБ. Нормативная база: Закон РК «Об информатизации», Единые требования в области ИКТ и обеспечения ИБ, ISO/IEC 27001, ISO/IEC 27007, ISO 19011. Планирование аудита: объём, программа, ресурсы, аудиторская группа. Сбор аудиторских свидетельств: анализ документации, интервьюирование, технические проверки. Анализ защищённости периметра и внутренней инфраструктуры, сканирование уязвимостей. Аудит конфигураций ОС, СУБД и сетевого оборудования. Анализ исходного кода и тестирование на проникновение в рамках аудита. Оценка рисков и выявление несоответствий. Подготовка отчёта и аудиторского заключения, план корректирующих мероприятий.
Компетенции дисциплины	-знать виды, этапы и нормативную базу аудита информационной безопасности; -понимать методы сбора аудиторских свидетельств, оценки рисков и анализа защищённости объектов аудита; -применять инструментальные средства анализа защищённости и методики проверки соответствия требованиям стандартов; -быть компетентным в планировании аудита, документировании его результатов и подготовке аудиторского заключения.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Прохорова, О.В. Информационная безопасность и защита информации. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. http://rmebrk.kz/book/1183813 2. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов. . - М: Юрайт, 2022. - 104 с. - (Высшее образование). - ISBN 978-5-534-14590-8. http://rmebrk.kz/book/1179658 3. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 4. Жангисина, Г.Д. Теория и методика компьютерного моделирования для задач базы данных и глобальной сети

	[Текст]: учеб. пособие / Г.Д. Жангисина, Т. Хакимова.- Алматы: Ғылым, 2007.- 94с. https://lib.kaznaru.edu.kz/res/Injenerlik/Hakimova%20T.7.index.pdf **Дополнительная** 5. Peltier, T. R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. — Springer, 2020. https://link.springer.com/book/10.1007/978-3-030-58290-6 6. ISO/IEC 27001:2022 Information security management systems — Requirements. — ISO, 2022 https://www.iso.org/standard/27001 7. Senft, S., Gallegos, F., Davis, A. Information Technology Control and Audit. — Elsevier, 2016. https://www.sciencedirect.com/book/9780128024379

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА: 7М06301 – «ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Присуждаемая степень: магистр технических наук по образовательной программе 7М06301 – «Интеллектуальные системы информационной безопасности»

2 КУРС

Цикл	Код	Дисциплины	Академ. кредиты
3 семестр – 30 академических кредитов			
Вузовский компонент – 7 кр.			
ПД	ITAZI 6310	Интеллектуальные технологии анализа и защиты информации	7
Компонент по выбору – 20 кр.			
ПД	BBDOI 6315	Безопасность больших данных и облачных инфраструктур	7
	TUIB 6316	Технологии управления информационной безопасностью	
ПД	IMMIB 6317	Интеллектуальные модели и методы в информационной безопасности	7
	SAMISIB 6318	Системный анализ и моделирование в интеллектуальных системах информационной безопасности	
ПД	IIAU 6319	Искусственный интеллект в анализе угроз	6
	GIIK 6320	Генеративный искусственный интеллект в кибербезопасности	
Научно-исследовательская работа магистранта – 3 кр.			
НИРМ	NIRM 6503	Научно-исследовательская работа магистранта	3
4 семестр – 30 академических кредитов			
Вузовский компонент – 5 кр.			
ПД	IP 6311	Исследовательская практика	5
Научно-исследовательская работа магистранта – 17 кр.			
НИРМ	NIRM 6504	Научно-исследовательская работа магистранта	17
Итоговая аттестация – 8 кр.			
ИА	—	Оформление и защита магистерской диссертации (ОиЗМД)	8

Формуляр для описания дисциплины

Код и название дисциплины	**ITAZI 6310 Интеллектуальные технологии анализа и защиты информации**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/ВК
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	7
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Методы исследований в кибербезопасности, Анализ сетевой безопасности / Аналитические информационные системы безопасности, Криптографические методы и средства защиты информации / Принципы построения криптографических протоколов
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование у магистрантов компетенций по применению и разработке методов Data Mining, машинного обучения и искусственного интеллекта для анализа данных безопасности, выявления аномалий, обнаружения и прогнозирования киберугроз.
Содержание дисциплины	Интеллектуальные технологии в системах защиты информации. Источники и типы данных безопасности. Предобработка данных, инженерия и отбор признаков. Методы Data Mining: классификация, кластеризация, ассоциативные правила. Обнаружение аномалий и вторжений. Нейронные сети и глубокое обучение в задачах ИБ. Анализ текстов и журналов событий (NLP). Интеллектуальные системы поддержки принятия решений в SOC. Оценка качества и интерпретируемость моделей (XAI). Безопасность самих интеллектуальных систем: состязательные атаки, отравление данных. Разработка прототипа интеллектуальной системы защиты на Python.
Компетенции дисциплины	-знать методы Data Mining, машинного обучения и искусственного интеллекта, применяемые для анализа и защиты информации; -понимать особенности данных безопасности и ограничения интеллектуальных моделей, включая их уязвимость к состязательным атакам; -применять интеллектуальные методы для обнаружения аномалий, классификации угроз и анализа журналов событий; -быть компетентным в разработке, оценке и оптимизации моделей обработки данных и прогнозирования угроз.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)

Список литературы	**Основная** 1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 2. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 3. Яворский, В.В. Процессы формирования и развития информационных систем [Текст]: учеб. пособие / В.В. Яворский, Т.О. Перемитина.- Алматы: Эпиграф, 2022.- 108 с. 4. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 5. Партыка, Т.Л. Информационная безопасность [Текст]: учеб. пособие / Т.Л. Партыка, И.И. Попов.- 5-е изд., перераб. и доп.- М.: Форум; ИНФРА-М, 2014.- 432 с **Дополнительная** 6. Абдиев К.С. Информационные технологии производства статистических данных [Текст] / Абдиев К.С.- Алматы: Агенства РК по статистике, 2006.- 280 с. 7. Черикбаева, Л.Ш. Деректерді талдаудың топтық шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 8. Остроух, А.В. Введение в искусственный интеллект: монография. — Красноярск: Научно-инновационный центр, 2020. — 250 с. — ISBN 978-5-907208-26-1. — DOI: 10.12731/978-5-907208-26-1. https://rmebrk.kz/book/1188729 9. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с.

Код и название дисциплины	**BBDOI 6315 Безопасность больших данных и облачных инфраструктур**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	7
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ безопасности операционных систем / Кибербезопасность информационных систем, Анализ сетевой безопасности / Аналитические информационные

	системы безопасности, Криптографические методы и средства защиты информации / Принципы построения криптографических протоколов
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование способности проектировать защищённые конвейеры обработки больших данных и облачные среды, анализировать данные безопасности в масштабе, выявлять аномалии и обеспечивать защиту персональных данных и приватность.
Содержание дисциплины	Архитектуры больших данных (Hadoop, Spark, Kafka) и модели угроз. Модели облачных услуг IaaS, PaaS, SaaS и модель разделённой ответственности. Управление доступом в облаке, шифрование данных при хранении и передаче. Безопасность контейнеров и Kubernetes, проверка Infrastructure as Code. Защита распределённых хранилищ и NoSQL. Приватность: анонимизация, псевдонимизация, дифференциальная приватность, гомоморфное шифрование. Потоковая аналитика журналов и обнаружение аномалий на платформах больших данных. Мониторинг облачной безопасности: CSPM, CWPP, облачные SIEM. ISO/IEC 27017/27018, законодательство РК о персональных данных.
Компетенции дисциплины	-знать архитектуры платформ больших данных и облачных сред, их модели угроз и механизмы защиты; -понимать модель разделённой ответственности и методы обеспечения приватности данных; -применять технологии обработки больших данных для анализа событий безопасности и обнаружения аномалий; -быть компетентным в проектировании защищённых облачных сред и конвейеров данных с учётом требований к защите персональных данных.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Бимұрат, Ж. Big Data технологияларының негіздері [Мәтін]: оқу құралы / Ж. Бимұрат; Ғ.Дәукеев атын. Алматы энергетика және байланыс ун-ті КЕАҚ.- Алматы:Альманахъ,2023.-131б. 2. Bart Baesens Analytics in a Big Data World: The Essential Guide to Data Science and its Applications. : Wiley, 2014. - 243- ISBN 978-1-118-89270-1. https://rmebrk.kz/book/1178447 3. Цехановский, В.В. Управление данными [Текст]: учебник / В.В. Цехановский, В.Д. Чертовской.- СПб.: Лань, 2015.- 432 с 4. Mukasheva, A.K. et al. Big Data analytics : Textbook (for students of all specialties). / A.K. Mukasheva, T.F. Umarov, I.A. Zimin. - Almaty: Lantar books LLC, 2022. - 116- ISBN 978-601-7659-94-3. https://rmebrk.kz/book/1177465

	5. Силен, Д. Основы Data Science и Big Data. Python и наука о данных [Текст] / Д. Силен, А. Мейсман, М. Али.- СПб.: Питер, 2020.- 336 с.- (Б-ка программиста). **Дополнительная** 6. Казагачев, В.Н. Цифровизация производства (по отраслям) [Текст]: учеб.-метод. пособие / В.Н. Казагачев, А.А. Мусина.- Алматы: Эпиграф, 2023.- 204 с. 7. Черикбаева, Л.Ш. Деректерді талдаудың топтық шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 8. Кайбасова Д.Ж. Автоматтандырылған ақпараттық жүйелерді жобалауда деректер қорын қолдану тәсілдері: Монография /Д.Ж. Кайбасова, Б.О. Мухаметжанова, Э.К. Сейпишева; Қарағанды мемлекеттік техникалық университеті. – Алматы: Эверо, 2020. - 186 б. https://baraev.elib.kz/ru/search/read_book/3992/ 9. García, L., Parra, L., Jimenez, J. M., Lloret, J. IoT and Big Data Analytics for Smart Agriculture. — Springer Nature, 2020. https://link.springer.com/book/10.1007/978-3-030-35389-6

Код и название дисциплины	**TUIB 6316 Технологии управления информационной безопасностью**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	7
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ безопасности операционных систем / Кибербезопасность информационных систем, Аудит информационной безопасности, Управление проектами кибербезопасности
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование способности проектировать, внедрять и совершенствовать систему менеджмента информационной безопасности организации, обосновывать решения по обработке рисков и оценивать эффективность процессов управления ИБ.
Содержание дисциплины	Нормативно-правовая база ИБ в РК: Закон «Об информатизации», Единые требования в области ИКТ и обеспечения ИБ. Стандарты и фреймворки: ISO/IEC 27000, NIST CSF 2.0, COBIT. Построение СМИБ, цикл PDCA. Управление рисками ИБ по ISO/IEC 27005. Разработка политик, регламентов и нормативной документации. Управление инцидентами (ISO/IEC 27035)

	и взаимодействие с оперативными центрами ИБ. Управление непрерывностью бизнеса (ISO 22301). Метрики и оценка эффективности СМИБ (ISO/IEC 27004), подготовка к сертификации. GRC-платформы.
Компетенции дисциплины	-знать национальную нормативную базу и международные стандарты в области управления ИБ; -понимать процессный подход к построению СМИБ и методы оценки и обработки рисков; -применять методики разработки политик, регламентов и планов обеспечения непрерывности бизнеса; -быть компетентным в оценке эффективности СМИБ и подготовке организации к аудиту и сертификации.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Борух, О.А. Облачные вычисления [Текст]: учеб. пособие / О.А. Борух.- Алматы: Alem book, 2024.- 200 с. 2. Бабаш, А.В., Баранова, Е.К., Ларин, Д.А. Информационная безопасность. История специальных методов криптографической деятельности. — М., 2020. — 236 с. https://rmebrk.kz/book/1176322 3. Гумерова, Г.И. Электронное правительство [Текст]: учебник для вузов / Г.И. Гумерова, Э.Ш. Шаймиева.- 5-е изд., испр. и доп.- М.: Юрайт, 2023.- 227 с. 4. Zarubin, M.Yu., Ybytaeva, G.S. Cryptographic Systems. — Almaty: Bastau, 2021. — 320 p. https://rmebrk.kz/book/1176885 5. Жатканбаева, А.Е. Информационное право (Общая часть) [Текст]: учеб. пособие / А.Е. Жатканбаева; КазНУ им. аль-Фараби.- Алматы: Қазақ университеті, 2020.- 150 с. **Дополнительная** 6. Мазалов, В.В. Математическая теория игр и приложения [Текст]: учеб. пособие / В.В. Мазалов.- СПб.: Лань, 2010.- 448 с. 7. Дусекеев, Р.М., Мутанов, Г.М., Мамыкова, Ж.Д. Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета // Вестник КазГУ. — 2016. — № 4. — С. 80–88. 8. Тлеккабылова, Д.Ж., Иксебаева, Ж.С. Информационная безопасность как элемент информационной культуры. - 2014. - С.103-104. https://rmebrk.kz/book/1144347 9. Якубова, М.З., Сериков, Т.Г., Мукашева, А.К. Қазіргі заманғы криптографиялық қорғау және стеганография әдістерін өзгерту арқылы IP PBX ASTERISK негізінде IP телекоммуникациялық желісінің қауіпсіздік деңгейін арттыру әдістерін талдау, зерттеу, модельдеу және әзірлеу: монография. — Алматы: Дарын, 2024. — 190 б.

Код и название дисциплины	**IMMIB 6317 Интеллектуальные модели и методы в**

	информационной безопасности
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	7
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ сетевой безопасности / Аналитические информационные системы безопасности, Методы исследований в кибербезопасности
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование способности разрабатывать, обучать, оценивать и оптимизировать интеллектуальные модели для задач обнаружения вторжений, классификации вредоносного ПО и оценки рисков в условиях неопределённости и неполноты данных.
Содержание дисциплины	Интеллектуальные системы в ИБ: классы задач и обзор методов. Подготовка данных безопасности, эталонные наборы (CIC-IDS, UNSW-NB15). Классические методы машинного обучения для обнаружения вторжений и вредоносного ПО. Нейросетевые модели и глубокое обучение. Нечёткая логика и нечёткий вывод для оценки рисков. Байесовские сети и вероятностные модели угроз. Эволюционные и роевые алгоритмы оптимизации систем защиты. Метрики качества, валидация и интерпретируемость моделей (XAI). Состязательное машинное обучение и устойчивость моделей.
Компетенции дисциплины	-знать классы интеллектуальных моделей и методов, применяемых в задачах информационной безопасности; -понимать ограничения моделей, метрики их качества и вопросы устойчивости к состязательным атакам; -применять методы машинного обучения, нечёткой логики и вероятностного вывода для обнаружения угроз и оценки рисков; -быть компетентным в разработке, валидации и оптимизации интеллектуальных моделей в условиях неопределённости.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Андрейчиков, А.В., Андрейчикова, О.Н., 2024. — 530 с. 2. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 3. Шукаев, Д.Н. Прикладные методы оптимизации [Текст]: учебник / Д.Н. Шукаев; МОН РК.- Алматы:

	Эверо, 2020.- 220 с. 4. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 5. Силен, Д. Основы Data Science и Big Data. Python и наука о данных [Текст] / Д. Силен, А. Мейсман, М. Али.- СПб.: Питер, 2020.- 336 с.- (Б-ка программиста). **Дополнительная** 6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 7. Бурибаев, Ж.А. Нысанды тану мен жіктеу жүйесіне арналған машиналық оқытудың тиімді алгоритмдерін әзірлеу [Мәтін]: монография / Ж.А. Бурибаев; әл-Фараби атын. ҚазҰУ.- Алматы: Дарын, 2022.- 126 б. 8. Остроух, А.В. Введение в искусственный интеллект: монография. — Красноярск: Научно-инновационный центр, 2020. — 250 с. — ISBN 978-5-907208-26-1. — DOI: 10.12731/978-5-907208-26-1. https://rmebrk.kz/book/1188729 9. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с.

Код и название дисциплины	**SAMISIB 6318 Системный анализ и моделирование в интеллектуальных системах информационной безопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	7
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ сетевой безопасности / Аналитические информационные системы безопасности, Методы исследований в кибербезопасности, Управление проектами кибербезопасности
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование методологии системного анализа и моделирования сложных информационных и социотехнических систем, умений строить модели систем защиты, оценивать их эффективность и надёжность и оптимизировать решения по повышению безопасности в условиях неопределённости.

Содержание дисциплины	Основы системного анализа: система, структура, свойства; интеллектуальная система ИБ как сложная система. Структурное моделирование: IDEF0, UML/SysML, декомпозиция. Графы и деревья атак, модели распространения угроз. Марковские модели и модели надёжности систем защиты. Теоретико-игровые модели «атакующий — защитник». Имитационное моделирование процессов ИБ: дискретно-событийный и агентный подходы. Многокритериальный анализ и методы принятия решений (МАИ, TOPSIS). Оптимизация систем защиты при ограниченных ресурсах. Оценка эффективности и киберустойчивости.
Компетенции дисциплины	-знать методы системного анализа, структурного, вероятностного и имитационного моделирования; -понимать свойства сложных информационных и социотехнических систем и критерии их эффективности и надёжности; -применять графы атак, марковские, теоретико-игровые и имитационные модели для исследования процессов ИБ; -быть компетентным в обосновании и оптимизации решений по повышению безопасности систем в условиях неопределённости.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Андрейчиков, А.В., Андрейчикова, О.Н., 2024. — 530 с. 2. Емелина Н.К. Методы принятия оптимальных решений: учебно-практическое пособие / Н.К. Емелина.– Алматы: Эверо, 2020.- 216 с. https://baraev.elib.kz/ru/search/read_book/1170/ 3. Боуш, Г.Д. Методология научного исследования (в кандидатских и докторских диссертациях) [Текст]: учебник / Г.Д. Боуш, В.И. Разумов.- М.: ИНФРА-М, 2025.- 227 с.- (Высшее образование). 4. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ 5. Федотова, Е.Л. Информационные технологии в науке и образовании [Текст]: учеб. пособие / Е.Л. Федотова, А.А. Федотов.- Москва: "ФОРУМ"; ИНФРА-М, 2024.- 335 с.- (Высшее образование). **Дополнительная** 6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 7. Черикбаева, Л.Ш. Деректерді талдаудың топтық шешімдер негізіндегі әдістері мен алгоритмдері [Мәтін]: монография / Л.Ш. Черикбаева; Ақпараттық және

	есептеуіш технологиялар ин-ты.- Алматы: Дарын, 2024.- 129 б. 8. Методы и модели исследования сложных систем и обработки больших данных : монография. / И.Ю. Парамонов, В.А. Смагин, Н.Е. Косых, А.Д. Хомоненко; под ред. В.А. Смагина, А.Д. Хомоненко. - Санкт-Петербург: Лань, 2020. - 236 с. - ISBN 978-5-8114-4006-1. https://rmebrk.kz/book/1179911 9. Mitchell, M. Complexity: A Guided Tour. — Oxford University Press / Springer access, 2009. https://link.springer.com/book/10.1007/978-3-030-27672-0

Код и название дисциплины	**IIAU 6319 Искусственный интеллект в анализе угроз**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности
Кол-во академических кредитов	6
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ сетевой безопасности / Аналитические информационные системы безопасности, Методы исследований в кибербезопасности
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование навыков разработки и внедрения решений на основе искусственного интеллекта для выявления, классификации и прогнозирования киберугроз, интерпретации их результатов и интеграции в процессы центра мониторинга ИБ.
Содержание дисциплины	Жизненный цикл анализа угроз и роль ИИ, матрица MITRE ATT&CK. Сбор и подготовка данных об угрозах, инженерия признаков. Обнаружение сетевых вторжений методами машинного и глубокого обучения. Классификация и кластеризация вредоносного ПО по данным статического и динамического анализа. Обнаружение фишинга методами NLP. Поведенческая аналитика и обнаружение аномалий (UEBA, автоэнкодеры). Прогнозирование угроз и анализ временных рядов. ИИ в Threat Intelligence и Threat Hunting, интеграция с SIEM/SOAR. Этические и правовые аспекты применения ИИ в ИБ.
Компетенции дисциплины	-знать методы искусственного интеллекта, применяемые для анализа, классификации и прогнозирования киберугроз; -понимать жизненный цикл анализа угроз и место ИИ-решений в процессах мониторинга и реагирования; -применять методы машинного и глубокого обучения, NLP и анализа временных рядов к реальным данным об угрозах;

	-быть компетентным в интерпретации результатов ИИ-моделей и их интеграции в процессы SOC с учётом этических требований.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/ 3. Актаева, А. Надежность систем: тестирование и защита информации [Текст]: Ч.1.: учебник / А. Актаева, Л. Давлеткереева, А. Муканова.- Алматы: Эверо, 2020.- 324 с. 4. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 5. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с. https://baraev.elib.kz/ru/search/read_book/3586/ **Дополнительная** 6. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с. 7. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – P. 70–83. https://rmebrk.kz/magazine/6475# 8. Amanzholova, S., Mutanov, G., Mukhanov, S., Ussatova, O., & Razaque, A. AI-powered system for network activity monitoring and detection of SQL injection attacks using Zabbix and Grafana // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – Is. 3. – P. 61–83. https://rmebrk.kz/magazine/6475#

Код и название дисциплины	**GIIK 6320 Генеративный искусственный интеллект в кибербезопасности**
ППС дисциплины	ППС кафедры IT-технологий: _____
Цикл дисциплины	ПД/КВ
Уровень обучения	Магистратура (научно-педагогическое направление)
Образовательная программа	7М06301 – Интеллектуальные системы информационной безопасности

Кол-во академических кредитов	6
Форма обучения	очная
Семестр	3
Пререквизиты дисциплины	Анализ безопасности операционных систем / Кибербезопасность информационных систем, Анализ сетевой безопасности / Аналитические информационные системы безопасности, Методы исследований в кибербезопасности
Постреквизиты дисциплины	Исследовательская практика, Научно-исследовательская работа магистранта, Оформление и защита магистерской диссертации
Цель изучения дисциплины	Формирование способности проектировать, исследовать и внедрять инновационные решения на основе генеративного ИИ для задач кибербезопасности, а также выявлять и нейтрализовать угрозы, связанные с генеративными моделями, с учётом этических и правовых требований.
Содержание дисциплины	Генеративные модели: трансформеры, GAN, VAE, диффузионные модели. LLM в центре мониторинга ИБ: анализ журналов, суммаризация инцидентов, ассистенты аналитика. Генеративный ИИ в анализе и безопасной разработке кода. Генерация синтетических данных для обучения систем обнаружения. Угрозы безопасности LLM: промпт-инъекции, утечки данных, отравление; OWASP Top 10 for LLM Applications. Дипфейки и ИИ-социальная инженерия, методы обнаружения. Защита генеративных моделей: red teaming, защитные механизмы, RAG-архитектуры. Регулирование и этика ИИ: NIST AI RMF, ISO/IEC 42001. Исследовательский мини-проект.
Компетенции дисциплины	-знать архитектуры генеративных моделей и области их применения в кибербезопасности; -понимать угрозы, связанные с генеративным ИИ, и принципы ответственного использования ИИ; -применять генеративные модели для анализа журналов, кода и генерации синтетических данных, а также меры защиты LLM-систем; -быть компетентным в проектировании и исследовании инновационных решений на базе генеративного ИИ с оценкой их эффективности и соблюдением этических требований.
Форма итогового контроля	Экзамен
Продолжительность дисциплины	1 академический период (20 недель)
Список литературы	**Основная** 1. Андрейчиков, А.В., Андрейчикова, О.Н. Интеллектуальные информационные системы и методы искусственного интеллекта: учебник. — М.: ИНФРА-М, 2024. — 530 с. 2. Яворский В.В. Интеллектуальные информационные технологии: учебник / В.В. Яворский. – Алматы: Эверо, 2020. – 344 с. https://baraev.elib.kz/ru/search/read_book/3961/

	3. Баженов, Р.И. Интеллектуальные информационные технологии в управлении: учебное пособие. — М.: Ай Пи Ар Медиа, 2023. — 124 с. https://lib.kaznaru.edu.kz/res/ebook_1930/index.html 4. Абденов А.Ж., А.А. Абденова Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2020. – 152 с. https://baraev.elib.kz/ru/search/read_book/3586/ 5. Горлушкина Н.Н. Системный анализ и моделирование информационных процессов и систем. – СПб: Университет ИТМО, 2016. – 120 с. https://nqrt.elib.kz/ru/search/read_book/10982/ **Дополнительная** 6. Абдыкаримов, Б.А. Разработка моделей и алгоритмов автоматизированной оценки знаний с использованием технологий искусственного интеллекта [Текст]: кн. 11 / Б.А. Абдыкаримов, В.В. Егоров, Г.М. Яворская; МОН РК; КГТУ.- Караганда: ЕГИ, 2006.- 162 с. 7. Кинтонова, А.Ж. Искусственный интеллект в образовательной и научно-исследовательской деятельности [Текст]: монография / А.Ж. Кинтонова.- Алматы: Эверо, 2025.- 176 с. 8. Alin, G., Konsbayev, A., & Abdikaparov, N. Harnessing artificial intelligence for advanced threat detection in network infrastructure // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – P. 70–83. https://rmebrk.kz/magazine/6475# 9. Amanzholova, S., Mutanov, G., Mukhanov, S., Ussatova, O., & Razaque, A. AI-powered system for network activity monitoring and detection of SQL injection attacks using Zabbix and Grafana // International Journal of Information and Communication Technologies. – 2025. – Vol. 6. – Is. 3. – P. 61–83. https://rmebrk.kz/magazine/6475#