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#