Институт т автоматики и информационных технологий
Кафедра «Кибербезопасность, обработка и хранение информации»

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
«7М06302 - Комплексное обеспечение информационной безопасности»
шифр и наименование образовательной программы

Код и классификация области образования: **7М06 Информационно-коммуникационные технологии**
Код и классификация направлений подготовки: **7М063 Информационная безопасность**
Группа образовательных программ: **М095 Информационная безопасность**
Уровень по НРК: **7**
Уровень по ОРК: **7**
Срок обучения: **1,5 года**
Объем кредитов: **90 кредитов**

Алматы 2025

Образовательная программа «7М06302 - Комплексное обеспечение информационной безопасности» утверждена на заседании Учёного совета КазНИТУ им. К.И.Сатпаева.
Протокол № _10___ от "__06__" _март___ 2025 г.

Рассмотрена и рекомендована к утверждению на заседании Учебно-методического совета КазНИТУ им. К.И.Сатпаева.
Протокол № __3__ от "_20___" _декабрь_ 2024 г.

Образовательная программа «7М06302 - Комплексное обеспечение информационной безопасности» разработан академическим комитетом по направлению «7М063 Информационная безопасность»

Ф.И.О.	Учёная степень/учёное звание	Должность	Место работы	Подпись
Председатель академического комитета:				
Покусов Виктор Владимирович		Председатель	Казахстанская Ассоциация Информационной безопасности	
Профессорско-преподавательский состав:				
Айтхожаева Евгения Жамалхановна	Кандидат технических наук, доцент	Профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Рахметулаева Сабина Батырхановна	Доктор PhD	Профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Сатыбалдиева Рысхан Жакановна	Кандидат технических наук	Ассоциированный профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Сербин Василий Валерьевич	Кандидат технических наук	Ассоциированный профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Жумагалиев Биржан Изимович	Кандидат технических наук, доцент	Ассоциированный профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Алимсеитова Жулдыз Кенесхановна	Доктор PhD	Ассоциированный профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Юбузова Халича Ибрагимовна	Доктор PhD	Ассоциированный профессор	НАО «КазНИТУ им.К.И.Сатпаева»	
Представители работодателей:				
Мамырбаев Оркен Жумажанович	Доктор PhD, ассоциированный профессор	Заместитель генерального директора	РГП «Институт информационных и вычислительных технологий»	
Конысбаев Әмірет Тұякұлы	Кандидат физико-математических наук	Президент	Ассоциация инновационных компаний СЭЗ «ПИТ»	
Батыргалиев Асхат Болатханович	Доктор PhD, ассоциированный профессор	Погранслужба КНБ, контрразведки	В/ч № 01068,	
Обучающиеся:				
Абилкайырова Алина Сериккызы		Обучающийся 3 курса	НАО «КазНИТУ им.К.И.Сатпаева»	
Элле Венера		Обучающийся 1 курса, докторантура	НАО «КазНИТУ им.К.И.Сатпаева»	

Оглавление

1. Описание образовательной программы

Образовательная программа 7М06302 «Комплексное обеспечение информационной безопасности» направлена на обучение магистрантов профильного направления. Программа включает базовые и профильные дисциплины с достижением соответствующих компетенций, а также прохождение различных видов практик (производственная практика, экспериментально-исследовательская и стажировка). Профессиональная деятельность магистров направлена на область защиты и безопасности информации, а именно на комплексное обеспечение информационной безопасности и инженерно-техническую защиту информации. Подготовка магистров профильного направления по информационной безопасности будет осуществляться по обновленной образовательной программе 7М06302 «Комплексное обеспечение информационной безопасности». Программы дисциплин и модулей образовательной программы имеют междисциплинарный и мультидисциплинарный характер, разрабатываются с учетом соответствующих образовательных программ ведущих университетов мира и международного классификатора профессиональной деятельности по направлению информационная безопасность. Образовательная программа обеспечивает применение индивидуального подхода к обучающимся, трансформацию профессиональных компетенций из профессиональных стандартов и стандартов квалификаций в результаты обучения и пути их достижения. Образовательная программа разрабатывалась на основе анализа трудовых функций администратора по информационной безопасности, аудитора информационной безопасности, инженера по защите информации, заявленных в профессиональных стандартах. Основным критерием завершенности обучения по программам магистратуры является освоение всех видов учебной и профессиональной деятельности магистранта. В случае успешного завершения полного курса обучающемуся присваивается степень магистр техники и технологий по образовательной программе 7М06302 «Комплексное обеспечение информационной безопасности». Выпускник может выполнять следующие виды трудовой деятельности: - проектно-конструкторская; - производственно-технологическая; - экспериментально-исследовательская; - организационно-управленческая; - эксплуатационная. В разработке образовательной программы участвовали представители казахстанских компаний и ассоциаций, специалисты ведомственных структур в области защиты и безопасности.

2. Цель и задачи образовательной программы

Цель ОП: Подготовка специалистов для профессиональной деятельности в сфере информационной безопасности, умеющих применять различные технологии, знания, навыки и компетенции в организации, управлении и проектировании систем защиты информации

Задачи ОП:

Подготовка высококвалифицированных специалистов, умеющих решать следующие задачи:

- планирование работы по аудиту информационной безопасности;
- организационное обеспечение аудита ИБ;
- проведение анализа соответствия проектной, эксплуатационной и технической документации по информационной безопасности требованиям в сфере ИКТ и обеспечения ИБ объекта аудита ИБ;
- анализ текущего состояния защищенности объекта аудита ИБ;
- выявление и устранение уязвимостей;
- проведение мониторинга и расследования инцидентов ИБ;
- разработка модели угроз безопасности информации в предприятиях;
- разработка технического задания на создание системы защиты информации.

Магистр образовательной программы 7М06302 «Комплексное обеспечение информационной безопасности» ориентирован на самостоятельное определение цели профессиональной деятельности и выбора адекватных методов и средств их достижения, осуществление инновационной деятельности по получению новых знаний. Кроме того, ориентирован на организацию, проектирование, разработку, управление и аудит систем защиты и безопасности информации прикладного назначения для всех отраслей экономики, государственных организаций и других областей деятельности

3. Требования к оценке результатов обучения образовательной программы

Образовательная программа разработано в соответствии с Государственными общеобязательными стандартами высшего и послевузовского образования, утвержденными приказом Министра науки и высшего образования Республики Казахстан от 20 июля 2022 года №2 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 28916) и отражает результаты обучения, на основании которых разрабатываются учебные планы (рабочие учебные планы, индивидуальные учебные планы обучающихся) и рабочие учебные программы по дисциплинам (силлабусы). Освоение дисциплин не менее 10% от общего объема кредитов образовательной программы с применением МООС на официальной платформе https://polytechonline.kz/cabinet/login/index.php/, а также посредством изучения дисциплин через международную образовательную платформу Coursera https://www.coursera.org/

Оценивание результатов обучения проводится по разработанным тестовым заданиям в рамках образовательной программы в соответствии с требованиями государственного общеобязательного стандарта высшего и послевузовского образования. При проведении оценивания результатов обучения для обучающихся создаются единые условия и равные возможности для демонстрации уровня своих знаний, умений и навыков. При проведении промежуточной аттестации в онлайн форме применяется онлайн прокторинг.

4. Паспорт образовательной программы

4.1. Общие сведения

№	Название поля	Примечание
1	Код и классификация области образования	7М06 Информационно-коммуникационные технологии
2	Код и классификация направлений подготовки	7М063 Информационная безопасность
3	Группа образовательных программ	М095 Информационная безопасность
4	Наименование образовательной программы	7М06302 - Комплексное обеспечение информационной безопасности
5	Краткое описание образовательной программы	Профессиональная деятельность выпускников включает в себя: образование, государственные и ведомственные структуры, экономику и промышленность государства, область здравоохранения. Объектами профессиональной деятельности выпускников магистерских программ по образовательной программе 7М06302 «Комплексное обеспечение информационной безопасности» являются: − органы государственного управления; − отделы информационной безопасности и департаменты ведомственных организаций; − отделы информационной безопасности, IT отделы и департаменты финансовых организаций; − отделы информационной безопасности, IT отделы и департаменты промышленных предприятий; − отделы и департаменты информационной безопасности государственных организаций и коммерческих структур. Основными функциями профессиональной деятельности магистрантов являются: проведение исследовательских работ в сфере защиты и безопасности информации; аудит, анализ уязвимостей и расследование инцидентов в системах информационной безопасности; проектирование, внедрение, эксплуатация, администрирование, сопровождение и тестирование систем информационной безопасности предприятий Направления профессиональной деятельности, следующие: − проектирование, разработка, внедрение и эксплуатация систем информационной безопасности; − анализ, тестирование и выявление уязвимостей системы; − аудит информационной безопасности
6	Цель ОП	Подготовка специалистов для профессиональной деятельности в сфере информационной безопасности, умеющих применять различные технологии, знания, навыки и компетенции в

		организации, управлении и проектировании систем защиты информации
7	Вид ОП	Обновленная ОП
8	Уровень по НРК	7
9	Уровень по ОРК	7
10	Отличительные особенности ОП	нет
11	Перечень компетенций образовательной программы:	Выпускник профильной магистратуры, должен: 1) иметь представление: – о противоречиях и социально-экономических последствиях процессов глобализации; – о профессиональной компетентности в области защиты и безопасности информации; – о технологии виртуализации ресурсов и платформ; – об интеллектуализации средств обеспечения информационной безопасности; - о технологиях защиты БД; – об алгоритмах криптографической защиты информации; – об анализе больших данных. 2) знать: – психологические методы и средства повышения эффективности и качества обучения; – алгоритмы криптографической защиты информации; – стандарты ИБ и критерии оценки безопасности ИТ; - технологии виртуализации ресурсов и платформ и системы виртуализации от ведущих производителей; - угрозы и риски систем виртуализации, принципы построения гипервизоров и их уязвимости; – организацию IP-сетей, структуру IP-пакетов и IPпротоколов; – внутреннюю организацию носителей информации ОС; – методы и средства хранения ключевой информации и шифрования; – разновидности и принципы аутентификации; – требования к межсетевым экранам и системам обнаружения вторжений; - технологии защиты БД и методы проектирования безопасных БД; - организацию системы защиты и безопасности БД; – методы и инструменты активного аудита; – инженерно-техническую защиту информации. 3) уметь: – критически анализировать существующие концепции, теории и подходы к анализу процессов и явлений; – интегрировать знания, полученные в рамках

		разных дисциплин для решения исследовательских задач в новых незнакомых условиях; – путем интеграции знаний выносить суждения и принимать решения на основе неполной или ограниченной информации; – проводить информационно-аналитическую и информационно-библиографическую работу с привлечением современных информационных технологий; – креативно мыслить и творчески подходить к решению новых проблем и ситуаций; – свободно владеть иностранным языком на профессиональном уровне, позволяющим проводить исследования; – обобщать результаты аналитической работы в виде диссертации, статьи, отчета, аналитической записки и др.; – применять алгоритмы криптографической защиты информации; - применять стандарты ИБ и проводить оценку безопасности ИТ; - применять системы виртуализации от ведущих производителей; - выявлять угрозы и риски систем виртуализации; – применять методы и средства хранения ключевой информации и шифрования; – работать с межсетевыми экранами и системами обнаружения вторжений; – применять технологии защиты БД и методы проектирования безопасных БД; – организовать систему защиты и безопасности БД; – применять методы и инструменты активного аудита; – применять инструменты анализа больших данных. 4) иметь навыки: – профессионального общения и межкультурной коммуникации; – организации и защиты безопасности БД; – проведения аудита информационной безопасности; – применения алгоритмов криптографической защиты информации; – выявления угроз и противодействия им; – работы с Big Data; – расширения и углубления знаний, необходимых для повседневной профессиональной деятельности 5) быть компетентным: – в организации систем информационной безопасности; – в проведении аудита информационной

		безопасности; – в обеспечении информационной безопасности организации; –в способах обеспечения постоянного обновления знаний, расширения профессиональных навыков и умений
12	Результаты обучения образовательной программы:	**РО1:** Уметь организовать устойчивую систему защиты и безопасности БД. Применять технологии защиты БД и методы проектирования безопасных БД. **РО2:** Знать и применять технологии виртуализации ресурсов и платформ и системы виртуализации от ведущих производителей. Знать угрозы и риски систем виртуализации, принципы построения гипервизоров и их уязвимости. **РО3:** Знать организацию IP-сетей, структуру IP-пакетов и IP-протоколов, разновидности и принципы аутентификации. Уметь проводить оценку защищенности сетевых операционных систем **РО4:** Быть компетентным в вопросах выявления киберпреступлении и компьютерной криминалистики. Уметь использовать средства распознавания и противодействия кибератакам. Знать технические средства и методы технической защиты информации, быть компетентным в организации инженерно-технической защиты информации. **РО5:** Уметь использовать на практике нормативные документы при планировании и организации научно-производственных работ в области информационной безопасности. Знать современные и перспективные направления развития криптографической защиты информации и применять ее на практике. **РО6:** Уметь самостоятельно приобретать, осмысливать, структурировать и использовать в профессиональной деятельности новые знания и умения, развивать свои инновационные способности для создания комплексной стойкой защищенной инфраструктуры организаций. **РО7:** Уметь анализировать большие данные, знать методы и средства анализа больших данных. Способность формулировать проблемы, задачи и методы научного исследования **РО8:** Уметь применять различные методы поддержки принятия решения, оперативно контролировать исполнение работ, разрешать противоречия между членами команды, управлять рисками, возникающими при реализации проектов. Знать современные стандарты в области управления проектами и их характеристики. Владение иностранными языками на

		профессиональном уровне для партнерства в интересах устойчивого развития
13	Форма обучения	Очное, онлайн
14	Срок обучения	1,5 года
15	Объем кредитов	90 кредитов
16	Языки обучения	Казахский, русский,
17	Присуждаемая академическая степень	магистр технических наук
18	Разработчик(и) и авторы:	Айтхожаева Е.Ж., Сатыбалдиева Р.Ж.,

4.2. Взаимосвязь достижимости формируемых результатов обучения по образовательной программе и учебных дисциплин

№	Наименование дисциплины	Краткое описание дисциплины	Кол-во кредитов	Формируемые результаты обучения (коды)							
				ON1	ON2	ON3	ON4	ON5	ON6	ON7	ON8
1	Иностранный язык (профессиональный)	Курс рассчитан на магистрантов технических специальностей для совершенствования и развития иноязычных коммуникативных умений в профессиональной и академической сфере. Курс знакомит обучаемых с общими принципами профессионального и академического межкультурного устного и письменного общения с использованием современных педагогических технологий (круглый стол, дебаты, дискуссии, анализ профессионально-ориентированных кейсов, проектирование). Курс завершается итоговым экзаменом. Магистрантам также необходимо заниматься самостоятельно (MIS).	2								v
2	Менеджмент	Цель дисциплины - формирование научного представления об управлении как виде профессиональной деятельности; освоение обучающимися общетеоретических положений управления социально-экономическими системами; овладение умениями и навыками практического решения управленческих проблем; изучение мирового опыта менеджмента, а также особенностей казахстанского менеджмента, обучение решению практических вопросов, связанных с	2						v		v

		управлением различными сторонами деятельности организаций.									
3	Психология управления	Курс направлен на овладение инструментами эффективного управления сотрудниками, опираясь на знания психологических механизмов деятельности руководителя. Дисциплина поможет овладеть навыками принятия решений, создания благоприятного психологического климата, мотивирования сотрудников, постановки цели, создания команды и коммуникации с сотрудниками. По окончанию курса магистранты научаться решать управленческие конфликты, создавать собственный имидж, анализировать ситуации в сфере управленческой деятельности, а также проводить переговоры, быть стрессоустойчивыми и эффективными лидерами.	2						v		v
Цикл базовых дисциплин Компонент по выбору											
4	Алгоритмы криптографической защиты информации	Современные проблемы криптографии и информационной безопасности. Официальная ссылка на криптосистему. Классические криптосистемы. Основные задачи криптоанализа. Потоковое шифрование. Криптосистемы с открытым ключом. Использование математического моделирования в криптографии. Преимущества и недостатки разных систем. Теоремы Эйлера и Ферма. Управление ключами. Система, в которой нет клавишного переключателя. Задачи	5	v			v				

		классификации по простым множителям. Проблемы с дискретным логарифмом. Проблемы с криптографией. Системы информационной безопасности, схемы электронной подписи, протоколы аутентификации и аутентификации.									
5	Безопасность систем виртуализации и облачных технологий	Целью освоения дисциплины является изучение вопросов безопасности облачных технологий, источники угроз в облачных вычислениях. Курс нацелен на изучение модели развертывания облаков: публичные, частные, гибридные облака, модели облачных технологий, особенности и характеристики облачных вычислений, стандарты информационной безопасности в сфере облачных технологий и систем виртуализации, средства обеспечения защиты облачных вычислений, шифрование, VPN-сети, аутентификация, изоляция пользователей.	5					v	v		
6	Криптографические методы и средства защиты информации	Магистратура. Современная криптография и задачи, связанные с проблемами защиты информации. Формальное определение криптосистемы. Классические криптосистемы. Основные задачи криптоанализа. Поточное шифрование. Криптосистемы с открытым ключом. Применения математического моделирования в криптографии. Достоинства и недостатки различных систем. Теоремы Эйлера и Ферма. Управление ключами, Система без передачи ключа. Проблема разложения на простые множители. Проблема дискретного	5	v			v				

		логарифмирования. Проблема криптостойкости. Системы защиты информации, схемы электронной подписи, протоколы аутентификации и идентификации.									
7	Phyton для решения задач ИБ	Курс нацелен на изучение вопросов решения высокоуровневых математических и технических задач с использованием пакетов NumPy и SciPy, анализа данных с помощью пакета Pandas. Спообствует развитию навыков работы с данными, связанными с информационной безопасностью: загрузка, фильтрация, преобразование, анализ и интерпретация данных с использованием известных моделей классификации, кластеризации, регрессии и пр. Изучаются основные методы работы с матрицами и матричными операциями. Изучаются инструменты визуализации данных	5				**v**			**v**	
Цикл профилирующих дисциплин Вузовский компонент											
8	Организация защиты и безопасности БД	Аспекты и критерии безопасности, политика безопасности. Угрозы безопасности данных. Защита и безопасность баз данных, целостность и надежность данных. Методы и средства защиты и защиты данных. Разработайте безопасную базу данных. CASE-инструменты дизайна. Инструменты администрирования базы данных. Впечатления как инструменты повышения безопасности данных. Влияние курсоров на безопасность базы данных. Управление транзакциями. Хранимые процедуры.	5	**v**						**v**	

		Триггеры. Мандатное и дискреционное управление доступом к СУБД. Роль и отчеты. Мониторинг и аудит СУБД. Криптографические инструменты для защиты базы данных. Репликация и восстановление данных. Инструменты высокой подготовки.									
9	Организация систем информационной безопасности	Концепция систем информационной безопасности. Стандарты систем информационной безопасности. Выберите объект для организации системы. Анализ угроз и разработка программного обеспечения для безопасности. Административный и процедурный уровни информационной безопасности. Анализ и выбор методов защиты информации. Обеспечение и оценка объектов	5	v		v					v
10	Управление IT проектами и информационными рисками	Целью освоения дисциплины является формирование знаний, умений и навыков в сфере управления рисками IT проектов, теоретическое и практическое овладение современными средствами анализа и оценки рисков, изучение требований к разработке документации по выявлению и оценке рисков, ознакомление с принципами и методами обработки рисков для совершенствования бизнес-процессов и IT инфраструктуры предприятия.	5			v			v		v
Цикл профилирующих дисциплин Компонент по выбору											
11	Анализ данных и извлечение данных	Эта дисциплина направлена на изучение методов поиска информации и интеллектуального анализа данных. Речь идет о том, как найти соответствующую	5	v						v	

		информацию, и впоследствии, извлечь из нее осмысленные шаблоны. В то время, как основные теории и математические модели поиска информации и интеллектуального анализа данных охвачены, дисциплина в первую очередь ориентирована на практические алгоритмы индексирования текстового документа, рейтинга релевантности, использования веб-ресурсов, текстовой аналитики, а также оценки их производительности. Также будут охвачены практические поисковые и интеллектуальные приложения, такие как веб-поисковые системы, системы персонализации и рекомендаций, бизнес-аналитика и обнаружение мошенничества.									
12	Аудит информационной безопасности	Аудит информационной безопасности Управление информационной безопасностью. Аудит информационной безопасности. Базовые термины, определения, понятия и принципы в сфере аудита информационной безопасности. Основные направления аудита информационной безопасности. Виды и цели аудита. Основные этапы аудита безопасности. Перечень исходных данных, необходимых для проведения аудита безопасности. Оценка текущего состояния системы информационной безопасности. Оценка уровня безопасности. Анализ рисков, оценка уровня защищенности, разработка политик безопасности и других организационно-распорядительных документов по защите информации.	5		**v**		**v**	**v**			

		Международные стандарты и лучшие практики проведения ИТ-аудита.									
13	Инженерно-техническая защита информации	Инженерная информация (ИТ) Информация. Проведение необходимых действий по защите информации с использованием активных и пассивных технических средств. Технические средства защиты информации, их классификация. Физические средства защиты объектов. Подходящие инструменты для поиска и поиска информационных потоков. Методы потоковой передачи аудиоинформации. Технические средства для получения и распространения информации. Несанкционированное звуковое информационное устройство. Наушники для телефона. Электронный стетоскоп. Оптико-электронный перехват звуковых сигналов с помощью лазерного зондирования оконных стекол. Технический канал утечки информации путем «высокочастотного наложения». Параметрические технические каналы утечки информации.	5	v	v						
14	Интеллектуализированные средства распознавания и противодействия кибератакам	Модели, цели, средства кибератаки. Активная защита - это метод предотвращения кибербезопасности. Эффективное противодействие. Компоненты активной защиты. Предотвращение сетей. Анализ аномалий, преимущества активной защиты.	5					v	v		
15	Киберпреступность и компьютерная криминалистика	Курс нацелен на исследование цифровых доказательств, методов поиска, получения и закрепления таких доказательств, а также анализ и расследование событий, в которых	5		v		v		v		

		фигурируют компьютерная информация либо компьютер как орудие совершения преступления или имеются иные цифровые доказательства. В курсе изучаются типовые модели киберпреступников и их поведение, основные виды кибератак, а также методы реагирования, расследования и документирования киберинцидентов.									
16	Риск менеджмент в кибербезопасности	Риск менеджмент в кибербезопасности Программа учебного курса «Риск менеджмент в кибербезопасности» направлена на изучение международных и национальных стандартов риск менеджмента в кибербезопасности, методов определения и управления рисками, практического применения стандартов и методов, изучения специализированных программных комплексов для оценки рисков.	5				v				v
17	Стеганографические методы защиты информации	Содержание дисциплины охватывает круг вопросов, связанных с защитой информации путем математических преобразований с помощью стеганографических алгоритмов и алгоритмов защиты авторских прав.	5	v			v	v			
18	Технологии защиты беспроводных сетей	Технология безопасности беспроводных сетей и мобильных приложений. Унифицированные решения. Классификация приложений для мобильных устройств. Методы сканирования и тестирования мобильных приложений. Комплексная система обеспечения безопасности беспроводных сетей. Анализ защищенности мобильных приложений. Угрозы и риски	5			v		v	v		

		безопасности беспроводных сетей и мобильных приложений. Протоколы безопасности беспроводных сетей. Механизм шифрования WEP. Пассивные и активные сетевые атаки. Аутентификация в беспроводных сетях и мобильных приложениях. Технологии целостности и конфиденциальности передаваемых данных. Развертывание беспроводных виртуальных сетей. Туннелирование. Протокол IPSec. Системы обнаружения вторжения в беспроводных сетях и мобильных приложениях, их характеристики.									
19	Big Data и анализ данных	Цель изучения курса - формирование у студентов профессиональной компетенции в области разработки и использования систем обработки и анализа больших массивов данных. Содержание дисциплины рассматривает методы анализа и хранения больших объемов данных, этапы жизненного цикла обработки больших данных, языки, наиболее приспособленные для обработки и аналитики больших данных, способы организации хранения и доступа к большим данным.	5	**v**						**v**	
20	Machine Learning & Deep Learning	Курс посвящен моделям глубокого обучения. Являясь областью в рамках машинного обучения, модели глубокого обучения иллюстрируют количественно-качественный переход. Новые модели и их свойства требуют отдельного изучения и практики настройки метапараметров таких моделей. В этом курсе изучаются основы глубокого обучения, нейронные сети,	5	**v**					**v**	**v**	

		сверточные сети, RNN, LSTM, Adam, Dropout, BatchNorm, инициализации Xavier/He.									
21	OLAP и хранилища данных	Целью освоения дисциплины является получение углубленных знаний о системах хранения данных и технологиях интеллектуального анализа и обработки данных. В содержание дисциплины входят вопросы по видам моделей данных, концепции и архитектурам хранилищ данных, реализации процедур и примеры современных корпоративных систем с применением OLAP технологии. По завершении курса магистранты смогут проектировать хранилища данных и применять технологии обработки данных для решения исследовательских задач.	5							v	v
22	Security Internet of things	Целью освоения курса является изучение основных направлений деятельности по обеспечению безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры. В результате освоения дисциплины магистранты научатся использовать принципы системного подхода; способы формирования требований к кибербезопасности систем «Интернета вещей»; основные положения стандартов по функциональной безопасности АСУТП («Индустриального Интернета вещей»); требования нормативно правовых актов и стандартов по разработке моделей угроз информационной безопасности.	5			v	v				

5. Учебный план образовательной программы