



Институт Автоматики и информационных технологий
Кафедра Кибербезопасности, обработки и хранения информации

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
7M06302 «Комплексное обеспечение информационной
безопасности»

Код и классификация области образования: **7M06 «Информационно-коммуникационные технологии»**

Код и классификация направлений подготовки: **7M063 Информационная безопасность»**

Группа образовательных программ: **M095 «Информационная безопасность»**

Уровень по НРК: **7**

Уровень по ОРК: **7**

Срок обучения: **1,5 года**

Объем кредитов: **90**

Алматы 2023

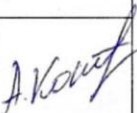
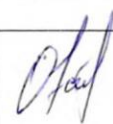
Образовательная программа 7М06302 «Комплексное обеспечение информационной безопасности» утверждена на заседании Учёного совета КазННТУ им. К.И.Сатпаева.

Протокол № 3 от «27» октября 2022 г.

Рассмотрена и рекомендована к утверждению на заседании Учебно-методического совета КазННТУ им. К.И.Сатпаева.

Протокол № 2 от «21» октября 2022 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:				
Сатыбалдиева Рысхан Жакановна	Кандидат технических наук	Заведующий кафедрой «Кибербезопасность, обработка и хранение информации», ассоциированный профессор	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», внутренний телефон: 70-60	
Айтхожаева Евгения Жамалхановна	Кандидат технических наук, доцент	Ассоциированный профессор	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», внутренний телефон: 73-61	
Казиев Галим Зулхарнаевич	Доктор технических наук	Профессор	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», внутренний телефон: 73-61	
Шукаев Дулат Нурмашевич	Доктор технических наук	Профессор	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», внутренний телефон: 73-61	
Жумагалиев Биржан Изимович	Кандидат технических наук, доцент	Ассоциированный профессор	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», внутренний телефон: 73-61	
Работодатели:				
Конуспаев Амирет Туякович	Кандидат физико-математических наук	Президент	Ассоциация инновационных компаний специальной экономической зоны «Парк инновационных технологий»	
Мамырбаев Оркен Жумажанович	Доктор PhD, ассоц. профессор	Заместитель генерального директора	РГП «Институт информационных и вычислительных технологий»	
Обучающиеся:				
Оган Аتكельды		Докторант 1 курса	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», мобильный телефон: +77076665721	

Оглавление

	Список сокращений и обозначений	4
1.	Описание образовательной программы	5
2.	Цель и задачи образовательной программы	6
3.	Требования к оценке результатов обучения образовательной программы	6
4.	Паспорт образовательной программы	7
4.1.	Общие сведения	7
4.2.	Взаимосвязь достижимости формируемых результатов обучения по образовательной программе и учебных дисциплин	11
5.	Учебный план образовательной программы	20

Список сокращений и обозначений

ОП – образовательная программа
БК – базовые компетенции
ПК – профессиональные компетенции
РО – результаты обучения
МООС – массовые открытые онлайн курсы
НРК – Национальная рамка квалификаций
ОРК – Отраслевая рамка квалификаций
БД – база данных
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
БД – база данных

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 7M06302 «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 разработана 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	Новая
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 IP-протоколов; – 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	PO1: Уметь самостоятельно приобретать, осмысливать, структурировать и использовать в профессиональной

	программы:	деятельности новые знания и умения, развивать свои инновационные способности. Применять на практике знания фундаментальных и прикладных разделов дисциплин, определяющих направленность (профиль) программы магистратуры. РО2: Быть компетентным в вопросах выявления киберпреступлений 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. РО3: 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. РО4: 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. РО5: 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. РО6: Знать организацию IP-сетей, структуру IP-пакетов и IP-протоколов, разновидности и принципы аутентификации. Уметь проводить оценку защищенности сетевых операционных систем. РО7: Уметь организовать систему защиты и безопасности БД. Применять технологии защиты БД и методы проектирования безопасных БД. РО8: Уметь анализировать большие данные, знать методы и средства анализа больших данных. Способность формулировать проблемы, задачи и методы научного исследования.
13	Форма обучения	Очная, онлайн
14	Срок обучения	1,5 года
15	Объем кредитов	90
16	Языки обучения	Казахский, русский
17	Присуждаемая академическая степень	Магистр техники и технологий
18	Разработчик(и) авторы:	и Сатыбалдиева Р.Ж., Айтхожаева Е.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)							
				PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
Цикл базовых дисциплин											
Вузовский компонент											
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 управлением различными сторонами деятельности организаций.	2			v					
3	Психология управления (МООС)	Курс направлен на овладение инструментами эффективного управления сотрудниками, опираясь на знания психологических механизмов деятельности	2			v					

		руководителя. Дисциплина поможет овладеть навыками принятия решений, создания благоприятного психологического климата, мотивирования сотрудников, постановки цели, создания команды и коммуникации с сотрудниками. По окончании курса магистранты научатся решать управленческие конфликты, создавать собственный имидж, анализировать ситуации в сфере управленческой деятельности, а также проводить переговоры, быть стрессоустойчивыми и эффективными лидерами.									
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. Поток 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 классификации по простым множителям. Проблемы с дискретным логарифмом. Проблемы с криптографией. Системы информационной безопасности, схемы электронной подписи, протоколы аутентификации и аутентификации.	4	v				v			
5	Безопасность систем виртуализации и облачных технологий (Coursera)	В процессе изучения курса будут рассмотрены вопросы безопасности облачных технологий, источники угроз в облачных вычислениях. Будут изучены модели развертывания облаков: публичные, частные, гибридные облака; модели облачных технологий; особенности и характеристики облачных	5						v	v	

		вычислений; стандарты информационной безопасности в сфере облачных технологий и систем виртуализации; средства обеспечения защиты облачных вычислений; шифрование; VPN-сети; аутентификация; изоляция пользователей.									
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 логарифмирования. Проблема криптостойкости. Системы защиты информации, схемы электронной подписи, протоколы аутентификации и идентификации.	4	v			v				
7	Python в научно-исследовательской деятельности	Курс изучает общие принципы работы с данными: загрузка, получение и обработка неструктурированных данных, получение данных через API, Визуализация и публикация данных, фильтрация, преобразование, анализ и интерпретация данных с использованием известных моделей классификации, кластеризации, регрессии и пр. Круг задач охватывает методы оптимизации, стохастическое моделирование, Гауссово моделирование, уравнения в частных производных, уравнение Навье-Стокса, уравнения теплопроводности.	5					v	v		
Цикл профилирующих дисциплин Вузовский компонент											
8	Организация систем	Концепция систем информационной безопасности.	5	v		v					v

	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									
9	Производственная практика I	Производственная практика направлена на укрепление знаний и развитие практического опыта в сфере информационной безопасности. Задачи практики включают в себя участие магистрантов в организации защиты компьютерной информации, сетевых технологии, организации вычислительных систем и сетей. Практика направлена на возможность самостоятельно проводить производственные, лабораторные и интерпретационные работы при решении практических задач.	5	v	v		v				
10	Производственная практика II	Производственная практика направлена на укрепление знаний и развитие практического опыта в сфере информационной безопасности. Практика направлена на возможность использовать современные методы обработки и интерпретации комплексной информации для решения производственных задач.	4	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 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	5	v						v	v

		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. Международные стандарты и лучшие практики проведения ИТ-аудита.	5		v		v				
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	5		v	v					

		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.									
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	Информационная безопасность экономических систем	Экономическая информация как объект безопасности и товар. Экономическая активность в Интернете. Виды угроз безопасности в экономических информационных системах. Политика безопасности. Основные способы несанкционированного доступа к информации. Средства защиты и методы, используемые в экономических системах, их классификация. Инструменты защиты оборудования. Инструменты обнаружения утечки информации. Межсетевые экраны. Системы обнаружения атак. DLP-система. Вредоносные программы. Системы восстановления данных и резервного копирования. Криптографические системы. Защита баз данных. Безопасность данных и облачные технологии.	5				v			v	v
16	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 фигурируют компьютерная информация либо компьютер как орудие совершения преступления или имеются иные цифровые доказательства. В курсе изучаются типовые модели киберпреступников и их поведение, основные	5		v		v		v		

		виды кибератак, а также методы реагирования, расследования и документирования киберинцидентов.									
17	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. 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.	5	v						v	
18	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
19	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				
20	Технологии защиты беспроводных сетей	Магистратура. Технология безопасности беспроводных сетей и мобильных приложений. Унифицированные решения. Классификация	5					v	v		

		приложений для мобильных устройств. Методы сканирования и тестирования мобильных приложений. Комплексная система обеспечения безопасности беспроводных сетей. Анализ защищенности мобильных приложений. Угрозы и риски 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.									
21	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	v
22	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 метопараметров таких моделей. В этом курсе изучаются основы глубокого обучения, нейронные сети, сверточные сети, RNN, LSTM, Adam, Dropout, BatchNorm, инициализации Xavier/He.	5	v							v
23	OLAP и хранилища	Целью освоения дисциплины является получение	5							v	v

	данных (Coursera)	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.									
24	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						
Экспериментально-исследовательская работа магистранта											
25	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	Систематизация теоретических знаний, наработка навыков по постановке задач по теме исследования и последовательному их решению. Исследовательская работа включает оценку объектов исследования, описывая его проблематику, выделение узкой области для исследовательской работы, проведение эксперимента, анализ результатов экспериментальной части, оформление и защита отчета по ЭИР и подведение итогов.	18	v	v	v	v				

5. Учебный план образовательной программы

НАО "КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени
К.И.САТБАЕВА"



УЧЕБНЫЙ ПЛАН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ для набора на 2023-2024 уч. год

Образовательная программа 7М06302 «Комплексное обеспечение информационной безопасности»
Группа образовательных программ М095 «Информационная безопасность»

Форма обучения: очная Срок обучения: 1,5 года Академическая степень: магистр техники и технологий

Код дисциплины	Наименование дисциплин	Цикл	Общий объём в кредитах	Всего часов	Аудиторный объём лек/лаб/пр	СРО (в том числе СРОП) в часах	Форма контроля	Распределение аудиторных занятий по курсам и семестрам		
								I курс		II курс
								1 семестр	2 семестр	3 семестр
ЦИКЛ БАЗОВЫХ ДИСЦИПЛИН (БД)										
М-1. Модуль базовой профессиональной подготовки (вузовский и компонент по выбору)										
LNG212	Иностранный язык (профессиональный)	БД, ВК	2	60	0/0/2	30	Э	2		
MNG726	Менеджмент	БД, ВК	2	60	1/0/1	30	Э	2		
HUM211	Психология управления	БД, ВК	2	60	1/0/1	30	Э	2		
CSE778	Алгоритмы криптографической защиты информации	БД, КВ	4	120	2/0/1	75	Э	4		
CSE779	Криптографические методы и средства защиты информации				2/0/1					
SEC244	Безопасность систем виртуализации и облачных технологий	БД, КВ	5	150	2/0/1	105	Э	5		
CSE738	Python в научно-исследовательской деятельности				1/0/2					
ЦИКЛ ПРОФИЛИРУЮЩИХ ДИСЦИПЛИН (ПД)										
М-2. Модуль профессиональной подготовки (вузовский и компонент по выбору)										
SEC215	Организация систем информационной безопасности	ПД, ВК	5	150	1/1/1	105	Э	5		
SEC246	Big Data и анализ данных	ПД, КВ	5	150	2/1/0	105	Э	5		
CSE746	Machine Learning & Deep Learning				2/0/1					
SEC248	Security Internet of things	ПД, КВ	5	150	1/0/2	105	Э	5		
SEC222	Технологии защиты беспроводных сетей				1/0/2					
SEC214	Организация защиты и безопасности БД	ПД, КВ	5	150	2/0/1	105	Э		5	
SEC209	Информационная безопасность экономических систем				2/0/1					
SEC204	Аудит информационной безопасности	ПД, КВ	5	150	2/0/1	105	Э		5	
SEC245	Риск менеджмент в кибербезопасности				2/0/1					
SEC234	OLAP и хранилища данных	ПД, КВ	5	150	1/1/1	105	Э		5	
CSE258	Анализ данных и извлечение данных				1/1/1					
CSE718	Инженерно-техническая защита информации	ПД, КВ	5	150	1/0/2	105	Э		5	

SEC238	Стеганографические методы защиты информации				1/0/2					
SEC240	Киберпреступность и компьютерная криминалистика	ПД, КВ	5	150	2/0/1	105	Э		5	
SEC247	Интеллектуализированные средства распознавания и противодействия кибератакам				2/0/1					
М-3. Практико-ориентированный модуль										
CSE782	Производственная практика I	ПД, ВК	5						5	
CSE783	Производственная практика II	ПД, ВК	4							4
М-4. Экспериментально-исследовательский модуль										
AAP249	Экспериментально-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерского проекта	ЭИРМ	18							18
М-5. Модуль итоговой аттестации										
ECA213	Оформление и защита магистерского проекта	ОиЗМП	8							8
Итого по УНИВЕРСИТЕТУ:								30	30	30
								60	30	

Количество кредитов за весь период обучения				
Код цикла	Циклы дисциплин	Кредиты		
		вузовский компонент (ВК)	компонент по выбору (КВ)	Всего
БД	Цикл базовых дисциплин	6	9	15
ПД	Цикл профилирующих дисциплин	14	35	49
	Всего по теоретическому обучению:	20	44	64
ЭИРМ	Экспериментально-исследовательская работа магистранта	18		18
ОиЗМП	Оформление и защита магистерского проекта	8		8
	ИТОГО:	46	44	90

Решение Учёного совета КазННТУ им. К.Сатпаева. Протокол № 3 от "27" октября 2022 г.

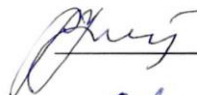
Решение Учебно-методического совета КазННТУ им. К.Сатпаева. Протокол № 2 от "21" октября 2022 г.

Решение Ученого совета института автоматизации и информационных технологий
Протокол № 2 от "21" сентября 2022 г.

Член Правления - Проректор по академическим вопросам

 Б.Б. Жаутиков

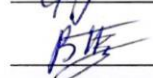
Директор института автоматизации и информационных технологий

 Р.К. Ускенбаева

Заведующий кафедрой "Кибербезопасности, обработки и хранения информации"

 Р.Ж. Сатыбалдиева

Представитель Совета от работодателей

 В.В. Покусов