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

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
7М06301 «Комплексное обеспечение информационной безопасности»

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: **2 года**
Объем кредитов: **120**

Алматы 2023

Образовательная программа 7М06301 «Комплексное обеспечение информационной безопасности» утверждена на заседании Учёного совета КазНИТУ им. К.И.Сатпаева.
Протокол №3 от «27» октября 2022 г.

Рассмотрена и рекомендована к утверждению на заседании Учебно-методического совета КазНИТУ им. К.И.Сатпаева.
Протокол №2 от «21» октября 2022 г.

Образовательная программа 7М06301 «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 Аткельды		Докторант 1 курса	НАО «Казахский национальный исследовательский технический университет имени К.И.Сатпаева», мобильный телефон: +77076665721	

Оглавление

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
ИКТ – информационно-коммуникационные технологии
ИБ – информационная безопасность
ОС – операционная система
БД – база данных
ИТ – информационные технологии

1. Описание образовательной программы

Образовательная программа 7М06301 «Комплексное обеспечение информационной безопасности» направлена на обучение магистрантов научно-педагогического направления. Программа включает базовые и профильные дисциплины с достижением соответствующих компетенций, а также прохождение различных видов практик (научно-исследовательская, педагогическая и стажировки).

Профессиональная деятельность магистров направлена в область защиты и безопасности информации, а именно на комплексное обеспечение информационной безопасности и инженерно-техническую защиту информации.

Подготовка магистров научно-педагогического направления по информационной безопасности будет осуществляться по обновленной образовательной программе 7М06301 «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 научной деятельности магистранта.

В случае успешного завершения полного курса обучающемуся присваивается степень магистр технических наук по образовательной программе 7М06301 «Комплексное обеспечение информационной безопасности».

Выпускник может выполнять следующие виды трудовой деятельности:

- проектно-конструкторская;
- производственно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая;
- эксплуатационная;
- научно-исследовательская.

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: Обеспечить подготовку специалистов научной деятельности и производства 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 информационной безопасности;
- 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 7М06301 «Комплексное обеспечение информационной безопасности» ориентирован на самостоятельное определение цели профессиональной деятельности и выбора адекватных методов и средств их достижения, осуществление научной, 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.

Программа призвана реализовать принципы демократического характера управления образованием, расширить границы академической свободы и полномочий учебных заведений, что обеспечит подготовку квалифицированных, высоко мотивированных кадров для инновационных и наукоемких отраслей экономики.

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.

В разработке образовательной программы участвовали представители казахстанских компаний и ассоциаций, специалисты ведомственных структур в области защиты и безопасности.

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	7М06301 «Комплексное обеспечение информационной безопасности»
5	Краткое описание образовательной программы	Профессиональная деятельность выпускников включает в себя: науку, образование, государственные и ведомственные структуры, экономику и промышленность государства, область здравоохранения. Объектами профессиональной деятельности выпускников магистерских программ по

		образовательной программе - «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; − высшие учебные заведения и научные учреждения; − отделы и департаменты информационной безопасности государственных организаций и коммерческих структур. Основными функциями профессиональной деятельности магистрантов являются: проведение научно-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	Обеспечить подготовку специалистов научной деятельности и производства 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:	Требования к ключевым компетенциям выпускников научно-педагогической магистратуры, должен: 1) иметь представление: – о роли науки и образования в общественной жизни; – о современных тенденциях в развитии научного познания; – об актуальных методологических и философских проблемах естественных (социальных, гуманитарных, экономических) наук; – о профессиональной компетентности

		преподавателя высшей школы; – 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: – методологию научного познания; – принципы и структуру организации научной деятельности; – психологию познавательной деятельности студентов в процессе обучения; – 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: – использовать полученные знания для оригинального развития и применения идей в контексте научных исследований; – 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; – применять знания педагогики и психологии высшей школы в своей педагогической деятельности; – применять интерактивные методы обучения; – 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 научные исследования и осуществлять преподавание специальных дисциплин в вузах; – обобщать результаты научно-исследовательской и аналитической работы в виде диссертации, научной 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: – научно-исследовательской деятельности, решения стандартных научных задач; – осуществления образовательной и педагогической деятельности по кредитной технологии обучения; – методики преподавания профессиональных дисциплин; – использования современных информационных технологий в образовательном процессе; – профессионального общения и межкультурной коммуникации; – ораторского искусства, правильного и логичного оформления своих мыслей в устной и письменной форме; – 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 и продолжения образования в докторантуре. 5) быть компетентным: – в области методологии научных исследований; – в области научной и научно-педагогической деятельности в высших учебных заведениях; – в вопросах современных образовательных технологий; – в выполнении научных проектов и исследований в профессиональной области; – 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: Обладать способностью самостоятельно формулировать цели исследований, устанавливать последовательность решения профессиональных задач. РО2: Обладать профессиональными компетенциями для создания и исследования модели изучаемых объектов на основе использования углубленных теоретических и практических знаний в области защиты и безопасности информации. РО3: Умение к проектированию комплексных научно-исследовательских и научно-производственных работ при решении профессиональных задач. Владение иностранными языками на профессиональном уровне. РО4: Применение нормативных документов при планировании и организации научно-производственных работ в области информационной безопасности. Анализировать современные и перспективные направления развития криптографической защиты информации и применять их на практике. РО5: Понимать философские вопросы науки, основные исторические этапы развития науки, уметь критически оценивать и анализировать научно-философские проблемы, понимать специфику инженерной науки, владеть навыками аналитического мышления. Быть компетентным в вопросах психологии и педагогики. РО6: Уметь организовать систему защиты и безопасности БД и применять технологии защиты БД,

		знать современные и перспективные направления развития криптографической защиты информации и применять ее на практике. РО7: Уметь проводить оценку защищенности сетевых операционных систем. Безопасно применять современные технологии виртуализации. Знать и применять методы и средства для проведения аудита информационной безопасности. РО8: Быть компетентным в вопросах выявления киберпреступлении и компьютерной криминалистики. Уметь использовать средства распознавания и противодействия кибератакам. РО9: Знать технические средства и методы технической защиты информации, быть компетентным в организации инженерно-технической защиты информации. РО10: 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	2 года
15	Объем кредитов	120
16	Языки обучения	Казахский, русский
17	Присуждаемая академическая степень	Магистр технических наук
18	Разработчик(и) и авторы:	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)									
				РО1	РО2	РО3	РО4	РО5	РО6	РО7	РО8	РО9	РО10
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 обучающихся 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).	5			V							
2	История и философия науки (МООС)	Предмет философии науки, динамика науки, специфика науки, наука и преднаука, античность и становление теоретической науки, основные этапы исторического развития науки, особенности классической науки, неклассическая и постнеклассическая наука, философия математики, физики, техники и технологий, специфика инженерных наук, этика науки, социально-нравственная ответственность ученого и инженера.	3					V					
3	Педагогика высшей школы (МООС)	В рамках курса магистранты освоят методологические и теоретические основы педагогики высшей школы, научатся использовать современные педагогические	3					V					

		технологии, планировать и организовывать процессы обучения и воспитания, овладеют коммуникативными технологиями субъект-субъектного взаимодействия преподавателя и магистранта в образовательном процессе вуза. Также магистранты изучат управление человеческими ресурсами в образовательных организациях (на примере высшей школы).											
4	Психология управления (МООС)	Дисциплина изучает современную роль и содержание психологических аспектов в управленческой деятельности. Рассматривается улучшение психологической грамотности обучающегося в процессе реализации профессиональной деятельности. Самосовершенствуется в области психологии и изучает состав и устройство управленческой деятельности, как на местном уровне, так и в зарубежном. Рассматривается психологическая особенность современных управленцев.	3					v					
5	Педагогическая практика	Нацелена на формирование практических навыков и методики преподавания. Педагогическая практика может проводиться в период теоретического обучения без отрыва от учебного процесса. При этом магистранты могут привлекаться к проведению занятий в бакалавриате.	6	v	v								
Цикл базовых дисциплин Компонент по выбору													
6	Алгоритмы криптографической защиты информации	Современные проблемы криптографии и информационной безопасности. Официальная ссылка на криптосистему. Классические криптосистемы. Основные задачи криптоанализа. Потоковое	5	v			v		v				

		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.											
7	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 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				v			
8	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.	5				v		v			v	

		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.											
9	Методы и средства защиты в ОС	В курсе изучаются защита от изменения и контроль целостности программного обеспечения. Методы и средства хранения ключевой информации. Принципы многофакторной аутентификации. Технические устройства идентификации и аутентификации. Программно-аппаратные средства шифрования. Обеспечение безопасности в системах Windows, Unix, ознакомление с внутренней организацией носителей информации. Системы обнаружения вторжений. Основные компоненты архитектуры межсетевых экранов. Современные требования к межсетевым экранам.	5				v					v	
10	Средства безопасности сетевых ОС	Основы сетевой безопасности. Интегрированный мониторинг программного обеспечения и защита от повреждения программного обеспечения. Принципы многолучевой аутентификации. Идентификация и аутентификация технических устройств. Подсистемы безопасной идентификации и	5		v					v			

		аутентификации. Идентификация и аутентификация пользователей с использованием биометрических устройств. Программное и аппаратное шифрование. Безопасность сетевых операционных систем. Безопасность в Windows, Unix. Системы для обнаружения грязи. Основные компоненты архитектуры брандмауэра. Современные требования к брандмауэрам.										
11	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													
12	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	5	v					v				v

		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.											
13	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						
14	Исследовательская практика	Исследовательская практика магистранта проводится с целью ознакомления с новейшими теоретическими, методологическими и технологическими достижениями отечественной и зарубежной науки, современными методами научных исследований, обработки и интерпретации экспериментальных данных.	8		v	v							
Цикл профилирующих дисциплин Компонент по выбору													
15	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.											
16	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			

		Международные стандарты и лучшие практики проведения ИТ-аудита.											
17	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	v	
18	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				v		
19	Искусственный интеллект	Целью исскуственного интеллекта является создание технических систем, способных решать задачи невычислительного характера и выполнять действия, требующие переработки содержательной информации и считающиеся прерогативой человеческого	5		v								v

		мозга.											
20	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 виды кибератак, а также методы реагирования, расследования и документирования киберинцидентов.	5								v		
21	Обработка естественного языка	Курс изучает теоретические и практические основы обработки естественного языка. В курсе рассматриваются теоретические аспекты NLP, включая базовые сведения из области лингвистики, и практические методы обработки текстов. Рассматриваются классические алгоритмы обработки текстовой информации, такие как регулярные выражения, измерение расстояний, подстановок, поиск строк и подстрок. Лингвистические деревья. Корпус текста. Таксономия. Рассматриваются модели Word2Vec, Text Embeding, LSTM модели нейронных сетей. Изучаются существующие библиотеки анализа текстовой информации.	5		v								v
22	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	5							v		v	

		управления рисками, практического применения стандартов и методов, изучения специализированных программных комплексов для оценки рисков.											
23	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	
24	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 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.	5		v					v	v		
25	Big Data и анализ данных	Цель изучения курса - формирование у студентов профессиональной компетенции в области разработки и использования систем	5			v			v				

		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.											
26	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, сверточные сети, RNN, LSTM, Adam, Dropout, BatchNorm, инициализации Xavier/He.	5			v			v				v
27	OLAP и хранилища данных (Coursera)	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

28	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								
Научно-исследовательская работа магистранта													
29	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	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 НИР и подведение итогов.	24	v	v	v							

5. Учебный план образовательной программы

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

SATBAYEV UNIVERSITY

УТВЕРЖДАЮ
Председатель правления - Ректор
М.М.Бегентаев
«01» 12 2022 г.

УЧЕБНЫЙ ПЛАН
ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ для набора на 2023-2024 уч.год
Образовательная программа 7М06301 "Комплексное обеспечение информационной безопасности"
Группа образовательных программ М095 "Информационная безопасность"

Форма обучения: очная **Срок обучения:** 2 года **Академическая степень:** магистр технических наук

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			
								1 курс		2 курс	
								1 семестр	2 семестр	3 семестр	4 семестр
ЦИКЛ БАЗОВЫХ ДИСЦИПЛИН (БД)											
М-1. Модуль базовой подготовки (вузовский компонент и компонент по выбору)											
LNG210	Иностранный язык (профессиональный)	БД ВК	5	150	0/0/3	105	Э	5			
HUM214	Психология управления	БД ВК	3	90	1/0/1	60	Э	3			
HUM212	История и философия науки	БД ВК	3	90	1/0/1	60	Э		3		
HUM213	Педагогика высшей школы	БД ВК	3	90	1/0/1	60	Э		3		
SEC221	Средства безопасности сетевых ОС	БД КВ	5	150	1/0/2	105	Э	5			
SEC211	Методы и средства защиты в ОС				1/0/2						
CSE738	Phyton для научно-исследовательской деятельности	БД КВ	5	150	1/0/2	105	Э	5			
SEC244	Безопасность систем виртуализации и облачных технологий				2/0/1						
SEC201	Алгоритмы криптографической защиты информации	БД КВ	5	150	2/0/1	105	Э		5		
SEC210	Криптографические методы и средства защиты информации				2/0/1						
ЦИКЛ ПРОФИЛИРУЮЩИХ ДИСЦИПЛИН (ПД)											
М-2. Модуль профильной подготовки (вузовский компонент и компонент по выбору)											
SEC 215	Организация систем информационной безопасности	ПД ВК	5	150	1/1/1	105	Э	5			
SEC 214	Организация защиты и безопасности БД	ПД ВК	5	150	2/0/1	105	Э		5		
CSE777	Искусственный интеллект	ПД КВ	5	150	2/0/1	105	Э		5		
CSE283	Обработка естественного языка				2/0/1						
CSE718	Инженерно-техническая защита информации	ПД КВ	5	150	1/0/2	105	Э		5		
SEC238	Стеганографические методы защиты информации				1/0/2						
SEC246	Big Data и анализ данных	ПД КВ	5	150	2/1/0	105	Э			5	
CSE746	Machine Learning & Deep Learning				2/0/1						
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						
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						
SEC248	Security Internet of things	ПД КВ	5	150	1/0/2	105	Э			5	
SEC222	Технологии защиты беспроводных сетей				1/0/2						
М-3. Практико-ориентированный модуль											
AAP229	Педагогическая практика	БД ВК	6						6		
AAP269	Исследовательская практика	ПД ВК	8								8
М-4. Научно-исследовательский модуль											
AAP251	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	2					2			
AAP241	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	3						3		

AAP254	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	5							5	
AAP255	Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации	НИРМ	14								14
М-5. Модуль итоговой аттестации											
ECA213	Оформление и защита магистерской диссертации	ОиЗМД	8								8
	Итого по УНИВЕРСИТЕТУ:							25	35	30	30
								60		**60**	

Количество кредитов за весь период обучения				
Код цикла	**Циклы дисциплин**	**Кредиты**		
		вузовский компонент (ВК)	**компонент по выбору (КВ)**	**Всего**
БД	Цикл базовых дисциплин	20	15	35
ПД	Цикл профилирующих дисциплин	18	35	53
	Всего по теоретическому обучению:	***38***	***50***	***88***
НИРМ	Научно-исследовательская работа магистранта	24		24
ОиЗМД	Оформление и защита магистерской диссертации	8		8
	ИТОГО:	**70**	**50**	**120**

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

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

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

Член Правления - Проректор по академическим вопросам **Б.Б.Жаутиков**

Директор института автоматики и информационных технологий **Р.К.Ускенбаева**

Заведующий кафедрой "Кибербезопасности, обработки и хранения информации" **Р.Ж.Сатыбалдиева**

Представитель Совета от работодателей **В.В.Покусов**