Х.ДОСМҰХАМЕДОВ АТЫНДАҒЫ АТЫРАУ МЕМЛЕКЕТТІК УНИВЕРСИТЕТІ
АТЫРАУСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Х. ДОСМУХАМЕДОВА

БЕКІТІЛДІ/УТВЕРЖДАЮ
«Х.Досмұхамедов атындағы Атырау мемлекеттік университеті» ШЖҚ РМК Ғылыми Кеңесінің шешімімен / Решением Ученого совета АтГУ им.Х.Досмухамедова
Ректор_____А.Талтенов
20<u>19</u>ж./г.«<u>28</u>»<u>04</u>, №<u>5</u> хаттама/протокола

БІЛІМ БЕРУ БАҒДАРЛАМАСЫ
ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
EDUCATION PROGRAMME

«7М06103 -КИБЕРБЕЗОПАСНОСТЬ»
Білім беру бағдарламасының атауы

«7М06103- КИБЕРҚАУІПСІЗДІК»
Название образовательной программы

«7М06103- CYBERSECURITY»
Name of education programme

Атырау, 2019

Факультет **«Физики, математики и информационных технологий»**

Кафедра **«Программная инженерия»**

Название ОП **«7М06103 -КИБЕРБЕЗОПАСНОСТЬ**

Тип ОП:

- ■ **Действующая**
- ☐ **Новая**
- ☐ **Инновационная**

РАЗРАБОТЧИКИ (Академический комитет):

Фамилия, имя отчество	Должность	Контактные данные	Подпись
Габбасова Жанна Дуйсембаевна	Заведующая кафедрой, канд.техн.наук,проф.	+77014382808	
Ярослав Култан	PhD доктор кафедры «Прикладная информатика» Братиславского Экономического университета (Словакия)	+421904364892	
Нуржауов Рустем	Магистрант	+77759627313	

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1 Цикл программы: Второй цикл: магистратура 7 уровень НРК / ОРК / МСКО

1.2 Присуждаемая степень: магистр в области информационно-коммуникационных технологий по образовательной программе «7М06103- Кибербезопасность»

1.3 Общий объем кредитов: 120 академических кредитов/60 ECTS

1.4 Типичный срок обучения: 2 год

1.5 Отличительные особенности ОП

Уникальность данной образовательной программы – профессиональная подготовка магистра в научной сфере, в сфере технологий и проблем обеспечения кибербезопасности, защиты информационных систем в различных сценариях кибер-угроз.

Магистратура по кибербезопасности предназначена для тех, кто хочет расширить свои технические и навыки программирования для обработки вызовов безопасности предприятия. Образовательная программа обеспечит прочную основу в ключевых технологиях, включая компьютер, и сетевую безопасность, криптографию, анализ архитектуры безопасности предприятия и т.д. Выпускники научатся ориентироваться в быстро меняющихся технологиях, адаптировать и контролировать новые угрозы и начать успешную карьеру в сфере безопасности предприятия.

Информационная безопасность востребована во всех сферах жизни. Программа включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере. Отличительной чертой направления подготовки является то, что специалист вне зависимости от предыдущей сферы деятельности сможет получить и в дальнейшем использовать навыки построения систем передачи данных с точки зрения безопасности, определять сегменты сетей с критически низким уровнем защиты, научится определять классы вредоносных программ с помощью полученных знаний в области кибербезопасности. Компетенции в области традиционных методов и средств обеспечения информационной безопасности входят в курс базовой подготовки.

Данная ОП разработана с учетом обобщения современного отечественного и мирового опыта подготовки по данному направлению, авторских и коллективных научных достижений, и учебно-методических разработок в области IT, требований работодателей и запросов рынка труда.

Общие результаты обучения по программе будут достигнуты посредством следующих учебно-научных мероприятий:

1) аудиторные занятия: лекции, научные семинары, исследовательская практика, практические и лабораторные занятия – проводятся с учетом инновационных технологий обучения, использованием новейших достижений науки, технологий и информационных систем и в интерактивной форме;

2) внеаудиторные занятия: самостоятельная работа обучающегося, в том числе под руководством преподавателя, индивидуальные консультации;

3) выполнение магистерской диссертации и ее публичная защита

2. ЦЕЛЬ И ОБОСНОВАНИЕ ОП

2.1 Цели ОП

Цель образовательной программы - подготовка высококвалифицированных кадров для государственных и коммерческих структур, способных обеспечивать кибербезопасность, защиту информационных систем в различных сценариях кибер-угроз.

Создание условий для овладения общими и специальными профессиональными компетенциями, а также инновационными подходами и исследовательскими навыками в области кибербезопасности, способствует социальной мобильности и устойчивости выпускника на рынке труда.

Образовательная программа формирует и личностные качества магистров: целеустремленность, лидерство, умение работать в команде, осуществлять научные исследования, применять современные методы научно-педагогического направления в сфере информационных технологий, ответственность за конечный результат своей профессиональной деятельности и способность к самосовершенствованию и саморазвитию.

Выпускник будет иметь компетенции: выявления сущности проблем, возникающих в профессиональной деятельности, используя общие законы науки и применяя математический аппарат в области информационных профессиональных задач; понимание сущности и значения информации в современном обществе, в применение информационных технологий, в поиске целевой информации в различных источниках и в глобальных компьютерных системах; использовании правовых рекомендаций в профессиональной области; управлении вспомогательным комплексом мер по обеспечению информационной безопасности, учете юридического обоснования, административной и технологической реализации и экономической эффективности, выявлении возможных угроз; контроле объектов в соответствии с требованиями государства и политики компании; участие и разработке подсистемы контроля, управления и эксплуатации; участие в предварительных анализах технико-экономической целесообразности для обеспечения кибербезопасности; составление технического задания с учетом действующих положений по информационной безопасности; программирование решений общих алгоритмов обеспечения информационной безопасности и применения программного обеспечения системных, прикладных и специальных типов; анализе явлений и процессов при исследовании и принятии проектных решений; анализе информационной безопасности объектов и систем с использованием национальных и зарубежных стандартов; экспериментах с использованием установленной процедуры обработки данных, оценке событий и определение погрешностей; поиске, реферирование и обобщение научно-технической литературы и рекомендаций по проблеме кибербезопасности; разработке технологий для улучшения системы менеджмента информационной безопасности; формировании и развитие комплекса мер (правил, процедур, практических рекомендаций) для управления информационной безопасностью.

2.2 Обоснование ОП для магистрантов

Образование магистра по направлению «7М06103-Кибербезопасность» дает большие перспективы карьерного и профессионального роста. Магистр по кибербезопасности выявляет угрозы информационной безопасности и риски потери данных, вырабатывает и внедряет меры противодействия угрозам и решения для защиты от потери информации; обеспечивает сохранность и конфиденциальность данных; участвует в разработке и внедрении IT-решений.

Мобильные телефоны, компьютеры, машины, а с некоторых пор даже бытовые приборы связывают себя и своего владельца огромным количеством данных. Гигантских

масштабов достигли информационные системы в бизнесе, торговле и финансах, подтверждением чему является текущий криптовалютный бум.

Все это привело к формированию новых ценностей, создаваемых или передаваемых в киберпространстве. Вместе с этим появилась, и угроза кражи этих ценностей, их порчи или подмены. Для противодействия злоумышленникам необходимы специалисты по кибербезопасности, способные защищать информацию, предугадывать действия преступников и создавать безопасную архитектуру пользования данными.

Потребность в таких специалистах особенно наглядно прослеживается сейчас, в связи с ростом числа киберпреступлений и случаев кибертерроризма. Хакерские атаки регистрируются во всех уголках мира. Среди самых резонансных стоит упомянуть распространение вирусов WannaCry, Petya/NotPetya, нанесших значительный урон банковским системам и крупным компаниям разных стран.

Обучающиеся получат способность анализировать фундаментальные и прикладные проблемы кибербезопасности в условиях становления современного информационного общества; способность анализировать угрозы кибербезопасности объектов защиты и разрабатывать организационно-технические мероприятия по обеспечению защиты информации на всех этапах жизненного цикла объектов защиты; способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методик и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок; способность проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента; способность оформлять научно-технические отчеты, обзоры, готовить публикации по результатам выполненных исследований, научные доклады.

Обучение по магистерской программе в качестве основных дисциплин включает:

1. Безопасное кодирование
2. Сетевая и веб-безопасность
3. Безопасность операционных систем
4. Право, этика и конфиденциальность
5. Кибер-атаки и кибер-обороны
6. Правительство и национальная безопасность
7. Экономика кибербезопасности
8. Криптография

Таким образом, цель обучения по данной программе - подготовка профессионалов по кибербезопасности, работающих в крупных финансовых и IT-компаниях, ценность подобных кадров отмечается и в государственных органах, оборонных ведомствах, где их основная задача – обеспечение национальной безопасности, предотвращение внедрения в государственную инфраструктуру.

2.3 Потребность на рынке труда

Кибербезопасность интересна, как спецификой технических средств, применяемых в данной сфере, будь то программные средства или аппаратные, так и тесной взаимосвязанностью с законодательством, как казахстанским, так и международным. На сегодняшний день специалисты по защите информации являются ценными кадрами, а опытные профессионалы, владеющие всеми тонкостями и механизмами данной профессии в остром дефиците.

Основываясь на данных собственного исследования, рекрутинговая компания Antal Kazakhstan составила список из 15 профессий, которые в недалеком будущем станут востребованы на рынке Казахстана, среди них в числе первых - профессия «специалист по кибербезопасности».

Знания и навыки обучающегося по данной программе:

- высокий уровень навыков программирования
- внимательность и аккуратность при работе с кодом, умение находить скрытые и неочевидные источники заражения
- сочетание навыков программирования со знанием физических свойств технических устройств
- аналитические навыки, способность просчитывать последствия тех или иных изменений
- возможность оперативной оценки угроз и их источников
- умение работать с большими массивами данных
- понимание принципов проведения кибератак, знание возможных путей защиты от них

Профессиональные компетенции обучающихся по данной образовательной программе:

- борьба с киберпреступностью во всех ее проявлениях, включая кибертерроризм и вымогательство
- разработка превентивных методов борьбы с вредоносным ПО, защита частной информации и интеллектуальной собственности
- обеспечение стабильности работы общественно важных информационных систем, предотвращение ситуаций коллапса банковской системы
- защита и предотвращение внешнего вмешательства в инфраструктуру, в том числе энергосети
- поиск потенциальных уязвимостей в уже существующих системах, их устранение
- создание системы защиты информации, ее аудите и мониторинге, анализируют информационные риски, разрабатывают и внедряют мероприятия по их предотвращению.

Всем перечисленным требованиям к магистру по кибербезопасности и отвечает данная образовательная программа.

2.4 Область профессиональной деятельности

Магистр технических наук осуществляет свою профессиональную деятельность:

- Сотрудниками научно - исследовательских институтов, центров в области информационных технологий;

- Специалистами в государственных органах, оборонных ведомствах, где их основная задача – обеспечение национальной безопасности

- Лаборантами и специалистами в вузах, научно-исследовательских институтах, организациях различных форм собственности, использующие инфокоммуникационные технологии.

Квалификационный уровень по НРК – 7

2.5 Объекты профессиональной деятельности

Объекты профессиональной деятельности: проектные и научно-исследовательские институты, органы управления, департаменты информационных технологий, финансовые организации, бизнес-структуры, образовательные организации, учебные заведения, промышленное производство, государственные органы и оборонных ведомствах.

2. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ОП

Результаты обучения магистра по специальности: «7М06103- Кибербезопасность» (7-й квалификационный уровень НРК) в соответствии с Дублинскими дескрипторами

второго уровня обучения предполагают владение следующими профессиональными компетенциями (РО):

Аналитическая и профессиональная деятельность:

- способен демонстрировать развивающиеся знания и понимание в изучаемой области, основанные на передовых знаниях этой области, при разработке и (или) применении идей в контексте исследования (РО 1);
- свободно владеет иностранным языком на профессиональном уровне, позволяющем проводить научные исследования и осуществлять преподавание профилирующих дисциплин в вузах (РО 2);
- применяет на профессиональном уровне знания педагогики и психологии управления высшей школы в своей научно-педагогической деятельности (РО 3);
- способен расширять и углублять знания, необходимые для повседневной профессиональной деятельности и продолжения образования в докторантуре (РО 4);
- обеспечение стабильности работы общественно важных информационных систем, предотвращение ситуаций коллапса банковской системы (РО-5);
- защита и предотвращение внешнего вмешательства в инфраструктуру, в IT и энергосети (РО-6);
- разработка превентивных методов борьбы с вредоносным ПО, защита частной информации и интеллектуальной собственности (РО-7);

Научно-исследовательская деятельность:

- проводить научные исследования и поиск новых моделей и методов совершенствования методов защиты информации (РО-9);
- разработка превентивных методов борьбы с вредоносным ПО, защита частной информации и интеллектуальной собственности (РО-10);
- организовывать самостоятельную и коллективную научно-исследовательскую работу (РО-11)
- ориентироваться в области специфики ВУЗа (что нового и полезного создано, как это работает (РО-12)
- сотрудничать с людьми, ведущими научные разработки, уметь понимать их требования и удовлетворять запросы рынка программных продуктов (РО-13)

4. УЧЕБНЫЙ ПЛАН ОП

Модуль коды Код модуля Module code	Модульдің компоненттері (коды және атауы)/ Составляющие модуля (код и название)/ Components of the module (code and name)	Цикл және компонент /Цикл и компонент /Cycle and component	Қорытынды бақылауды жүргізу формасы /Форма проведения итогового контроля/Theform conducting final control	Академиялық кредиттер саны Количество академических кредитов/Number of academic credits	Қалыптастырушы құзіреттілік/ Формируемые компетенции/ Formed competencies	Ескерту/ Примечание/ remark
AGGM 01 Әлеуметтік-гуманитарлық ғылымдар модулі/ MSGN 01 Модуль социально-гуманитарных наук/ SSHM 01 Social sciences and humanities module	GTPh5201 Ғылым тарихы мен философиясы/ IFN 5201 История и философия науки/ HP 5201 History and phylosophy of siense	БП, ЖК БД, ВК BD,ICC	емтихан/ экзамен/ examination	5	КҚ-1 ПК-1 CC-1	Әлеуметтік-гуманитарлық пәндер кафедрасы/ Кафедра социально-гуманитарных дисциплин/ Social and humanities subjects department
	ShT 5202 Шет (кәсіби) тілі / IYa 5202 Иностранный язык (профессиональный/ FL 5202 Foreign language (professional)	БП, ЖК БД, ВК BD,ICC	емтихан/ экзамен/ examination	5	КҚ-2 ПК-2 CC-2	Аударма ісі және шетел тілдері кафедрасы/Кафедра переводческого дела и иностранныхя зыков/ Translation studies and foreign languages department
	ZhMP 5203 Жоғары мектептің педагогикасы/ PVSh 5203 Педагогика высшей школы/ HSP5203 Higher School Pedagogy	БП, ЖК БД, ВК BD,ICC	Ауызша емтихан/ Устный экзамен/ oral examination	5	КҚ-3 ПК-3 CC-3	Педагогика кафедра зертханасы Кафедра-лаборатория «Педагогика» Department-laboratory «Pedagogy»
	PP 5205 Педагогикалық практика / PP 5205 Педагогическая практика/ PP 5205 Pedagogical		Есеп/ Отчет/ report		КҚ-4 ПК-4 CC-4	Педагогика кафедра зертханасы Кафедра-лаборатория

	practice					«Педагогика» Department-laboratory «Pedagogy»
	BP 5204 Басқару психологиясы / PU 5204 Психология управления / MP 5204 Management psychology	БП, ЖК БД, ВК BD,ICC	Презентация/ Презентация/ presentation	5	КҚ-5 ПК-5 СС-5	Психология және арнайы білім беру кафедрасы Кафедра «Психология и специальное образование Department of Psychology and special education
KKEM 02 Құқықтық қамтамасыз ету модулі / MPO 02 Модуль правового обеспечения/ LSM 02 Legal support module	KEK 5206 Құқық, этика және құпиялылық / PEK 5206 Право, этика и конфиденциальность/ LEC 5206 Law, ethics and confidentiality	БД, ТК БД, КВ BD,ES	Емтихан/ Экзамен/ Exam	8	КҚ 6-9 ПК 6-9 СС6-9	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	Kk 5206 Киберқылмыс/ Kp 5206 Киберпреступность Kc 5206 Cybercrime					
GZZhM 06 Ғылыми-зерттеу жұмысының модулі/MNIR 03 Модуль научно-исследовательской работы/ MRW 03 Module of research work	SOMDOKEMGZZh Стажировкадан өту және магистрлік диссертацияны орындауды қоса есептегендегі магистранттың ғылыми-зерттеу жұмысы/ NIRMVPSIVM Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации (НИРМ) / RWMIPIIMD Research work of masters, including passing of internship and implementation of master's degreedissertation		Есеп/ Отчет/ report	2	КҚ 20-22 ПК 20-22 СС 20-22	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
Итого за семестр				**30**		
KM 02 Криптография модулі / MSSU 02 Модуль криптографии/ TCM 02 The cryptographic module	Kg 5207 Криптография / Kg 5207 Криптография/ Cg 5207 Cryptography	БД, ТК БД, КВ BD,ES	Жоба/ Проект/ project	7	КҚ 6-9 ПК 6-9 СС 6-9	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	KK 5207 Қауіпсіз кодтау / BK 5207 Безопасное кодирование / SE 5207 Secure encoding					

	NUZhBK 5301 Нақты уақыт жүйелері үшін бағдарламалық қамтамасыз етуді әзірлеу технологиялары /TRPOSRV 5301 Технологии разработки программного обеспечения для систем реального времени / SDTRTS 5301 Software development technologies for real-time systems	КП, ЖК ПД, ВК PD, ICC	Емтихан/ Экзамен/ Exam	5 (2)	КҚ 6-9 ПК 6-9 CC 6-9	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
KSM 03 Киберқауіпсіздік стандарттарының модулі/ MSK 04 Модуль стандартов кибербезопасности/ CSM 04 Cybersecurity standards module	TZhU 5302 Тәуекелдердің жаңа үрдістері /NTR 5302 Новые тенденции рисков/ NTR 5302 New trends in risk	КП, ТК ПД, КВ PD, ES	Жоба/ Проект/ project	5	КҚ 10-13 ПК 10-13 CC 10-13	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	AKT 5302 Ақпараттық қауіпсіздік және тәуекелдер / IBR 5302 Информационная безопасность и риски / BC BC 5302 Business communications					
	KHS 5303 Киберқауіпсіздіктің халықаралық стандарттары/ MSK 5303 Международные стандарты кибербезопасности /IKS 5303 International cybersecurity standards	КП, ТК ПД, КВ PD, ES	Жоба/ Проект/ project	5	КҚ 10-13 ПК 10-13 CC 10-13	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	KUS 5303 Киберқауіпсіздіктің ұлттық стандарттары / Национальные стандарты кибербезопасности /NCS 5303 National cybersecurity standards					
	KKN 5304 Киберкеңістік және Киберқауіпсіздік негіздері/ KOK 5304 Киберпространство и основы кибербезопасности /CBC 5304 Cyberspace and the basics of cybersecurity	КП, ТК ПД, КВ PD, ES	Емтихан/ Экзамен/ Exam	5	КҚ 10-13 ПК 10-13 CC 10-13	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	UHZK 5304 Ұлттық және халықаралық заңнамадағы киберқауіпсіздік / NIODP 5304 Кибербезопасность в национальном и					

	международном законодательстве / CNIL 5304 Cybersecurity in national and international law					
GZZhM 06 Ғылыми-зерттеу жұмысының модулі/MNIR 03 Модуль научно-исследовательской работы/ MRW 03 Module of research work	SOMDOKEMGZZh Стажировкадан өту және магистрлік диссертацияны орындауды қоса есептегендегі магистранттың ғылыми-зерттеу жұмысы/ NIRMVP Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации (НИРМ)/ RWM Research work of masters, including passing of internship and implementation of master's degreedissertation		Есеп/ Отчет/ report	3	ҚҚ 20-22 ПК 20-22 CC 20-22	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
Итого за семестр				**30**		
3 семестр						
КМ 04 Киберқауіпсіздік модулі / МК 05 Модуль кибербезопасности/ CSM 05 Cyber security module	ККАК 6305 Қашықтан кіру арқылы киберқауіпсіздік / KUD 6305 Кибернападения из удаленного доступа / CAfRA 6305 Cyber attacks from remote access	КП, ТК ПД, КВ PD, ES	Жоба/ Проект/ project	5	ҚҚ 14-15 ПК 14-15 CC 14-15	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	BZhKKZh 6305 Болған жағдайда киберқауіпсіздік кол жеткізу/ KNLD 6305 Кибернападения при наличии локального доступа/ CAPLA 6305 Cyber attacks in the presence of local access's					
	HP 6306 Хаттамалар мен платформалар/ PP 6305 Протоколы и платформы/ PP 6306 Protocols and platforms	КП, ТК ПД, КВ PD, ES	Емтихан/ Экзамен/ Exam	5	ҚҚ 14-15 ПК 14-15 CC 14-15	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	UKKM 6306 Ұлттық контексте киберқауіпсіздік менеджменті / MKNK 6306 Менеджмент кибербезопасности в					

	национальном контексте / CMNC 6306 Cybersecurity management in the national context					
ZhKAM 05 Желілік қауіпсіздік архитектурасы модулі / MASB 06 Модуль архитектуры сетевой безопасности / NSAM 06 Network security architecture module	ZhKAKKPB 6307 Желілік қауіпсіздік архитектурасы және қауіпсіздікті қамтамасыз ету процесін басқару/ ASBiUPOB 6307 Архитектура сетевой безопасности и управление процессом обеспечения безопасности/NSASM 6307 Network security architecture and security management	КП, ТК ПД, КВ PD, ES	Емтихан/ Экзамен/ Exam	5	КҚ 16-19 ПК 16-19 CC 16-19	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	ZhK 6307 Желілік қауіпсіздік/ SB 6307 Сетевая безопасность / NS 6307 Network security					
	OZhK 6308 Операциялық жүйелердің қауіпсіздігі / BOS 6308 Безопасность операционных систем /OSS 6308 Operating system security	КП, ТК ПД, КВ PD, ES	Жоба/ Проект/ project	8	КҚ 16-19 ПК 16-19 CC 16-19	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	WK 6308 Web-қауіпсіздік/WB 6308 Web-безопасность)/ WS 6308 Web- security					
GZZhM 06 Ғылыми-зерттеу жұмысының модулі/ MNIR 03 Модуль научно-исследовательской работы/ MRW 03 Module of research work	SOMDOKEMGZZh Стажировкадан өту және магистрлік диссертацияны орындауды қоса есептегендегі магистранттың ғылыми-зерттеу жұмысы/ NIRMVPSIVM Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации (НИРМ) / RWMIPIIMD Research work of masters, including passing of internship and implementation of master's degreedissertation		Есеп/ Отчет/ report	7	КҚ 20-22 ПК 20-22 CC 20-22	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
Итого за семестр				30		
4 семестр						

GZZhM 06 Ғылыми-зерттеу жұмысының модулі/MNIR 03 Модуль научно-исследовательской работы/ MRW 03 Module of research work	SOMDOKEMGZZh Стажировкадан өту және магистрлік диссертацияны орындауды қоса есептегендегі магистранттың ғылыми-зерттеу жұмысы/ NIRMVPSIVM Научно-исследовательская работа магистранта, включая прохождение стажировки и выполнение магистерской диссертации (НИРМ) / RWMIPIIMD Research work of masters, including passing of internship and implementation of master's degreedissertation		Есеп/ Отчет/ report	12	КҚ 20-22 ПК 20-22 CC 20-22	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
	ZP 6309 Зерттеу практикасы / IP 6309 Исследовательская практика/Research practice	КП, ЖК ПД, ВК PD, ICC	Есеп/ Отчет/ report	6	КҚ 20-22 ПК 20-22 CC 20-22	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
ҚАМ 07 Қорытынды аттестаттау модулі/ MIA Модуль итоговой аттестации/ TMFA The module final assessment	Магистрлік диссертацияны тіркеу және қорғау /Оформление и защита магистерской диссертации (ОиЗМД)/ Registration and defense of a master's thesis	ҚА ИА FA	Қорғау/ Защита/ Defense	12	КҚ 23-25 ПК 23-25 CC 23-25	Бағдарламалық инженерия кафедрасы/ Кафедра программной инженерии/ Software engineering department
Итого за семестр				**30**		
Итого:				**120**		

6. МАТРИЦА КОРРЕЛЯЦИИ

результатов обучения по образовательной программе в целом с формируемыми компетенциями (результатами обучения составляющих компонентов)

	РО1	РО2	РО3	РО4	РО5	РО6	РО7	РО8	РО9	РО10	РО11	РО12
ПК-1	+											
ПК-2	+	+										
ПК-3	+		+									
ПК-4	+			+								
ПК-5	+				+							
ПК-6	+	+		+								
ПК-7	+						+		+			
ПК-8	+						+		+			
ПК-9	+	+							+	+		
ПК-10	+			+	+				+	+		
ПК-11	+				+					+		
ПК-12					+		+	+				
ПК-13			+		+		+	+				+
ПК-14			+		+				+			+
ПК-15			+						+			+
ПК-16			+	+		+						+
ПК-17	+										+	+
ПК-18	+							+			+	+
ПК-19	+							=			+	
ПК-20	+					+						
ПК-21	+					+						+
ПК-22	+				+							+
ПК-23					+							
ПК-24			+	+	+	+	+	+			+	+
ПК-25	+	+	+	+	+	+	+	+	+	+	+	+

7. СВОДНАЯ ТАБЛИЦА

Семестр	БД ВК	БД КВ	ПД ВК	ПД КВ	НИРМ	ИА	Всего	Продолжительность (в т.ч. сессия, но без каникул)
1	20	8			2		30	
2		7	5	15	3		30	
3				23	7		30	
4		5	6 пр		12	12	30	
Итого	20	15	11	38	24	12	120	

8. ЛИСТ АДМИНИСТРИРОВАНИЯ ОП

ЭКСПЕРТЫ:

Фамилия, имя отчество	Должность	Подпись и дата
Кушумбаев Арсен Сайранович	Главный менеджер Департамента развития Информационных технологий АО KTZ Express	

Образовательная программа **рассмотрена и рекомендована к утверждению** на заседаниях:

Учебно-методического совета кафедры Программной инженерии

протокол № 2 "25" 12 2019 г.

Заведующая кафедрой _____ Габбасова Ж.Д.

Учебно-методического совета факультета математики, физики и ИТ

протокол № 3 "23" 01 2019 г.

Председатель УМС факультета _____ Кенжегулов Б.З

Учебно-методического совета университета

протокол № 4 "25" 01 2019 г.

Председатель УМС университета _____ Джарасова Г.С.