АТЫРАУСКИЙ УНИВЕРСИТЕТ ИМ. Х. ДОСМУХАМЕДОВА
КАФЕДРА «ПРОГРАММНАЯ ИНЖЕНЕРИЯ»

Утверждено на заседании факультета
«Физики, математики и информационных технологий»
Декан факультета _____ Б.У. Асанова
протокол № 6 от «22» 02 2022г.

КАТАЛОГ ЭЛЕКТИВНЫХ ДИСЦИПЛИН

«7М06103 –КИБЕРБЕЗОПАСНОСТЬ»

(наименование образовательной программы)

на 2022 - 2023 учебные годы

Атырау, 2022

№	Код и наименование дисциплины	Цель курса Краткое содержание основных разделов (2-3 предложения)	Пререквизиты	Формируемы компетенции (не более 30 слов)	Цикл дисциплины		Объем академ. кредитов	Рекомендуемый семестр
					(ООД, БД, ПД)	ВК, КВ		
			2 курс					
1	KUD 6305 Кибернападения из удаленного доступа	С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального дисциплины должен: **иметь практический опыт:** - настройки сервера и рабочих станций для безопасной передачи информации; - установки web-сервера, организации доступа к локальным и глобальным сетям, сопровождения и контроля использования почтового сервера, SQL сервера; - расчёта стоимости лицензионного программного обеспечения сетевой инфраструктуры; - сбора данных для анализа использования и функционирования программно – технических средств компьютерных сетей;	Криптография,Технологии разработки программного обеспечения, Новые тенденции рисков, Международные стандарты кибербезопасности, Киберпространство и основы кибербезопасности	В результате изучения обучающийся будет: иметь основное представление о сценариях нападения со стороны сервера (использование слабых конфигураций, имитация ИП (IP), обеспечение отказа/ дистрибутивного отказа в обслуживании (DoS и DDoS), внедрение SQL и переполнение сетевого буфера на основе протоколов; уметь определить и обсудить отношения между нападениями со стороны клиента и методами действий на основе обмана, «фишинг» (phishing) и нападения на предприятие; иметь представление о сценариях, выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу, подделка межсайтовых запросов, использование веб-браузеров в своих целях и документы, содержащие вредоносные вирусы.	ПД	КВ	5	3
2	KNLD 6305 Кибернападения при наличии локального доступа	В результате изучения магистранты смогут понять системный подход в процессе планирования с целью устойчивости в отношении угроз, атак и аналогичных происшествий; создавать практические условия для задействования устойчивых систем в рамках национального контекста; анализировать универсальность рамок и матриц для планирования и делегирования полномочий. Изучение национальных методов работы, принципы действия и организации по киберустойчивости; ознакомление с национальными структурами кибербезопасности; аудит и оценка	Киберпреступность, Технологии разработки программного обеспечения,	В результате обучающиеся смогут демонстрировать знания о существовании угроз организации, которые могут исходить от ее сотрудников; описать нападения на основе локального доступа и выявлять составные части такого нападения; объяснить разницу между нападением на основе удаленного и локального доступов; продемонстрировать понимание различия между понятиями «разрешение» и «привилегия» и как они используются для контроля доступа пользователей к информационным ресурсам системы; указать, как структурировать информацию на основе здравой политики				

		безопасности на национальном уровне		зонирования сетевой безопасности.				
3	PP 6305 Протоколы и платформы	Цель изучения дисциплины «Протоколы и платформы» состоит в повышении профессиональной компетентности слушателей, приобретении знаний теории и методологии создания, использования и развитие информационных систем предприятий, организаций и ведомств Республики Казахстан. Основной задачей дисциплины является ознакомление с методологией выбора аппаратно-программной платформы, соответствующей потребностям прикладной области. В процессе обучения слушателей используются следующие методы (технологии) обучения: -технологии проблемно -модульного обучения; -проектные технологии; -технологии анализа проблемных ситуаций; -технологии дистанционного обучения. Средствами обучения слушателей являются: -электронный конспект лекций; -презентационные материалы; -раздаточные материалы по темам.	Криптография,Технологии разработки программного обеспечения Новые тенденции рисков, Международные стандарты кибербезопасности, Киберпространство и основы кибербезопасности	В результате освоения Дисциплины «Протоколы и платформы» слушатель должен знать: -состав и назначение основных компонентов корпоративной информационной системы; -ключевые понятия и основные положения организации современных микропроцессорных архитектур; -иметь представление о современных компьютерных архитектурах и путях их развития; -назначение и функции, -Выполняемые операционными системами; -основные возможности современных операционных систем, их достоинства и недостатки; -методологию применения аппаратных и программных платформ при построении и развитии информационных систем; -принципы построения компьютерных сетей; -назначение и функции сете зависимой и сете не зависимой подсистем корпоративной сети; -методологию создания информационных служб соответствующих потребностям конкретной прикладной области; уметь характеризовать: -требования предъявляемые к корпоративным ИС необходимые для достижения целей деятельности организаций; -влияние отдельных компонент ИС на ее производительность и масштабируемость; -основные цели и задачи обеспечения эффективного использования ИС в целях управления предприятием; -приоритетные направления обеспечения жизнедеятельности ИС предприятия; уметь анализировать: -методы объединения отдельных сетей предприятий в единую корпоративную сеть;	ПД	КВ	5	3

				-роль базовых информационных служб корпоративных сетей; -текущее состояние ИС с целью выявления узких мест и определения путей развития информационной системы; -реальные и потенциальные угрозы снижения эффективного функционирования ИС; приобрести навыки: -определения влияния отдельных характеристик программно-аппаратных платформ на производительность и надежность функционирования информационных служб; -использования знаний об архитектурах отдельных компонентов аппаратно- программных платформ для решения задач выбора конкретных программных и аппаратных средств при создании либо модернизации информационных систем; -практического управления корпоративными информационными системами.				
4	MKNK 6306 Менеджмент кибербезопасности в национальном контексте	В результате изучения магистранты смогут понять системный подход в процессе планирования с целью устойчивости в отношении угроз, атак и аналогичных происшествий; создавать практические условия для задействования устойчивых систем в рамках национального контекста; анализировать универсальность рамок и матриц для планирования и делегирования полномочий. Изучение национальных методов работы, принципы действия и организации по киберустойчивости; ознакомление с национальными структурами кибербезопасности; аудит и оценка безопасности на национальном уровне.	Киберпреступность, Технологии разработки программного обеспечения,	В результате изучения данной дисциплины магистранты должны иметь представление: - о предпосылках и факторах формирования национальной безопасности; - об основных направлениях внешнеполитической деятельности, направленной на укрепление суверенитета страны. Знать: - теоретико-методологические аспекты национальной безопасности; - национальные интересы как основу национальной безопасности; - геополитические аспекты национальной безопасности; - механизм обеспечения устойчивости социальной системы и политику безопасности; - угрозы национальной безопасности Республики Казахстан в условиях глобализации; - концепцию национальной безопасности				

				Республики Казахстан; - внутриполитическую безопасность, социально-экономическую, информационную, духовно-нравственную, военную безопасность Республики Казахстан. Уметь: - анализировать сущность и формы национальной безопасности; - применять навыки анализа современных систем обеспечения национальной безопасности.				
5	ASBiUPOB 6307 Архитектура сетевой безопасности и управление процессом обеспечения безопасности	Задачи изучения: готовить (на базовом уровне, с подготовкой схем сетей) необходимое зонирование сети и размещение межсетевых экранов; учитывать и понимать общенациональные стандарты и руководящие указания для проведения оценок угроз и рисков, подготовки концепций сетевой безопасности для предприятий и организаций, а также для создания архитектуры элементов безопасности сетей; знать комбинацию уровней безопасности в эшелонированной обороне сети предприятия, его защищенность в случае отказа одного из механизмов безопасности или использования злоумышленниками уязвимого места в системе.	Криптография,Технологии разработки программного обеспечения, Новые тенденции рисков, Международные стандарты кибербезопасности, Киберпространство и основы кибербезопасности	В результате освоения Дисциплины «Архитектура сетевой безопасности и управление процессом обеспечения безопасности» слушатель должен Знать: –методологические и технологические основы обеспечения информационной безопасности сетевых автоматизированных систем; –угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем; типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения; –принципы функционирования основных защищенных сетевых протоколов; –правила определения политики сетевой безопасности; –стандарты по оценке защищенных сетевых систем и их теоретические основы; методы и средства проектирования, реализации и оценки защищенных сетевых систем. Уметь: –разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы; –применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации; –реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем. Владеть:	ПД	КВ	5	3

				–методами анализа сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности; –навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях; –способами и правилами применения сетевых протоколов для защиты информации в сетях.				
6	SB 6307 Сетевая безопасность	Изучение безопасности Сетевых систем, для которых характерны сетевые, или удаленные угрозы. В рамках дисциплины рассматриваются защиты подключений к внешним сетям; защиты корпоративных потоков данных, передаваемых по открытым сетям; защиты потоков данных между клиентами и серверами; обеспечение безопасности распределенной программной среды; защиты важнейших сервисов (web-сервиса); аутентификация в открытых сетях.	Киберпреступность, Безопасное кодирование, Технологии разработки программного обеспечения для систем реального времен, Информационная безопасность и риски, Национальные стандарты кибербезопасности, Кибербезопасность в национальном и международном законодательстве	В результате освоения дисциплины магистрант должен: *знать*: -основные понятия информационной безопасности; -основные направления защиты информации; -законодательство Республики Казахстан в области защиты информации; -современные методы и средства защиты информации в информационно-телекоммуникационных системах; -архитектуру защищённых экономических систем. *Уметь*: -разрабатывать политику информационной безопасности; -проводить оценку угроз безопасности объекта информатизации; -реализовывать простые информационные технологии реализующие методы защиты информации; -применять методики оценки уязвимости в информационно-телекоммуникационных сетях; -проектировать системы защиты информации. *Владеть*: -методами защиты информации; -средствами защиты информации в сетях ЭВМ; -навыками программирования алгоритмов криптографической защиты информации.				
7	BOS 6308 Безопасность операционных систем	Освоение магистрантами архитектуры сетевой безопасности и управление процессом обеспечения безопасности операционных систем. Овладение умением	Киберпреступность, Безопасное кодирование,	В результате освоения дисциплины магистрант должен: ***Знать:*** - требования к защищенным ОС;	ПД	КВ	8	3

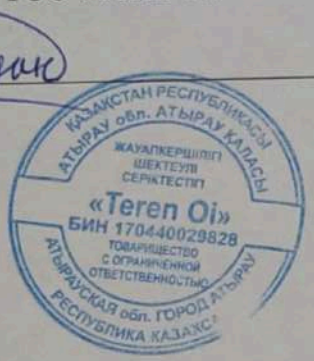
		применять методы для создания архектуры предприятия (Enterprise Architecture), позволяющей сформировать набор принципов, подходов и технологий, подходы к созданию архитектур — TOGAF, Zachman Framework, FEAF, DoDAF.	Технологии разработки программного обеспечения для систем реального времен, Информационная безопасность и риски, Национальные стандарты кибербезопасности, Кибербезопасность в национальном и международном законодательстве	- критерии оценки эффективности и надежности средств защиты ОС; - принципы организации и структуру подсистем защиты ОС семейств Unix и Windows; -критерии и методы оценивания механизмов защиты. ***Уметь:*** оценивать эффективность и надежность защиты ОС; выявлять слабости защиты ОС и использовать их для вскрытия защиты; - планировать политику безопасности ОС; - пользоваться средствами защиты, предоставляемыми ОС; - проводить анализ и оценивание механизмов защиты. ***Владеть:*** навыками построения защиты ОС Windows, Unix.				
8	WB 6308 Web-безопасность	Целями освоения дисциплины являются «Web-безопасность» направлен на достижение следующих целей и подготовку профессиональных специалистов и их деятельность связанную с разработкой, эксплуатацией и обслуживанием серверов, серверного программного обеспечения и интернет-сайтов размещенных в сети Интернет. Для решения цели поставлены следующие задачи: овладение основами Интернет-технологий; изучение принципов установки, настройки и эксплуатации ПО серверных систем размещенных в сети Интернет; разработка безопасных приложений для интернет-сайтов и оценка безопасности готовых программных решений для построения интернет-сайтов способы защиты от взлома и обеспечение	Киберпреступность, Безопасное кодирование, Технологии разработки программного обеспечения для систем реального времен, Информационная безопасность и риски, Национальные стандарты кибербезопасности, Кибербезопасность в национальном	В результате освоения дисциплины магистрант должен: Знать: -о структуре, устройстве и функционировании сети Интернет; -об архитектуре и работе серверных операционных систем; -о работе веб-сайтов в сети Интернет. Уметь: -программировать на языке Си, Си++, Java Scipt; -знать язык гипертекстовой разметки HTML; -знать устройство, архитектуру, принципы работы семейства операционных систем на базе ОС Linux. Владеть: -свободного использования компьютерной техники и сети Интернет; -программирования на нескольких языках, основой которых является языки Си и Java;				

		безопасности работающих интернет-сайтов и серверов размещенных в сети Интернет.	и международном законодательстве	-обеспечения безопасности компьютерной техники и серверных операционных систем; -использования операционной системы Ubuntu 12.1 Linux.				

Согласовано:

Директор ТОО «Teren Oi»

_____ А.Алдан



Согласовано:

Руководитель офиса обеспечения и повышения академического качества и развития образовательных программ _____ Сулейменова Ж.У.

Заведующий кафедрой _____ Байтемирова Н.Б.