Аннотация к рабочей программе
дисциплины «Cybersecurity (Кибербезопасность)»

Учебный курс «Cybersecurity (Кибербезопасность)» предназначен для студентов направления подготовки 38.04.02 Менеджмент, магистерская программа «International Business and Project Management / Международный бизнес и управление проектами (на английском языке)».

Дисциплина «Cybersecurity (Кибербезопасность)» включена в состав дисциплин по выбору вариативной части блока «Дисциплины (модули).

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (36 часов, в том числе МАО 18 часов), самостоятельная работа (54 часа). Дисциплина реализуется на 2 курсе в 3 семестре.

Дисциплина «Cybersecurity (Кибербезопасность)» основывается на знаниях, умениях и навыках, полученных в результате изучения дисциплин «Управление проектами», «Теория организации и организационное поведение», «Управленческая экономика» и позволяет подготовить студентов к освоению ряда таких дисциплин, как «Маркетинговое управление», «Менеджмент качества при создании инновационных продуктов» и «Strategic Management (Стратегический менеджмент)».

Содержание дисциплины состоит из трех разделов и охватывает следующий круг вопросов:

1. Введение в проблему кибербезопасности: информационная безопасность кибернетических систем; обеспечение безопасности автоматизированных систем управления технологическими процессами;
2. Особенности защиты кибернетических систем: основные угрозы, уязвимости, риски в области безопасности Интернета вещей, Требования к системам защиты информации при интеграции с системами реального времени и методы экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.

3. Технологии угроз сетевой безопасности: Основы правового регулирования защиты информации критически важных объектов и современные методы управления корпоративными финансами для решения стратегических задач, механизмы противодействия сетевым атакам.

Цель – формирование у студентов системного представления о кибербезопасности, практических методах и инструментах обеспечения информационной безопасности, необходимых для эффективной работы в современном бизнес-пространстве.

Задачи:

- изучение понятийного аппарата дисциплины, основных теоретических положений и методов;
- формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач;
- формирование знаний теоретических основ в сфере обеспечения безопасности цифровой информации; этапы обеспечения информационной безопасности кибернетических систем, в том числе обеспечение безопасности автоматизированных систем управления технологическими процессами; технологии угроз сетевой безопасности, а также механизмы противодействия сетевым атакам;
- формирование у студентов профессиональных умений и навыков в области использования современных техник и международных стандартов в области оценивания текущих ситуаций и прогнозов будущих рисков, связанных с угрозами кибербезопасности; технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам.

Для успешного изучения дисциплины «Кибербезопасность» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность к логическому мышлению, анализу, систематизации, обобщению, критическому осмыслению информации;
- способность осуществлять сбор, анализ, систематизацию, оценку и

интерпретацию данных, необходимых для решения профессиональных задач.

- способность к самосовершенствованию и саморазвитию в профессиональной сфере, к повышению общекультурного уровня;
- готовность интегрироваться в научное, образовательное, экономическое, политическое и культурное пространство России и АТР;
- способность проявлять инициативу и принимать ответственные решения, осознавая ответственность за результаты своей профессиональной деятельности;
- способность использовать современные методы и технологии (в том числе информационные) в профессиональной деятельности;
- способность к самоорганизации и самообразованию.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-3 – способность использовать современные методы управления корпоративными финансами для решения стратегических задач;	знает	сущность решений защиты информации кибернетических систем; основы оценивания влияния средств защиты информации на критически важные экономические объекты информатизации.
	умеет	находить решения стандартных задач профессиональной деятельности на основе методов оптимизации систем защиты информации и управления корпоративными финансами для решения стратегических задач.
	владеет	способность формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.
ПК-9 владением методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде	знает	сущность методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде.
	умеет	формировать требования для системы защиты информации, для систем реального времени с учетом особенностей функционирования экономического объекта защиты и рынков в глобальной среде.

	владеет	способность оценивать влияние средств защиты информации на критически важные экономические объекты информатизации.

Для формирования вышеуказанных компетенций в рамках дисциплины «Cybersecurity (Кибербезопасность)» применяются следующие методы активного/ интерактивного обучения: лекция-презентация, лекция-дискуссия, кейс-стади.