МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

ГОУ ВПО Кыргызско-Российский Славянский университет

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информатики**

Учебный план Направление 41.03.05 Международные отношения

Квалификация **бакалавр**

Форма обучения **очная**

Программу составил(и): к.т.н., доцент Евтушенко А.И.; ст.преподаватель, Фейгин Я.Д.

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	18	18	18	18
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная	36	36	36	36
Сам. работа	36	38	36	38
Итого	72	74	72	74

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Основной целью дисциплины является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России и Кыргызстана по данному вопросу.
1.2	Изучение дисциплины «Информационная безопасность» направлено на решение следующих задач:
1.3	¯ получения студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
1.4	¯ формирование навыковбезопасной работы в различных сетевых структурах, в т.ч. и социальных сетях

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационно-аналитическая работа

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОК-5: владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией; способностью работать с информацией в глобальных компьютерных сетях	
Знать:	
Уровень 1	основы информационно-коммуникационных технологий, приемы безопасной работы в локальных и глобальных сетях
Уровень 2	программные и аппаратные средства получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	концепции современной информационной безопасности; методы и технологии (парольные, криптографические, стеганографические) защиты компьютерной информации
Уметь:	
Уровень 1	применять на практике информационно-коммуникационные технологии для безопасной работы в локальных и глобальных сетях
Уровень 2	использовать современные программные и аппаратные средства получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	использовать парольные, криптографические, стеганографические технологии защиты компьютерной информации при ее хранении и передаче
Владеть:	
Уровень 1	приемами безопасной работы в локальных и глобальных сетях
Уровень 2	навыками использования современных программных и аппаратные средств получения, хранения и переработки информации с учетом всех требований информационной безопасности
Уровень 3	навыками использования парольных, криптографических, стеганографических технологий защиты компьютерной информации при ее хранении и передаче

ОПК-8: способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	
Знать:	
Уровень 1	основные понятия и определения, используемые при изучении информационной безопасности; классификацию угроз информационной безопасности; как организовать информационную безопасность на предприятии
Уровень 2	криптографические и стеганографические методы защиты информации при передаче
Уровень 3	классификацию "компьютерных вирусов", какую угрозу они представляют для безопасности информации и правила защиты от "компьютерных вирусов"; методы социальной инженерии и способы и приемы безопасной работы в сети
Уметь:	
Уровень 1	подключить организацию к Internet с соблюдением требований информационной безопасности
Уровень 2	применять криптографические средства защиты от несанкционированного доступа при передаче данных через Интернет, квалифицированно использовать парольные средства защиты при хранении данных на компьютере
Уровень 3	правильно выбрать и использовать антивирусную программу

Владеть:	
Уровень 1	методами организации безопасной работы в локальнных АИС на предприятии
Уровень 2	парольными и криптографическими средствами защиты от несанкционированного доступа прихранении данных и при передаче через Интернет
Уровень 3	антивирусными средствами защиты компьютера

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	иметь представление:
3.1.2	о концепциях современной информационной безопасности;
3.1.3	о месте, роли и тенденциях развития методов и технологий защиты компьютерной информации;
3.1.4	об особенностях и проблемах защиты информации в будущей профессиональной деятельности;
3.1.5	знать:
3.1.6	фундаментальные понятия информационной безопасности;
3.1.7	основные принципы и правила хранения, передачи и защиты компьютерной правовой информации;
3.1.8	состав, функции и конкретные возможности аппаратно-программного обеспечения в процессе решения задач профессионально-служебной деятельности;
3.1.9	основные нормативные документы, законы и указы, регламентирующие организацию защиты информации.
3.2	**Уметь:**
3.2.1	•использовать современные аппаратно-программные средства в области защиты информации
3.2.2	•грамотно управлять системой защиты информации при работе на персональном компьютере
3.2.3	•выявлять и классифицировать источники внешних и внутренних угроз
3.2.4	•защищать информационные ресурсы от вредоносного программного обеспечения.
3.3	**Владеть:**
3.3.1	•использования основных защитных механизмов, мер и средств обеспечения информационной безопасности
3.3.2	•комплексного подхода к построению системы защиты информации
3.3.3	•использования криптографических методов защиты информации
3.3.4	.использования парольных и биометрических методов защиты информации