

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ  
ИМЕНИ Г.В. ПЛЕХАНОВА» В Г. ТАШКЕНТЕ**

**ФАКУЛЬТЕТ ЭКОНОМИКИ, БИЗНЕСА И ФИНАНСОВ**

**КАФЕДРА «ГУМАНИТАРНЫЕ И МАТЕМАТИЧЕСКИЕ ДИСЦИПЛИНЫ»**

**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ  
Б1.В.ДВ.4.3 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

**Направление подготовки:** 38.03.01 - «ЭКОНОМИКА»

**Профиль подготовки:**  
Финансы и кредит

**Квалификация выпускника:** Бакалавр (академический)

**ТАШКЕНТ – 2015**

## **Цель дисциплины**

Цель преподавания дисциплины «Основы информационной безопасности» - овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты информации, генерируемой в процессе функционирования предприятий различных форм собственности и сфер бизнеса.

## **Учебные задачи дисциплины**

- ознакомить студентов с тенденциями развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации;
- способствовать получению теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- способствовать формированию системных представлений об управлении информационными рисками; изучению методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- способствовать освоению и систематизации знаний об уровнях информационной безопасности (личности, общества, государства), угрозах на каждом уровне; мерах обеспечения состояния информационной безопасности (законодательного, административного, процедурного, программно-технического).

## **Требования к результатам освоения содержания дисциплины**

В результате освоения дисциплины студент должен овладеть основными методами обеспечения информационной безопасности, правильно оценивать тенденции развития и результаты исследований, выбирать практические рекомендации по формам и методам применения различных технологий в обеспечении безопасности экономической информации.

В ФГОС по направлению 38.03.01 «Экономика» предусмотрен ряд компетенций, являющихся базой для оценки профессиональных знаний, формируемых в процессе изучения дисциплины «Основы информационной безопасности».

Обучающийся должен владеть следующими компетенциями, формирующиеся в процессе изучения дисциплины, определяются практическими навыками расчетно-экономической, аналитической и научно-исследовательской деятельности:

**ОК-6** - способностью использовать основы правовых знаний в различных сферах деятельности

**ОПК-1** - способностью решать стандартные задачи профессиональной

деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности

**ОПК-2** - способностью осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач

**ПК-7** - способностью, используя отечественные и зарубежные источники информации, собирать необходимые данные, анализировать их и готовить информационный обзор и/или аналитический отчет

**ПК-8** - способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии.

**ПК-10** способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии

В результате освоения компетенции **ОК-6** студент должен:

**Знать** основы правовых знаний в сфере информационной безопасности;

**Уметь** применять действующую законодательную базу в области информационной безопасности;

**Владеть** навыками использования нормативно-правовых документов в сфере информационной безопасности.

В результате освоения компетенции **ОПК-1** студент должен:

**Знать** содержание основных понятий обеспечения информационной безопасности, источники угроз безопасности информации;

**Уметь** применять методы оценки уязвимости информации;

**Владеть** способами создания, организации и обеспечения функционирования систем комплексной защиты информации.

В результате освоения компетенции **ОПК-2** студент должен:

**Знать** технологии сбора, анализа и обработки данных, необходимых для решения задач информационной безопасности.

**Уметь** проводить самостоятельные исследования в соответствии с разработанной программой; представлять результаты проведенного исследования в виде статьи или доклада.

**Владеть** навыками разработки проектов положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

В результате освоения компетенции **ПК-7** студент должен:

**Знать** сущности и основные принципы обеспечения информационной безопасности, виды и признаки компьютерных преступлений.

**Уметь** применять методы управления и оценки состояния информационной безопасности на предприятии.

**Владеть** основной терминологией и поиска в Интернет ресурсов, относящихся к вопросам информационной безопасности.

В результате освоения компетенции **ПК-8** студент должен:

**Знать** методы разработки и обоснования критериев эффективности информационных систем с учетом обеспечения безопасности использования информации.

**Уметь** оценить предлагаемые варианты управленческих решений по вопросам информационной безопасности.

**Владеть** возможностями оперативных решений в управлении операционной деятельности организаций.

В результате освоения компетенции **ПК-10** студент должен:

**Знать** источники информации, методы сбора необходимых данных, подготовки информационного обзора и/или аналитического отчета.

**Уметь** работать с информацией в информационных системах, анализировать данные и подготовить аналитические отчеты.

**Владеть** методами решения коммуникативных задач обеспечения информационной безопасности современными техническими средствами и информационными технологиями.

### 3. Тематический план изучения дисциплины

№ п/п	Наименование тем	Аудиторные часы			Самостоятельная работа (формы, часы)	Интерактивные формы обучения		Формы текущего контроля
		Лекции	Практические занятия	Всего				
<b>V семестр</b>								
Раздел 1. Теоретические аспекты информационной безопасности								
1.	Основные понятия	4	4	8	10			Лит
2.	Информационные угрозы	4	4	8	16	2	2	П.з.
3.	Государственное регулирование информационной безопасности	4	4	8	16		2	Р.а.з.
Раздел 2. Принципы построения системы информационной безопасности								
4.	Политика информационной безопасности	4	6	10	12	2	2	Лит
5.	Подходы, принципы, методы и средства обеспечения безопасности.	4	6	10	16		2	П.з.
6.	Криптографические методы защиты информации	4	6	10	16		2	Р.а.з.
7.	Защита информации в Интернете.	4	6	10	16	2	2	
<b>Итого:</b>		28	36	64	102	<b>18</b>		

<b>Промежуточная аттестация</b>						<b>зачет</b>
<b>Всего по дисциплине</b>	<b>28</b>	<b>36</b>	<b>64</b>	<b>102</b>	<b>12%</b>	

### **Формы контроля**

Контроль за освоением дисциплины осуществляется в каждом дисциплинарном разделе отдельно.

*Рубежный контроль:* тестирования по отдельным разделам дисциплины.

*Промежуточная аттестация в 5 семестре* - зачет в письменной и устной форме.

Результаты текущего контроля и промежуточной аттестации формируют рейтинговую оценку работы студента. Распределение баллов при формировании рейтинговой оценки работы студента осуществляется в соответствии с «Положением о рейтинговой системе оценки успеваемости и качества знаний студентов в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Российский экономический университет имени Г.В. Плеханова».

**Зав. кафедрой «ГиМД»,**

**к.ф.-м. н. Шамсуддинов Б.Р.**

**Разработчик: ст. преп. Ташбаев У.В.**