

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.09 Информационная безопасность

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация выпускника: экономист

Форма обучения: заочная

1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» является усвоение теоретических знаний и практического опыта по участию в построении комплексной системы защиты информации на предприятии и обеспечения режима конфиденциальности информации в условиях использования информационно-телекоммуникационных сетей.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Информационная безопасность» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Дисциплина	Раздел
Микроэкономика	1
Экономическая безопасность	2

Таблица 2.2 – Требования к постреквизитам дисциплины

Дисциплина	Раздел
Итоговая аттестация	ГАК

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Этап 1: требования к системам информационной инфраструктуры предприятия и критически важным информационным системам. Этап 2: расширенную структуру информационного законодательства по обеспечению информационной безопасности;	Этап 1: строить модель угроз и нарушителя; Этап 2: рассчитывать вероятность реализации угроз.	Этап 1: общего порядка организации защиты информации на предприятии. Этап 2: методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.
ПСК-1 - способностью осуществлять предупреждение правонарушений, выявлять и устранять причины и условия,	Этап 1: методы оценки защищенности информационной системы предприятия; Этап 2: методы	Этап 1: формировать комплекс мероприятий по снижению информационных рисков;	Этап 1: общего порядка организации защиты информации на предприятии. Этап 2: методами и навыками решения задач, связанных с

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
способствующие их совершению	поддержки принятия решения по обоснованию мер защиты информации на предприятии.	Этап 2: анализировать уровень защищенности ИС предприятия;	организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.
ПК-27 -способностью анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение;	Этап 1: методы анализа результатов контроля, методы исследований причин и последствий выявленных отклонений, нарушений и недостатков; Этап 2: методики подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.	Этап 1: анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков; Этап 2: готовить предложения, направленные на устранение выявленных отклонений, нарушений и недостатков.	Этап 1: анализа результатов контроля, исследования и обобщения причин и последствий выявленных отклонений, нарушений и недостатков; Этап 2: подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.

4. Объем дисциплины

Объем дисциплины «Информационная безопасность» составляет 3 зачетных единиц (108 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

**Таблица 4.1 – Распределение объема дисциплины
по видам учебных занятий и по периодам обучения, академические часы**

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 9	
				КР	СР
1	Лекции (Л)	4	-	4	-
2	Лабораторные работы (ПЗ)	4	-	4	-
3	Практические занятия (ПЗ)	2	-	2	-
4	Семинары (С)	-	-	-	-
5	Курсовое проектирование (КП)	-	-	-	-
6	Рефераты (Р)	-	-	-	-
7	Эссе (Э)	-	-	-	-
8	Индивидуальные домашние задания (ИДЗ)	-	-	-	-
9	Самостоятельное изучение вопросов (СИВ)	-	60	-	60
10	Подготовка к занятиям (ПкЗ)	-	36		36
11	Промежуточная аттестация	2	-	2	-
12	Наименование вида промежуточной аттестации	х	х	зачет	
13	Всего	12	96	12	96

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	Раздел 1. Информационная безопасность и уровни её обеспечения. Компьютерные вирусы и защита от них	9	2	2	2	x	x	x	x	30	18	x	ОК-12 ПСК-1 ПК-27
1.1.	Тема 1 Понятие «Информационная безопасность». Составляющие информационной безопасности	9	1	x	2	x	x	x	x	6	9	x	ОК-12 ПК-27
1.2.	Тема 2 Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»	9	1	2	x	x	x	x	x	6	9	x	ПСК-1 ПК-27
1.3.	Тема 3 Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ	9	-	x	-	x	x	x	x	6	x	x	ОК-12 ПК-27
1.4.	Тема 4 Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»	9	-	-	x	x	x	x	x	6	x	x	ПСК-1 ПК-27
1.5.	Тема 5 - Классификация компьютерных вирусов и характеристика вирусоподобных программ. Антивирусные программы и профилактика компьютерных вирусов	9	-	x	-	x	x	x	x	6	x	x	ОК-12 ПСК-1 ПК-27
2.	Раздел 2. Информационная безопасность вычислительных сетей. Механизмы	9	2	2	-	x	x	x	x	30	18	x	ОК-12 ПСК-1

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	обеспечения информационной безопасности												ПК-27
2.1.	Тема 6 - Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.	9	1	2	x	x	x	x	x	8	9	x	ОК-12 ПК-27
2.2.	Тема 7 Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей	9	1	x	-	x	x	x	x	6	9	x	ПСК-1 ПК-27
2.3	Тема 8 - Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.	9	-	x	x	x	x	x	x	8	x	x	ОК-12 ПК-27
2.4	Тема 9 Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)	9	-	x	-	x	x	x	x	8	x	x	ПСК-1 ПК-27
3.	Контактная работа	x	4	4	2	x	x	x	x	x	x	2	x
4.	Самостоятельная работа	x				x	x	x	x	60	36	x	x
5.	Объем дисциплины в 9 семестре	x	4	4	2	x	x	x	x	60	36	2	x
6.	Всего по дисциплине	x	4	4	2	x	x	x	x	60	36	2	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Понятие «Информационная безопасность». Составляющие информационной безопасности	1
Л-2	Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»	1
Л-3	Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.	1
Л-4	Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей	1
Итого по дисциплине		4

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
ПЗ-1	Понятие «Информационная безопасность». Составляющие информационной безопасности	2
Итого по дисциплине		2

5.2.3. – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
ЛР-1	Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»	2
ЛР-2	Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.	2
Итого по дисциплине		4

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1	Понятие «Информационная безопасность». Составляющие информационной безопасности.	1. Основы обеспечения информационной безопасности предприятия.	3
		2. Основные способы защиты информации предприятия	3
2	Нормативно-правовые основы информационной	1. Структура информационного законодательства.	3

	безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»	2. Информационно-правовые нормы международных актов.	3
3	Стандарты информационной безопасности распределенных систем. Стандарты информационной безопасности в РФ	1 Стандарты информационной безопасности распределенных систем	3
		2 Стандарты информационной безопасности в РФ	3
4	Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»	1. Административный уровень обеспечения информационной безопасности	3
		2. Классификация угроз «Информационной безопасности»	3
5	Классификация компьютерных вирусов и характеристика вирусоподобных программ. Антивирусные программы и профилактика компьютерных вирусов	1. Характерные черты компьютерных вирусов	3
		2. Особенности работы антивирусных программ. Классификация антивирусных программ	3
6	Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.	1 Особенности обеспечения информационной безопасности в компьютерных сетях	3
		2 Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика	4
7	Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей	1 Причины успешной реализации удаленных угроз в вычислительных сетях.	3
		2 Принципы защиты распределенных вычислительных сетей	4
8	Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа.	1 Идентификация и аутентификация. Криптография и шифрование	4
		2. Методы разграничение доступа.	4
9	Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)	1 Регистрация и аудит. Межсетевое экранирование.	4
		2. Технология виртуальных частных сетей (VPN)	4
Итого по дисциплине			60

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М.: Издательство Юрайт, 2016. — 321 с. — ЭБС «Юрайт».

2. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2016. — 325 с. — ЭБС «Юрайт».

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1 Внуков, А. А. Защита информации [Электронный ресурс]: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — ЭБС «Юрайт».

2. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 с.- ЭБС «IPRbooks»

6.3 Методические указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие включающее:

- конспект лекций
- методические указания по выполнению лабораторных работ
- методические указания по проведению практических занятий.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие включающее:

- методические рекомендации по самостоятельному изучению вопросов
- методические рекомендации по подготовке к занятиям

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. OpenOffice
2. JoliTest

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС «Юрайт». www.biblio-online.ru
2. ЭБС «IPR books». <http://www.iprbookshop.ru/>
3. eLIBRARY.RU: www.elibrary.ru/
5. Википедия: <https://ru.wikipedia.org/>

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, оборудованных учебной доской, рабочим местом преподавателя (стол, стул), а также посадочными местами для обучающихся, число которых соответствует численности обучающихся в группе.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций.

Текущий контроль и промежуточная аттестация проводятся в учебных аудиториях для текущего контроля и промежуточной аттестации.

Самостоятельная работа студентов проводится в помещении для самостоятельной работы.

Таблица 7.1 – Материально-техническое обеспечение лабораторных занятий

Вид и № занятий	Тема занятия	Название аудитории	Название оборудования	Название технических и электронных средств обучения и контроля знаний
ЛР-1	Тема 2 Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности: «Общие критерии»	Компьютерный класс	Компьютер	Презентация в OpenOffice
ЛР-2	Тема 4 Административный уровень обеспечения информационной безопасности. Классификация угроз «Информационной безопасности»	Компьютерный класс	Компьютер	Презентация в OpenOffice
ЛР-3	Тема 6 - Особенности обеспечения информационной безопасности в компьютерных сетях. Классификация удаленных угроз в вычислительных сетях.	Компьютерный класс	Компьютер	Презентация в OpenOffice
ЛР-4	Тема 8 - Идентификация и аутентификация. Криптография и шифрование. Методы разграничения доступа.	Компьютерный класс	Компьютер	Презентация в OpenOffice

Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 38.05.01 Экономическая безопасность, утвержденным приказом Министерства образования и науки РФ от 16 января 2017 г. №20.

Разработал(а): _____

О.Я. Набокина