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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.23 Основы управления информационной безопасностью

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

1. **Цели освоения дисциплины**

- изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

2. **Место дисциплины в структуре образовательной программы**

Дисциплина «Основы управление информационной безопасностью» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Основы управление информационной безопасностью» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОПК-7	Информационные технологии
	Теоретические основы защиты информаци
ПК-5, ПК-7	Технология построения защищенных автоматизированных систем
ПК-13	Маркетинг

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-5, ПК-7, ПК-13	Производственная эксплуатационная практика
	Производственная (преддипломная) практика
ОПК-7, ПК-5, ПК-7, ПК-13	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

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
ОПК-7 - Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных	Этап 1: Знание информационных ресурсов	Этап 1: Умения анализа структуры и содержания информационных процессов на объекте защиты	Этап 1: Навыки определять информационные ресурсы, подлежащие защите,

процессов и особенностей функционирования объекта защиты			
ОПК-7 - Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Этап 2: Угрозы безопасности и возможные пути их реализации	Этап 2: Умения анализа особенностей функционирования объекта защиты	Этап 2: Навыки определения угрозы безопасности информации и возможные пути их реализации
ПК-5 - Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Этап 1: Знание государственных нормативных документов	Этап 1: Умения аттестации объектов информатизации по требованиям безопасности информации	Этап 1: Навыки организовать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-5 - Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Этап 2: Знание корпоративных нормативных документов	Этап 2: Умения составления отчетной документации по результатам аттестации	Этап 2: Навыки сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-7 - Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих	Этап 1: Знания разработки информационных систем	Этап 1: Умения проектирования информационных систем и средств обеспечения информационной безопасности	Этап 1: Навыки собрать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности

проектных решений			
ПК-7 - Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Этап 2: Знания основ информационной безопасности	Этап 2: Умения проведения технико-экономического обоснования соответствующих проектных решений	Этап 2: Навыки провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
ПК-13 - Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 1: Общие методологические принципы построения комплексных систем обеспечения информационной безопасности;	Этап 1: Умениями работы с нормативно-правовыми актами	Этап 1: Навыки участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
ПК-13 - Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 2: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем;	Этап 2: Первичными навыками работы с основными средствами обеспечения информационной безопасности	Этап 2: Навыки управления процессом реализации комплекса мер по обеспечению информационной безопасности

4. Объем дисциплины

Объем дисциплины «Безопасность систем баз данных» составляет 2 зачетные единицы (72 академических часа), 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 № 8	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	26		26	
2	Лабораторные работы (ЛР)				
3	Практические занятия (ПЗ)	36		36	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		4		4
10	Подготовка к занятиям (ПкЗ)		4		4
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации	х	х	зачет	
13	Всего	64	8	64	8

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 Введение в управление информационной безопасностью**	8	8		12			x		2	2	x	ОПК-7, ПК-5, ПК-7, ПК-13
1.1.	**Тема 1** Предмет, цели, задачи и содержание курса	8	4		6			x		2		x	ОПК-7, ПК-5, ПК-7, ПК-13
1.2.	**Тема 2** Структура и штаты службы защиты информации	8	4		6			x			2	x	ОПК-7, ПК-5, ПК-7, ПК-13
2.	**Раздел 2 Организационные основы и принципы деятельности службы защиты информации**	8	10		12			x		2		x	ОПК-7, ПК-5, ПК-7, ПК-13
2.1	**Тема 3** Основные принципы организации	8	6		6			x		2		x	ОПК-7, ПК-5,

№ 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
	и деятельности службы защиты информации												ПК-7, ПК-13
2.2	**Тема 4** Подбор кадров службы защиты информации	8	4		6			x				x	ОПК-7, ПК-5, ПК-7, ПК-13
3	**Раздел 3 Принципы и методы управления службой защиты информации**	8	8		12			x			2	x	ОПК-7, ПК-5, ПК-7, ПК-13
3.1.	**Тема 5** Организация труда сотрудников службы защиты информации	8	4		6			x			2	x	ОПК-7, ПК-5, ПК-7, ПК-13
3.2.	**Тема 6** Технология управления службой защиты информации	8	4		6			x				x	ОПК-7, ПК-5, ПК-7, ПК-13
3.	**Контактная работа**	8	26		36			x				2	x

№ 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
4.	**Самостоятельная работа**	8						x		4	4		x
5.	**Объем дисциплины в семестре**	8	26		36			x		4	4	2	x
6.	**Всего по дисциплине**	x	26		36			x		4	4	2	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах	**2**
Л-2	Задачи и функции службы защиты информации	**2**
Л-3	Задачи и функции службы защиты информации	**2**
Л-4	Общая структурная система службы защиты информации	**2**
Л-5	Порядок создания службы защиты информации	**2**
Л-6	Порядок создания службы защиты информации	**2**
Л-7	Подбор, расстановка и обучение сотрудников службы защиты информации	**2**
Л-8	Структура и содержание должностных инструкций сотрудников службы защиты информации	**2**
Л-9	Структура и содержание должностных инструкций сотрудников службы защиты информации	**2**
Л-10	Принципы управления службой защиты информации	**2**
Л-11	Принципы управления службой защиты информации	**2**
Л-12	Значение управленческих решений	**2**
Л-13	Значение управленческих решений	**2**
Итого по дисциплине		

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1	Оценочные стандарты в информационной безопасности	**2**
ПЗ-2	Роль стандартов ИБ	**2**
ПЗ-3	Оценочные стандарты в информационной безопасности Международный стандарт ISO/IEC 15408	**2**
ПЗ-4	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.	**2**
ПЗ-5	Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	**2**
ПЗ-6	Служба защиты информации, ее назначение	**2**
ПЗ-7	Создание СУИБ на предприятии	**2**
ПЗ-8	Основные процессы СУИБ	**2**
ПЗ-9	Процессы улучшения СУИБ	**2**
ПЗ-10	Процесс «Мониторинг эффективности».	**2**

ПЗ-11	Основные процессы СУИБ	**2**
ПЗ-12	Подбор кадров службы защиты информации	**2**
ПЗ-13	Методика оценки рисков информационной безопасности предприятия	**2**
ПЗ-14	Метод оценки рисков на основе модели угроз и уязвимостей	**2**
ПЗ-15	Методика оценки рисков информационной организации на основе модели информационных потоков	**2**
ПЗ-16	Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков	**2**
ПЗ-17	Оценка рисков по факторам	**2**
ПЗ-18	Табличные методы оценки рисков	**2**
Итого по дисциплине		

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Предмет, цели, задачи и содержание курса	Формы повышения квалификации сотрудников. Охрана труда. Культура труда. Карты организации трудового процесса.	2
2.	Основные принципы организации и деятельности службы защиты информации	Социально-психологические факторы, влияющие на расстановку кадров.	2
Итого по дисциплине			**4**

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c.

2. Астахов А.М. Искусство управления информационными рисками [Электронный ресурс]/ Астахов А.М.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 312 с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1 Шаньгин, В.Ф.Защита информации в компьютерных системах и сетях. Издательство: ДМК Пресс, 2012. - 591 с.

2 Лапонина, О.Р.Межсетевое экранирование: Учебное пособие. Издательство: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007 - 344 с.

3 Семененко, В. А. Программно-аппаратная защита информации: учеб.пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.

4 Грибунин, В. Г. Комплексная система защиты информации на предприятии: учеб.пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 413 с.

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

Электронное учебное пособие, включающее:

- конспект лекций;
- методические указания по выполнению практических (семинарских) работ.

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

Электронное учебное пособие, включающее:

- методические рекомендации для студентов по самостоятельной работе;
- 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. Open Office
2. JoliTest (JTRun, JTEditor, TestRun)

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

1. http://fstec.ru/normotvorcheskaya/akty
2. http://ivo.garant.ru/#/startpage:0
3. http://www.consultant.ru/

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

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

Номер ПЗ	Тема практических занятий	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ПЗ-1	Оценочные стандарты в информационной безопасности	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-2	Роль стандартов ИБ	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-3	Оценочные	941 аудитория -	ПЭВМ	1. Windows XP/7

	стандарты в информационной безопасности Международный стандарт ISO/IEC 15408	лаборатория аппаратных средств защиты информации		2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-4	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-5	Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-6	Служба защиты информации, ее назначение	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-7	Создание СУИБ на предприятии	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-8	Основные процессы СУИБ	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-9	Процессы улучшения СУИБ	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel

				4. Microsoft Power Point 5. Paint
ПЗ-10	Процесс «Мониторинг эффективности».	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-11	Основные процессы СУИБ	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-12	Подбор кадров службы защиты информации	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-13	Методика оценки рисков информационной безопасности предприятия	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-14	Метод оценки рисков на основе модели угроз и уязвимостей	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-15	Методика оценки рисков информационной организации на основе модели информационных потоков	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint

ПЗ-16	Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-17	Оценка рисков по факторам	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint
ПЗ-18	Табличные методы оценки рисков	941 аудитория - лаборатория аппаратных средств защиты информации	ПЭВМ	1. Windows XP/7 2. Microsoft Office Word 3. Microsoft Office Excel 4. Microsoft Power Point 5. Paint

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочный материал для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 6.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ от «01» декабря 2016 г. № 1515

Разработал(и): _____ Полищук Ю.В