ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

- освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.02 Аудит информационной безопасности относится к части, формируемой участниками образовательных отношений учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Аудит информационной безопасности» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-4	Системы реального времени Математическая статистика Основы научных исследований Маркетинг
ПК-6	Системы реального времени Математическая статистика Основы научных исследований Маркетинг Моделирование систем

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-4	КОИБАС Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика Технология построения защищенных автоматизированных систем
ПК-5	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика
ПК-6	КОИБАС Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Производственная (преддипломная) практика Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ)

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

Код и наименование компетенции	Код и наименование индикатора	Планируемые результаты обучения по дисциплине (модулю)
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	*Знать:* Риск утечки конфиденциальной информации *Уметь:* Анализировать риски информационной безопасности, которые напрямую связаны с возможностью осуществления угроз безопасности для предприятия в отношении ресурсов информационной системы *Владеть:* Навыками определения основных видов угроз безопасности, рассматриваемыми при проведении аудита информационной безопасности
	ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	*Знать:* Оценку информационной системы предприятия на предмет соответствия существующим стандартам и нормативно-правовым документам в области информационной безопасности *Уметь:* Исследовать локальные вычислительные системы *Владеть:* Постановкой задачи аудита информационной безопасности

ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	*Знать:* Принципы организации информационных систем в соответствии с требованиями по защите информации *Уметь:* Правильно формулировать требования к программам для решения системных задач *Владеть:* Методами формализации информационных процессов объекта и связей между ними
	ПК-4.4 Применяет нормативные документы по противодействию технической разведки	*Знать:* Требования стандартов и другой нормативной документации в области информационной безопасности *Уметь:* Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня технических средств защиты информации *Владеть:* Навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты

ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Применяет существующие методики для аттестации объектов информатизации	*Знать:* Методы проведения аттестация объектов информатизации по требованиям стандартов и другой нормативной документации *Уметь:* Разрабатывать меры поддержки по обеспечению информационной безопасности *Владеть:* Навыками организации и проведении контрольных проверок работоспособности и эффективности применяемых средств защиты информации
ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы	ПК-6.1 Проводит оценку рисков информационной безопасности на основе существующих методик	*Знать:* Риск распространения дискредитирующей во внешней среде информации *Уметь:* Работать с основными средствами защиты информации *Владеть:* Навыками использования математических методов и моделей для решения задач

4. Объем дисциплины

Объем дисциплины Б1.В.02 Аудит информационной безопасности составляет 3 зачетных(ые) единиц(ы) (ЗЕ), (108 академических часов), распределение объёма 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

Вид учебной работы	Итого КР	Итого СР	Семестр №7	
			КР	СР
Лекции (Л)	18		18	
Лабораторные работы (ЛР)				
Практические занятия (ПЗ)	34		34	
Семинары(С)				
Курсовое проектирование (КП)				

Самостоятельная работа		52		52
Промежуточная аттестация	4		4	
Наименование вида промежуточной аттестации	x	x	Экзамен	
Всего	56	52	56	52

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		Лекции	Лабораторная работа	Практические занятия	Семинары	Курсовое проектирование	Индивидуальные домашние задания (контрольные работы)	Самостоятельноеизучение вопросов	Подготовка к занятиям	Промежуточная аттестация	
Тема 1. Понятие аудита безопасности	7	2		2				6			ПК-4.1, ПК-4.2, ПК-4.3,
Тема 2. Методы анализа данных при аудите информационной безопасности	7	2		4				6			ПК-4.1, ПК-6.1, ПК-4.2, ПК-4.3
Тема 3. Анализ и управление рисками информационной безопасности	7	2		4				6			ПК-4.1, ПК-6.1
Тема 4. Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	7	2		4				6			ПК-4.4, ПК-5.1

Тема 5. Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	7	2		4				6			ПК-5.1
Тема 6. Лицензирование и сертификация деятельности в области защиты информации	7	2		4				6			ПК-4.4, ПК-5.1
Тема 7. Стандарты, применяемые для оценки информационной безопасности	7	2		4				6			ПК-4.3, ПК-4.2
Тема 8. Методики проведения аудита информационной безопасности	7	2		4				6			ПК-5.1, ПК-6.1
Тема 9. Применение программных средств для аудита информационной безопасности	7	2		4				4			ПК-4.1
Контактная работа	7	18		34						4	x
Самостоятельная работа	7							52			x
Объем дисциплины в семестре	7	18		34				52		4	x
Всего по дисциплине		18		34				52		4	

5.2. Темы курсовых работ (проектов)

Данный вид работы не предусмотрен учебным планом

5.3. Темы индивидуальных домашних заданий (контрольных работ)

Данный вид работы не предусмотрен учебным планом

5.4 Вопросы для самостоятельного изучения по очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Понятие аудита безопасности	Какая информация является конфиденциальной	6
2	Методы анализа данных при аудите информационной безопасности	Что относится к защищаемой информации	6
3	Анализ и управление рисками информационной безопасности	Что понимается под политикой безопасности	6
4	Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	Что понимается под несанкционированным воздействием на защищаемую информацию?	6
5	Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	Дайте понятие конфиденциальности, целостности и доступности информации	6
6	Лицензирование и сертификация деятельности в области защиты	Дайте определение информационной безопасности	6

7	Стандарты, применяемые для оценки информационной безопасности	Какие цели и задачи включает в себя концепция национальной безопасности РФ	6
8	Методики проведения аудита информационной безопасности	Перечислите основные виды угроз информационной безопасности РФ	6
9	Применение программных средств для аудита информационной безопасности	Дайте определение комплексного обеспечения информационной безопасности	4
		Всего	52

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2007. — 201 с. — ISBN 978-5-868889-467-1. — Текст : электронный // Лань : электронно-библиотечная система.
2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система.
3. Нормативное обеспечение эксплуатации средств защиты информации : учебное пособие / А. В. Красов, И. И. Лившиц, Д. В. Юркин [и др.]. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Стеганографические и криптографические методы защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система.
2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

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, укомплектованных специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа-проектором, компьютером и учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант +

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

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 7 от 22.03.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.В.02 Аудит информационной безопасности на 2021-2022 учебный год.

В программу вносятся следующие изменения: без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2022 г.

Зав. кафедрой _____ Урбан Владимир Александрович