ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07 КОИБАС

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

– овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.07 КОИБАС относится к части, формируемой участниками образовательных отношений учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «КОИБАС» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-1	Основы защиты АИС Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) Производственная (преддипломная) практика
ПК-3	Безопасность операционных систем Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) Производственная (преддипломная) практика
ПК-4	Математическая статистика Аудит информационной безопасности Маркетинг Производственная (преддипломная) практика
ПК-6	Математическая статистика Моделирование систем Аудит информационной безопасности Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) Маркетинг Производственная (преддипломная) практика

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-1	Производственная (преддипломная) практика Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Безопасностьсистембазданных
ПК-3	Производственная (преддипломная) практика Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Безопасностьсистембазданных
ПК-4	Производственная (преддипломная) практика Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-6	Производственная (преддипломная) практика Подготовка к процедуре защиты и защита выпускной квалификационной работы (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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	*Знать:* О политике безопасности и мерах защиты в ИС *Уметь:* Разбираться в реализации комплексного подхода к обеспечению информационной безопасности *Владеть:* Навыками разработки политики безопасности
	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	*Знать:* Основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам *Уметь:* Применять технические средства защиты информации *Владеть:* Использованием основных методов и средств инженерно-технической защиты информации

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* Методы и средства обнаружения враждебного воздействия *Уметь:* Создавать механизм оперативного мониторинга и реагирования на нарушения *Владеть:* Анализом структуры внутренних угроз и наиболее серьезных нарушений в области информационной безопасности
	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* О предметной области комплекса проблем в сфере информационных технологий, качественных и количественных методах *Уметь:* Использовать основные положения и методы при решении задачи в области информационной безопасности *Владеть:* Способностью к обобщению, анализу и восприятию информации, навыками системного подхода к оценке уровня профессиональной квалификации для ее эффективного повышения

ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	*Знать:* Современные критерии оценки риска и стандарты в области управления рисками для анализа безопасности распределенных компьютерных систем *Уметь:* Применять на практике подходы к аналитическому оцениванию рисков, в том числе при нерегулярности распределения ущербов и их динамики *Владеть:* Технологиями обеспечения информационной безопасности в части проведения анализа и управления риска
	ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	*Знать:* Требования к встроенным средствам защиты информации программного обеспечения *Уметь:* Анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации *Владеть:* Навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования

ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	*Знать:* Руководящие нормативные и методические документы уполномоченных федеральных органов исполнительной власти по защите информации *Уметь:* Разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности) *Владеть:* Навыками планирования мероприятий по обеспечению защиты информации и организации работы персонала автоматизированной системы с учетом требований по защите информации
	ПК-4.4 Применяет нормативные документы по противодействию технической разведки	*Знать:* нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации *Уметь:* Разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации *Владеть:* Навыками по разработке политики безопасности объекта информатизации

ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы	ПК-6.1 Проводит оценку рисков информационной безопасности на основе существующих методик	*Знать:* Методики проведения риск-анализа и управления рисками, а также тестирования средств обеспечения информационной безопасности *Уметь:* Анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации *Владеть:* Средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками

4. Объем дисциплины

Объем дисциплины Б1.В.07 КОИБАС составляет 4 зачетных(ые) единиц(ы) (ЗЕ), (144 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 №8	
			КР	СР
Лекции (Л)	26		26	
Лабораторные работы (ЛР)				
Практические занятия (ПЗ)	24		24	
Семинары(С)				
Курсовое проектирование (КП)				
Самостоятельная работа		94		94
Промежуточная аттестация				
Наименование вида промежуточной аттестации	x	x	Зачёт	
Всего	50	94	50	94

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименованиетем	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)	Самостоятельное изучение вопросов	Подготовка к занятиям	Промежуточная аттестация	
Тема 1. Классификация угроз ИБ	8	2		2				6			ПК-1.1, ПК-1.2, ПК-3.1
Тема 2. Анализ угроз ИБ	8	2		2				2			ПК-3.2, ПК-4.1, ПК-4.2
Тема 3. Технические каналы утечки информации	8	2		2				4			ПК-4.3, ПК-4.4, ПК-6.1
Тема 4. Акустические каналы утечки информации	8	2		2							ПК-3.2
Тема 5. ПЭМИН	8							8			ПК-3.1, ПК-3.2, ПК-4.1
Тема 6. Закладные устройства	8							2			ПК-4.2
Тема 7. Визуально-оптические каналы утечки информации	8							6			ПК-4.3, ПК-6.1
Тема 8. Материально-вещественные каналы утечки информации	8							6			ПК-3.1
Тема 9. Методология построения КОИБАС	8	2		2				4			ПК-6.1, ПК-4.2, ПК-4.1
Тема 10. Определение состава компонентов КСИБ	8	2		2							ПК-1.1, ПК-1.2
Тема 11. Стадии и этапы проектирования КСИБ	8	2		2				4			ПК-4.1, ПК-4.3, ПК-6.1
Тема 12. Формирование задач защиты информации	8	2		2				4			ПК-1.1, ПК-3.1, ПК-4.3

Тема 13. Функциональные и обеспечивающие подсистемы КСИБ	8							4			ПК-1.1
Тема 14. Правовые аспекты защиты информации	8							6			ПК-1.1
Тема 15. Организационные мероприятия по защите информации	8							6			ПК-3.1
Тема 16. Инженерно-технические мероприятия по ЗИ	8							2			ПК-3.1
Тема 17. Политика информационной безопасности	8	2		1				4			ПК-1.1, ПК-3.1, ПК-4.2
Тема 18. Модель нарушителя	8	2		1				4			ПК-3.1, ПК-3.2,
Тема 19. Классификация защищенности АС	8	2		2							ПК-3.2, ПК-4.4, ПК-6.1
Тема 20. Оценка защищенности АС	8	2		2				4			ПК-1.1, ПК-4.3, ПК-6.1
Тема 21. Аттестация объектов защиты	8	2		2				4			ПК-4.4, ПК-1.2, ПК-4.2
Тема 22. Эксплуатационная документация КСИБ	8							2			ПК-4.1
Тема 23. Оценка технико-экономического уровня и эффективности КСИБ	8							6			ПК-4.3
Тема 24. Управление деятельностью организации по КОИБАС	8							2			ПК-1.1, ПК-6.1
Тема 25. Перспективы развития элементов КОИБАС	8							2			ПК-1.1, ПК-4.1
Тема 26. Натурные испытания КС защиты	8							2			ПК-4.3
Контактная работа	8	26		24							x
Самостоятельная работа	8							94			x
Объем дисциплины в семестре	8	26		24				94			x
Всего по дисциплине		26		24				94			

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 изученияпо очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Классификация угроз ИБ	Назначение и характер аппаратных средств защиты информации	6
2	Анализ угроз ИБ	Анализ криптостойкости методов защиты информации в операционных системах Microsoft Window	2
3	Технические каналы утечки информации	Комплекс технических решений по защите информации, записанной на отчуждаемых электронных носителях от несанкционированного копирования и распространения	4
4	ПЭМИН	Методика выявление каналов НСД и ПЭМИН	8
5	Закладные устройства	Выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников	2
6	Визуально-оптические каналы утечки информации	Средства контроля эффективности защиты информации	6
7	Материально-вещественные каналы утечки информации	Методы определения границ охраняемой зоны (территории)	6
8	Методология построения КОИБАС	Повышение информационной безопасности предприятия	4
9	Стадии и этапы проектирования КСИБ	Подготовка технического задания к КСИБ	4
10	Формирование задач защиты информации	Организация безопасной корпоративной компьютерной сети в предприятии	4
11	Функциональные и обеспечивающие подсистемы КСИБ	Разработка наполнения и документации к КСИБ	4
12	Правовые аспекты защиты информации	Международные стандарты для построения системы	6

13	Организационные мероприятия по защите информации	Организационно-технические мероприятия по защите информации	6
14	Инженерно-технические мероприятия по ЗИ	Технические мероприятия по защите конфиденциальной информации	2
15	Политика информационной безопасности	Аудит информационной безопасности банка	4
16	Модель нарушителя	Целевая функция информационной безопасности	4
17	Оценка защищенности АС	Разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий	4
18	Аттестация объектов защиты	Внедрение аппаратной аутентификации защиты на предприятии	4
19	Эксплуатационная документация КСИБ	Подбор средств для КСИБ	2
20	Оценка технико-экономического уровня и эффективности КСИБ	Оценка качества разработанной КСИБ	6
21	Управление деятельностью организации по КОИБАС	Организация безопасной корпоративной компьютерной сети в предприятии	2
22	Перспективы развития элементов КОИБАС	Современные модели и методы оценки безопасности информации	2
23	Натурные испытания КС защиты	Защита баз данных	2
		Всего	94

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Бурова, М. А. Информационная безопасность и защита информации : учебное пособие / М. А. Бурова, А. С. Овсянников. — Самара : СамГУПС, [б. г.]. — Часть 2 — 2012. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система.
2. 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.
3. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система.
2. Информационные технологии. Базовый курс : учебник для вузов / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 604 с. — ISBN 978-5-8114-8776-9. — 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 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.В.07 КОИБАС 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 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович