Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:

Ректор
_____ / Н.В. Дубив/

«____»_____ 2025 г.

Рабочая программа учебной дисциплины

Безопасность объектов критической информационной инфраструктуры

образовательной программы высшего образования –
программы магистратуры

13.04.02 – Электроэнергетика и электротехника

Направленность:
Цифровые технологии в электроэнергетике

Формы обучения: **заочная**

Курган 2025

Рабочая программа дисциплины «Безопасность объектов критической информационной инфраструктуры» составлена в соответствии с учебными планами по программе магистратуры: «Электроэнергетика и электротехника» (Цифровые технологии в электроэнергетике), утвержденными

- для заочной формы обучения 27 июня 2025 г.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 3 июля 2025 года, протокол № 17.

Рабочую программу разработал
заведующий кафедрой
«Безопасность информационных и
автоматизированных систем» _____ Д.И. Дик

Согласовано:

Заведующий кафедрой
«Цифровая энергетика» _____ Ж.В. Нечеухина

Руководитель программы
магистратуры _____ В.И. Мошкин

Специалист по учебно-методической
работе учебно-методического отдела _____ Г.В. Казанкова

Начальник управления образовательной
деятельности _____ Н.В. Григоренко

1 ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины - 4 зачетных единицы (144 акад. часа)

Вид учебной работы	Распределение трудоемкости по семестрам и видам учебных занятий, акад. часов	
	Всего	Семестры
		3
Аудиторные занятия в том числе:	**8**	**8**
Лекции	4	4
Лабораторные работы	4	4
Самостоятельная работа в том числе:	**136**	**136**
Подготовка к зачету	18	18
Другие виды самостоятельной работы	118	118
Общая трудоемкость дисциплины	**144**	**144**
Виды промежуточной аттестации	**Зачет**	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Безопасность объектов критической информационной инфраструктуры» является вариативной дисциплиной по выбору Блока 1 и относится к части, формируемой участниками образовательных отношений.

Для освоения дисциплины необходимы компетенции, в области основ информационной безопасности, правоведения, основ управленческой деятельности, формируемые соответствующими дисциплинами программ бакалавриата или специалитета.

Результаты изучения дисциплины необходимы при подготовке магистерской диссертации.

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является формирование у обучающихся представления об обеспечении информационной безопасности объектов критической информационной инфраструктуры, приобретение комплекса теоретических и практических знаний в области обеспечении информационной безопасности объектов критической информационной инфраструктуры.

Задачами дисциплины являются:

– дать основы законодательства Российской Федерации об обеспечении безопасности критической информационной инфраструктуры;

– ознакомление с основами угрозами информационной безопасности объектов критической информационной инфраструктуры;

– дать основы требований, предъявляемых к организационным и техническим мерам защиты информации значимых объектах критической информационной инфраструктуры.

Компетенции, формируемые в результате освоения дисциплины:

- способен применять методы и средства обеспечения информационной безопасности (ПК-5).

В результате изучения дисциплины обучающийся должен:

знать:

– понятие субъектов и объектов критической информационной инфраструктуры (для ПК-5);

– основные угрозы безопасности информации, обрабатываемой на объектах критической информационной инфраструктуры (для ПК-5);

– основные уязвимости объектов критической информационной инфраструктуры (для ПК-5);

– знать порядок создания системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры (для ПК-5);

уметь:

– выполнять категорирование объектов критической информационной инфраструктуры (для ПК-5);

– определять основные угрозы безопасности информации, обрабатываемой на объектах критической информационной инфраструктуры (для ПК-5);

владеть:

– навыками выбора организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры (для ПК-5).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Безопасность объектов критической информационной инфраструктуры», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Безопасность объектов критической информационной инфраструктуры», индикаторы достижения компетенций ПК-5, перечень оценочных средств

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1пк-5	Знать: порядок создания системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	З (ИД-1пк-5)	Знает: порядок создания системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	Вопросы теста
2.	ИД-2 пк-5	Уметь: определять основные угрозы безопасности информации, обрабатываемой на объектах критической информационной инфраструктуры	У (ИД-2пк-5)	Умеет: определять основные угрозы безопасности информации, обрабатываемой на объектах критической информационной инфраструктуры	Комплект имитационных задач
3.	ИД-3 пк-5	Владеть: навыками выбора организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры	В (ИД-3пк-5)	Владеет: навыками выбора организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры	Вопросы для сдачи зачета

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Учебно-тематический план

Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
		Лекции	Лабораторные работы
1	Субъекты КИИ: понятие, определение принадлежности.	0,5	–
2	Объекты КИИ: типы и виды.	0,5	–
3	Категорирование объектов КИИ	0,5	2
4	Угрозы безопасности информации, обрабатываемой на объектах КИИ	0,5	–
5	Требования по обеспечению безопасности значимых объектов КИИ	0,5	2
6	Система безопасности значимого объекта КИИ	0,5	–
7	Взаимодействие с ГосСОПКА	0,5	–
8	Аутсорсинг услуг.	0,5	–
	Всего:	**4**	**4**

4.2 Содержание лекционных занятий

Тема №1. Субъекты КИИ: понятие, определение принадлежности.

Понятие «субъект КИИ». Исходные данные для определения сферы функционирования организации. Алгоритм определение принадлежности организации (предприятия, учреждения и т.п.) к субъектам КИИ.

Тема №2. Объекты КИИ: типы и виды.

Виды систем, имеющихся у субъектов КИИ. Классификация объектов КИИ по значимости, сфере деятельности, виду. Права субъекта КИИ. Обязанности субъекта КИИ. Основные нормативно-правовые акты, предусматривающие меры обеспечения безопасности объектов КИИ.

Тема №3. Категорирование объектов КИИ.

Понятие категорирования объектов КИИ. Процедура категорирования. Формирование комиссии по категорированию. Подготовка перечня объектов КИИ подлежащих категорированию. Категорирование (присвоение объекту КИИ категории, либо принятие мотивированного решения об отсутствии необходимости в ее присвоении). Оценка объектов КИИ в соответствии с показателями критериев значимости и присвоение каждому из объектов КИИ категории, либо принятие решения об отсутствии необходимости ее присвоения. Подготовка итоговых документов по результатам категорирования. Сроки категорирования.

Тема №4. Угрозы безопасности информации, обрабатываемой на объектах КИИ.

Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопас-

ности информации значимого объекта КИИ. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности информации и последствий от их реализации.

Тема №5. Требования по обеспечению безопасности значимых объектов КИИ.

Установление требований по обеспечению безопасности значимого объекта КИИ. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ. Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ.

Тема №6. Система безопасности значимого объекта КИИ.

Создание системы обеспечения информационной безопасности значимых объектов КИИ (СОИБ ЗОКИИ). Алгоритм функционирования системы. Этапы создания СОИБ ЗОКИИ: планирование, реализация, мониторинг и контроль, совершенствование.

Тема №7. Взаимодействие с ГосСОПКА.

Основные термины и определения применяемые в сфере функционирования ГосСОПКА. Нормативно-правовые акты по вопросам взаимодействия с ГосСОПКА. Структура ГосСОПКА. Основные задачи центров ГосСОПКА. Взаимодействие субъекта КИИ с ГосСОПКА. Базовый комплект документации ведомственного (корпоративного) центра (сегмента) ГосСОПКА.

Тема №8. Аутсорсинг услуг.

Облачный провайдер как субъект КИИ. Перенос ответственности с субъекта КИИ на аутсорсера.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторной работы	Норматив времени, час.

3	Категорирование объектов КИИ	Выполнение категорирования объектов КИИ.	2
5	Требования по обеспечению безопасности значимых объектов КИИ	Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ	2
		Итого:	**4**

5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Лекционный курс базируется на пассивном методе обучения, реализующем традиционную объяснительно-иллюстративную образовательную технологию, в рамках которой магистры выступают в роли слушателей, воспринимающих учебный материал и участвующих в дискуссиях и экспресс-опросах.

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано применение на лабораторных работах разбор конкретных ситуаций.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела:	**110**
Субъекты КИИ: понятие, определение принадлежности.	10
Объекты КИИ: типы и виды.	12
Категорирование объектов КИИ	16
Угрозы безопасности информации, обрабатываемой на объектах КИИ	19
Требования по обеспечению безопасности значимых объектов КИИ	19
Система безопасности значимого объекта КИИ	14
Взаимодействие с ГосСОПКА	12
Аутсорсинг услуг	8
Подготовка к лабораторным работам (по 4 часа на каждую работу)	8
Подготовка к зачету	18
Всего:	**136**

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1 Перечень оценочных средств

1. Отчеты обучающихся по лабораторным работам.
2. Вопросы к зачету.

6.2 Процедура оценивания результатов освоения дисциплины

Зачет – в форме устного ответа на 2 вопроса. Перечень вопросов преподаватель выдает заранее. Время, отводимое обучающемуся на подготовку вопросов, составляет 1 академический час.

Результаты зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4 Примеры оценочных средств для зачета

Примерный перечень вопросов к зачету

1. Понятие субъекта КИИ. Исходные данные для определения сферы функционирования организации.
2. Алгоритм определение принадлежности организации к субъектам КИИ.
3. Классификация объектов КИИ по значимости
4. Классификация объектов КИИ сфере деятельности
5. Классификация объектов КИИ виду.
6. Права субъекта КИИ.
7. Обязанности субъекта КИИ.
8. Процедура категорирования объектов КИИ.
9. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ.
10. Модель угроз безопасности информации значимого объекта КИИ.
11. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
12. Источники угроз безопасности информации.
13. Уязвимости объектов КИИ, классификация уязвимостей.
14. Способы реализации угроз безопасности информации и их последствия.
15. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей
16. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.
17. Организационные и технические меры, направленные на блокирова-

ние (нейтрализацию) угроз безопасности информации.

18. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ.

19. Алгоритм функционирования системы обеспечения информационной безопасности значимых объектов КИИ

20. Этапы создания СОИБ ЗОКИИ: планирование, реализация, мониторинг и контроль, совершенствование.

21. Структура ГосСОПКА.

22. Основные задачи центров ГосСОПКА.

23. Взаимодействие субъекта КИИ с ГосСОПКА.

24. Облачный провайдер как субъект КИИ.

25. Перенос ответственности с субъекта КИИ на аутсорсера.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Безопасность объектов критической информационной инфраструктуры организации Общие рекомендации (версия 2.0) / Ассоциацией руководителей служб информационной безопасности (АРСИБ). – Электрон. текст. дан. – М : [?], 2019. – 111 с. – Режим доступа: http://aciso.ru/files/docs/metodichka_2.0.pdf, свободный

2. Ярочкин, В. И. Информационная безопасность : учебник для вузов / Ярочкин В. И. - Москва : Академический Проект, 2020. - 544 с. - Доступ ЭБС «Консультант студента»

7.2 Дополнительная учебная литература

1. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2021. – 432 с. – Доступ ЭБС «Znanium».

2. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. – Доступ ЭБС «Znanium».

7.3 Методическая литература

1. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность объектов критической информационной инфраструктуры».

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. Справочная правовая система «Гарант» - http://www.garant.ru;
3. Справочная правовая система «Консультант Плюс» - http://www.counsultant.ru;
4. ЭБС «Лань» - https://e.lanbook.com/;
5. ЭБС «Znanium» - https://znanium.com/;
6. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
7. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/
8. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань»
2. ЭБС «Консультант студента»
3. ЭБС «Znanium.com»
4. «Гарант» - справочно-правовая система

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально- техническое обеспечение по реализации дисциплины осуществляется в соответствии с требованиями ФГОС ВО по данной образовательной программе.

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами (все – в стандартной комплектации для лабораторных работ и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет, мультимедийное оборудование (переносной персональный компьютер, мультимедийный проектор, мультимедийный экран).

11. **Для студентов, обучающихся с использованием дистанционных образовательных технологий**

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

Аннотация
рабочей программы учебной дисциплины
«Безопасность объектов критической информационной инфраструктуры»
образовательной программы высшего образования –
программы магистратуры
13.04.02 – Электроэнергетика и электротехника

Направленность:
Цифровые технологии в электроэнергетике
Формы обучения: **заочная**

Трудоемкость дисциплины: 4 ЗЕ (144 академических часа)
Семестры: 3-й
Форма промежуточной аттестации: зачет

Содержание дисциплины

Субъекты КИИ: понятие, определение принадлежности. Объекты КИИ: типы и виды. Категорирование объектов КИИ. Угрозы безопасности информации, обрабатываемой на объектах КИИ. Требования по обеспечению безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Взаимодействие с ГосСОПКА. Аутсорсинг услуг.