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:
Первый проректор

_____ / Т.Р. Змызгова/

«____»_____ 2024 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: **очная, заочная**

Курган 2024

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 очной и заочной форм обучения 28 июня 2024 г.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 августа 2024 года, протокол № 1.

Рабочую программу разработал
заведующий кафедрой БИАС _____ Д.И. Дик

Согласовано:

Заведующий кафедрой «Безопасность информационных и автоматизированных систем» _____ Д.И. Дик

Заведующий кафедрой «Цифровая энергетика» _____ В.И. Мошкин

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)

Очная форма обучения

Вид учебной работы	Распределение трудоемкости по семестрам и видам учебных занятий, акад. часов	
	Всего	Семестры
		3
Аудиторные занятия в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	16	16
Самостоятельная работа в том числе:	**112**	**112**
Подготовка к зачету	18	18
Другие виды самостоятельной работы	94	94
Общая трудоемкость дисциплины	**144**	**144**
Виды промежуточной аттестации	**Зачет**	

Заочная форма обучения

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).

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

Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Лабораторные работы
Рубеж 1	1	Субъекты КИИ: понятие, определение принадлежности.	1	–
	2	Объекты КИИ: типы и виды.	1	–
	3	Категорирование объектов КИИ	2	2
	4	Угрозы безопасности информации, обрабатываемой на объектах КИИ	4	6
Рубеж 2	4	Угрозы безопасности информации, обрабатываемой на объектах КИИ	–	4
	5	Требования по обеспечению безопасности значимых объектов КИИ	3	4
	6	Система безопасности значимого объекта КИИ	2	–
	7	Взаимодействие с ГосСОПКА	2	–
	8	Аутсорсинг услуг.	1	–
		Всего:	**16**	**16**

Заочная форма обучения

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 безопасности 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 органи-

зационным 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

Очная форма обучения

Номер темы	Наименование темы	Наименование лабораторной работы	Норматив времени, час.
3	Категорирование объектов КИИ	Выполнение категорирования объектов КИИ.	2
4	Угрозы безопасности информации, обрабатываемой на объектах КИИ.	Сбор информации из открытых источников (рекогносцировка цели)	5
	1-ый рубежный контроль	***Тестирование***	***1***
4	Угрозы безопасности информации, обрабатываемой на объектах КИИ.	Определение угроз ИБ	4
5	Требования по обеспечению безопасности значимых объектов КИИ	Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ	3
	2-ой рубежный контроль	***Тестирование***	***1***
		Итого:	**16**

Заочная форма обучения

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.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, к рубежным контролям (для очной формы обучения) и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Очная форма обучения

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела:	**74**
Субъекты КИИ: понятие, определение принадлежности.	6
Объекты КИИ: типы и виды.	8
Категорирование объектов КИИ	10
Угрозы безопасности информации, обрабатываемой на объектах КИИ	14
Требования по обеспечению безопасности значимых объектов КИИ	14
Система безопасности значимого объекта КИИ	10
Взаимодействие с ГосСОПКА	8
Аутсорсинг услуг	4
Подготовка к лабораторным работам (по 4 часа на каждую работу)	16
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**112**

Заочная форма обучения

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. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (для очной формы обучения)

2. Отчеты обучающихся по лабораторным работам.

3. Банк тестовых заданий к рубежным контролям № 1, № 2 (для очной формы обучения).

4. Вопросы к зачету.

6.2 Система балльно-рейтинговой оценки работы обучающихся по дисциплине (для очной формы обучения)

№	Наименование	Содержание					
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторных работ	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$2_б$ х 8 =$16_б$	$8_б$ х 4 = $32_б$	10	12	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачете	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично					

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контролей не менее 51 балла. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежных контролей. При этом, на усмотрение преподавателя, балльная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог балльной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 51 балла, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3 Процедура оценивания результатов освоения дисциплины

Очная форма обучения

Мероприятия текущего контроля проводятся на аудиторных занятиях в соответствии с расписанием.

Основной вид текущего контроля результатов освоения дисциплины - защита отчетов по выполненным лабораторным работам.

В процессе защиты отчетов оценивается уровень понимания обучающимися методики проведения работы, полнота и качество выполнения заданий, а также обоснованность выводов, сделанных обучающимся по результатам выполнения заданий.

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 10 и 12 вопросов соответственно. На каждое тестирование при рубежном контроле обучающемуся отводится 1 академический час.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании.

Зачет проводится в форме устного ответа на 2 вопроса. Билет состоит из 2 вопросов. Перечень вопросов преподаватель выдает заранее. Время, отводимое обучающемуся на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

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

Заочная форма обучения

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 рубежных контролей и зачета

Примерные тестовые задания для рубежного контроля №1

1) Можно ли создавать разные комиссии для категорирования объектов КИИ в филиалах территориально распределенной организации?

а) да

б) нет

2) Какие из этих описаний характеризует распределенные DoS-атаки?

а) это злонамеренные действия, выполняемые для запрещения легальному пользователю доступа к системе, сети, приложению или информации;

б) для осуществления атаки система-отправитель посылает огромное количество TCP SYN-пакетов (пакетов с синхронизирующими символами) к системе-получателю, игнорируя ACK-пакеты, добиваясь переполнения буфера очереди соединений

в) в осуществлении атаки участвует большое количество систем, которыми управляет одна главная система и один хакер. Выход системы из строя достигается путем огромного объема передаваемых данных.

3) Способами обнаружения активных сетевых узлов являются:

а) Ping-разведка;

б) ARP-разведка;

в) TCP-разведка;

г) SMTP-разведка;

д) POP3-разведка.

Примерные тестовые задания для рубежного контроля №2

1) Согласно государственным стандартам определение состояния системы, процесса или работы — это …

а) мониторинг;

б) измерение;

в) доступность;

г) аудит.

2) Согласно государственным стандартам одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают информационной безопасности — это …

а) событие информационной безопасности;

б) инцидент информационной безопасности;

в) менеджмент информационной безопасности;

г) оценка информационной безопасности.

3) Силами ФСБ России создаются:

а) главный центр ГосСОПКА,

б) региональные центры ГосСОПКА

в) территориальные центры ГосСОПКА

г) центры ГосСОПКА органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации

д) корпоративные центры ГосСОПКА

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 блокирование (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, рубежных контролей 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 СИСТЕМ

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

При чтении лекций используются слайдовые презентации.

Минимальные требования к программному обеспечению компьютера, используемого при показе слайдовых презентаций: офисный пакет LibreOffice (лицензия Mozilla Public License Version 2.0).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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: **очная, заочная**

Трудоемкость дисциплины: 4 ЗЕ (144 академических часа)
Семестры: 3-й (для очной формы обучения)
3-й (для заочной формы обучения)
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.

ЛИСТ
регистрации изменений (дополнений)
в рабочую программу 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: **очная, заочная**

Изменения / дополнения в рабочую программу
на 20__ / 20__ учебный год:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Ответственный преподаватель _____ / Д.И.Дик /

Изменения утверждены на заседании кафедры БИАС «___»_____20__ г., Протокол № ___

Заведующий кафедрой _____ / Д.И.Дик /