Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Безопасность критической информационной инфраструктуры объектов энергетики

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.1 Администрирует системы защиты информации автоматизированных систем

ПК-1.2 Управляет защитой информации в автоматизированных системах

ПК-1.3 Выполняет мониторинг защищенности информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Защита задания

1. Контрольное задание 1 (Деловая игра)
2. Контрольное задание 2 (Деловая игра)

Форма реализации: Письменная работа

1. Контрольная работа 1 (Контрольная работа)
2. Тест (Тестирование)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Организация защиты информации на объектах КИИ					
Правовое регулирование безопасности объектов КИИ		+		+	
Категорирование объектов КИИ		+		+	
Энергетика как сфера функционирования КИИ.		+		+	
Обеспечение безопасности значимых объектов КИИ.			+	+	
Концепция цифровой электрической подстанции (ЦПС)					
Основы государственной политики в сфере энергетической безопасности.		+		+	
Основы цифровизации энергетики.			+		

Концепция цифровой электрической подстанции на основе открытого объектно-ориентированного стандарта МЭК-61850.	+			+
Структура программно- технического комплекса ЦПС.		+		
Направления совершенствования защиты объектов энергетики от кибератак и деструктивного воздействия.		+		
Организация и управление безопасностью объектов КИИ энергетики				
Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).			+	
Организация сбора информации о событиях от ЦПС.			+	
Программно-аппаратные решения безопасности российских производителей для объектов КИИ энергетики.			+	
Перспективы развития программного и программно-аппаратного обеспечения безопасности объектов КИИ энергетики.		+		
Вес КМ:	20	20	30	30

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ПК-1.1$_{ПК-1}$ Администрирует системы защиты информации автоматизированных систем	Знать: возможности программных и технических средств мониторинга защищенности объектов КИИ; перечень требований защиты информации на объектах КИИ; Уметь: планировать мероприятия мониторинга защищенности объектов КИИ	Контрольное задание 2 (Деловая игра) Контрольное задание 1 (Деловая игра)
ПК-1	ПК-1.2$_{ПК-1}$ Управляет защитой информации в автоматизированных системах	Знать: правила категорирования объектов КИИ энергетики; правовые основы защиты информации на объектах КИИ; Уметь: выполнять основные работы по категорированию объектов КИИ энергетики;	Контрольная работа 1 (Контрольная работа) Контрольное задание 1 (Деловая игра)

		формировать перечень и последовательность выполнения мероприятий по защите КИИ объектов энергетики;	
ПК-1	ПК-1.3$_{ПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах	Знать: основы концепции цифровой электрической подстанции (ЦПС); ланшафт угроз объектам КИИ энергетики и основные векторы атак на них; Уметь: правильно применять требования правовых и нормативных документов для обеспечения безопасности объектов КИИ выполнять основные процедуры, анализировать информацию мониторинга и разрабатывать рекомендации по результатам анализа	Контрольная работа 1 (Контрольная работа) Контрольное задание 2 (Деловая игра) Контрольное задание 1 (Деловая игра) Тест (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполнение письменной контрольной работы в течении 50 минут.

Краткое содержание задания:
Правовые основы защиты информации на объектах КИИ. Система законодательный и нормативно-правовых актов по защите объектов КИИ

Контрольные вопросы/задания:

Знать: правовые основы защиты информации на объектах КИИ;	1.Общая характеристика системы законодательных и нормативно-правовых актов по защите объектов КИИ
Знать: основы концепции цифровой электрической подстанции (ЦПС);	1.Порядок и технология категорирования объектов КИИ
Уметь: выполнять основные работы по категорированию объектов КИИ энергетики;	1.Особенности защиты объектов КИИ энергетической отрасли

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны полные и правильные ответы на вопросы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны правильные и достаточно полные ответы на вопросы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Даны в основном правильные ответы на вопросы, но имеется недостаточная их полнота

КМ-2. Контрольное задание 2

Формы реализации: Защита задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Защита результатов деловой игры проводится в рабочей группе (3-4 человека).

Краткое содержание задания:
Организация мониторинга защищенности объекта КИИ энергетики (на примере ЦПС) на основе анализа событий безопасности

Контрольные вопросы/задания:

Знать: возможности программных и технических средств мониторинга защищенности объектов КИИ;	1.Каким образом организован сбор информации о событиях безопасности ЦПС?
Знать: перечень требований защиты информации на объектах КИИ;	1.Какие программные (программно-аппаратные) средства используются для сбора событий безопасности?
Уметь: выполнять основные процедуры, анализировать информацию мониторинга и разрабатывать рекомендации по результатам анализа	1.Порядок распределения обязанностей в группе при организации мониторинга безопасности ЦПС. 2.Порядок и последовательность анализа событий безопасности ЦПС.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Анализ выполнен правильно, рекомендации разработаны адекватно

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Анализ выполнен в целом правильно, рекомендации разработаны адекватно

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Анализ выполнен с наличием неточностей, адекватность рекомендации сомнительна

КМ-3. Контрольное задание 1

Формы реализации: Защита задания
Тип контрольного мероприятия: Деловая игра
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Защита результатов деловой игры проводится в рабочей группе (3-4 человека).

Краткое содержание задания:
Разработка модели угроз для типового объекта КИИ энергетики (на примере ЦПС).

Контрольные вопросы/задания:

Знать: правила категорирования объектов КИИ энергетики;	1.Представление угроз, актуальных для объектов КИИ в Банке угроз ФСТЭК России
Знать: правовые основы защиты информации на объектах КИИ;	1.Порядок оценки актуальности угроз для объектов КИИ
Знать: ланшафт угроз объектам КИИ энергетики и основные векторы атак на них;	1.Каков перечень угроз безопасности объекта КИИ?
Уметь: планировать мероприятия мониторинга защищенности объектов КИИ	1.Разработка основных разделов модели угроз для объекта КИИ энергетики
Уметь: формировать перечень и	1.Какова практическая значимость модели угроз для

последовательность выполнения мероприятий по защите КИИ объектов энергетики;	организации системы безопасности объектов КИИ?
Уметь: правильно применять требования правовых и нормативных документов для обеспечения безопасности объектов КИИ	1.Что включает в себя модель угроз? 2.Какова цель моделирования угроз безопасности?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Модель угроз выполнена полно. качественно, профессиональным языком и в профессиональной терминологии. Особенности объектов КИИ энергетики учтены. В модели присутствуют элементы формализации (условных обозначений) угроз безопасности

Оценка: не зачтено
Описание характеристики выполнения знания: Нет оснований для оценки работы "зачтено"

КМ-4. Тест

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Тест выполняется в письменном виде во время из расчета 1 минута на ответ 1 вопроса. Тема: Цифровая электрическая подстанция (ЦПС). Концепция, организация информационного обмена на основе промышленных протоколов. Обеспечение безопасности

Краткое содержание задания:

1. Какая система из перечисленных в КСОБ ЦПС является лишней?
1 − система сбора и обработки информации (ССОИ);
2 − система охранного телевидения (СОТ);
3 − система экологической безопасности (СЭБ);
4 − система контроля и управления доступом (СКУД);
5 − система информационной безопасности.

2. Каков сохраняемый объем информации СКУД при пропадании напряжения на объекте, событий?
1. 100
2. 500
3. 1000
4. 1500
5. 2000

3. Каково минимальное количество технических средств с различными физическими принципами в системе периметровой охранной сигнализации?
1. 1
2. 2
3. 3
4. 4

4. Какая информация ПТК ЦПС не относится к защищаемой?

1. Обрабатываемая информация;
2. Персональные данные сотрудников.
3. Программные настройки технических средств;
4. Значения настраиваемых параметров средств защиты.

5. Каким средствам защиты информации отдается приоритет в соответствии?

1. Приобретенным
2. Стандартным
3. Встроенным
4. Организационным

Контрольные вопросы/задания:

Знать: основы концепции цифровой электрической подстанции (ЦПС);	1.Вопросы теста сформированы на основе содержания документа СТО 34.01 -21-004-2019 “Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ”

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны правильные ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Даны правильные ответы

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ «МЭИ»	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1 Кафедра *Безопасности и информационных технологий* Дисциплина Безопасность критической информационной инфраструктуры объектов энергетики	***Утверждаю:*** Зам. зав. кафедрой БИТ _____/*О.Р.Баронов*/ *Протокол заседания кафедры № ___* *«___» _____ 20___ г.*
1. Понятие критической информационной инфраструктуры. Перечень задач по обеспечению безопасности критической информационной инфраструктуры .(на примере объектов энергетики). 2. Порядок работы по категорированию объектов КИИ (на примере объектов энергетики). 3. Провести анализ событий безопасности, полученных от системы мониторинга ЦПС, сформировать выводы и дать рекомендации по уровню безопасности объекта КИИ. (Выполняется на основе дополнительного задания).		

Процедура проведения

Выполняется в письменном виде в течении 50 минут по экзаменационным билетам

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ПК-1.1$_{ПК-1}$ Администрирует системы защиты информации автоматизированных систем

Вопросы, задания

1.Общее содержание ФЗ-187 от 26.07.2017г. «О безопасности критической информационной инфраструктуры РФ». Основные положения: субъекты и объекты КИИ, понятия, типы и виды.

2.Нормативное регулирование безопасности объектов КИИ на основе положений приказа ФСТЭК России №239 от 25.12.2017. Состав мер безопасности значимых объектов КИИ в соответствии с их категорией значимости.

Материалы для проверки остаточных знаний

1.Понятие критической информационной инфраструктуры.

Ответы:

Ответы должны содержать формулировки, близкие по содержанию с официальными источниками (законы, приказы регуляторов и аналогичные). Приветствуется указание источника формулировки и его реквизитов.

Верный ответ: Критическая информационная инфраструктура (сокращенно - КИИ) - это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети

электросвязи, используемые для организации их взаимодействия. Под субъектами КИИ понимают компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ. Компьютерная атака на КИИ определяется как целенаправленное вредоносное воздействие на объекты КИИ для нарушения или прекращения их функционирования, а компьютерный инцидент - как факт нарушения или прекращения функционирования объекта КИИ и/или нарушения безопасности обрабатываемой объектом информации.

2.Что включает в себя система законодательства в области безопасности объектов КИИ?

Ответы:

Необходимо наиболее полно перечислить законодательные и нормативные акты и дать им краткую характеристику

Верный ответ: Федеральный закон 187-ФЗ “О безопасности критической информационной инфраструктуры РФ” Постановление Правительства 127 "Об утверждении правил категорирования КИИ…..” Постановление правительства 162 “Об утверждении правил государственного контроля в области обеспечения безопасности ЗО КИИ РФ" Ппиказ ФСТЭК № 227 Приказ ФСТЭК №236 Приказ ФСТЭК №235 Приказ ФСТЭК №239 Приказ ФСТЭК №229 Приказ ФСБ №№ 336, 367, 368, 281, 282

2. Компетенция/Индикатор: ПК-1.2$_{ПК-1}$ Управляет защитой информации в автоматизированных системах

Вопросы, задания

1.Общая характеристика системы законодательства в области безопасности объектов КИИ

Материалы для проверки остаточных знаний

1.Понятие значимых объектов КИИ и их категории

Ответы:

Необходимо дать полное определение ЗО КИИ и перечислить категории значимости

Верный ответ: Значимый объект критической информационной инфраструктуры — объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры; информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Выделяются 3 категории значимости объектов КИИ: первая, вторая и третья.

3. Компетенция/Индикатор: ПК-1.3$_{ПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах

Вопросы, задания

1.Понятие значимых объектов КИИ и их категории. Перечень объектов КИИ: ИС, АСУ, ИТКС.

2.Анализ угроз безопасности объектам КИИ энергетики и последствий реализации угроз. Анализ современного уровня цифровизации энергетики и перспективы ее цифровой трансформации.

Материалы для проверки остаточных знаний

1.Состав мер безопасности значимых объектов КИИ в соответствии с их категорией значимости.

Ответы:

Необходимо перечислить категории мер безопасности и дать им общую характеристику

Верный ответ: В значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры: идентификация и аутентификация (ИАФ); управление доступом (УПД); ограничение программной среды (ОПС); защита машинных носителей информации (ЗНИ); аудит безопасности (АУД); антивирусная защита (АВЗ); предотвращение вторжений (компьютерных атак) (СОВ); обеспечение целостности (ОЦЛ); обеспечение доступности (ОДТ); защита технических средств и систем (ЗТС); защита информационной (автоматизированной) системы и ее компонентов (ЗИС); планирование мероприятий по обеспечению безопасности (ПЛН); управление конфигурацией (УКФ); управление обновлениями программного обеспечения (ОПО); реагирование на инциденты информационной безопасности (ИНЦ); обеспечение действий в нештатных ситуациях (ДНС); информирование и обучение персонала (ИПО)

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Полностью правильно, источник правильно указан.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Правильно передан смысл.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Смысл ответа можно оценить, полноты ответа нет.

III. Правила выставления итоговой оценки по курсу

Итоговая оценка по курсу выставляется исходя из положений системы БАРС как семестровая и экзаменационная составляющая