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

Направление подготовки/специальность: 13.04.02 Электроэнергетика и электротехника

Наименование образовательной программы: Интеллектуальные системы защиты, автоматики и управления энергосистемами

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Основы кибербезопасности РЗА энергосистем

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Карантаев В.Г. Идентификатор: Rb72a6d42-KarantayevVG-03f56ea	В.Г. Карантаев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Волошин А.А. Идентификатор: Ra915003b-VoloshinAA-408ebd73	А.А. Волошин
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Волошин А.А. Идентификатор: Ra915003b-VoloshinAA-408ebd73	А.А. Волошин

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-2 Способен осуществить информационный обмен между устройствами релейной защиты и автоматики

ИД-1 Демонстрирует знание протоколов информационного обмена

ИД-2 Демонстрирует знание нормативно-технической документации

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА (Отчет)
2. КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850 (Отчет)
3. КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА (Отчет)
4. КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты (Отчет)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА					
Основы информационной безопасности. Понятия, определения		+			
Программная защита информации устройств РЗА		+			
Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»					
Способы обеспечения защиты информации			+		
Организационные меры защиты информации			+		
Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты					
Особенности реализации защиты устройств РЗА				+	
Техническая защита информации устройств РЗА				+	

Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850				
Криптографические методы защиты информации				+
Программно-технические меры защиты информации				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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-2	ИД-1$_{ПК-2}$ Демонстрирует знание протоколов информационного обмена	Знать: принципы передачи информации между РЗА технические средства реализации протоколов передачи данных устройств РЗА Уметь: настраивать защищенные соединения РЗА шифровать программное обеспечение устройств РЗА	КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА (Отчет) КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты (Отчет)
ПК-2	ИД-2$_{ПК-2}$ Демонстрирует знание нормативно-технической документации	Знать: способы защиты информации устройств РЗА возможные уязвимости и точки проникновения устройств РЗА Уметь: на основе анализа находить решения по защите от проникновения РЗА	КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА (Отчет) КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850 (Отчет)

		выстраивать модель уязвимостей РЗА	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Работа выполняется в соответствии с методическими указаниями к выполнения лабораторной работы. Защита лабораторной работы выполняется по отчету о выполнении лабораторной работы

Краткое содержание задания:
Настройка защищенного соединения между устройствами РЗА

Контрольные вопросы/задания:

Знать: принципы передачи информации между РЗА	1. Какое соединение между устройствами РЗА можно считать защищенным 2. Что такое локально вычислительная сеть
Знать: технические средства реализации протоколов передачи данных устройств РЗА	1. Какова структура построения защищенной локально вычислительной сети на ПС? 2. Какие основные особенности построения ЛВС на подстанции

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка «ОТЛИЧНО» выставляется студенту, правильно выполнившему практическое задание, который показал при ответе на вопросы экзаменационного билета и на дополнительные вопросы, что владеет материалом изученной дисциплины, свободно применяет свои знания для объяснения различных явлений и решения задач

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка «ХОРОШО» выставляется студенту, правильно выполнившему практическое задание и в основном правильно ответившему на вопросы экзаменационного билета и на дополнительные вопросы, но допустившему при этом непринципиальные ошибки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который в ответах на вопросы экзаменационного билета допустил существенные и даже грубые ошибки, но затем исправил их сам, а также не выполнил практическое задание из экзаменационного билета, но либо наметил правильный путь его выполнения, либо по указанию экзаменатора решил другую задачу из того же раздела дисциплины

Оценка: 2
Описание характеристики выполнения знания: Оценка «НЕУДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который: а) не ответил на вопросы экзаменационного билета и не

смог решить, либо наметить правильный путь решения задачи из билета; б) не смог решить, либо наметить правильный путь решения задачи из экзаменационного билета и другой задачи на тот же раздел дисциплины, выданной взамен нее; в) при ответе на дополнительные вопросы обнаружил незнание большого раздела экзаменационной программы

КМ-2. КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Работа выполняется в соответствии с методическими указаниями к выполнения лабораторной работы. Защита лабораторной работы выполняется по отчету о выполнении лабораторной работы.

Краткое содержание задания:
Обеспечение защиты информации и конфигурационных файлов устройств РЗА

Контрольные вопросы/задания:

Знать: возможные уязвимости и точки проникновения устройств РЗА	1.Что такое защита информации 2.Какие меры защиты информации вы знаете
Знать: способы защиты информации устройств РЗА	1.Что такое файрволл 2.Дайте понятие определению демилитаризованная зона

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Работа выполняется в соответствии с методическими указаниями к выполнения лабораторной работы. Защита лабораторной работы выполняется по отчету о выполнении лабораторной работы

Краткое содержание задания:
Взлом и подмена настроек устройств релейной защиты

Контрольные вопросы/задания:

Уметь: настраивать защищенные соединения РЗА	1.Что такое демилитаризованная зона
Уметь: шифровать программное обеспечение устройств РЗА	1.Кто являлся внутренним нарушителем при осуществлении данной атаки 2.Кто являлся внешним нарушителем при осуществлении данной атаки

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Работа выполняется в соответствии с методическими указаниями к выполнения лабораторной работы. Защита лабораторной работы выполняется по отчету о выполнении лабораторной работы

Краткое содержание задания:
Криптозащита передачи данных по протоколу МЭК61850

Контрольные вопросы/задания:

Уметь: выстраивать модель уязвимостей РЗА	1.Какие методы защиты информации предусмотрены протоколом МЭК61850 2.Каким образом осуществляется контроль целостности информации при использовании криптографического метода защиты
Уметь: на основе анализа находить решения по защите от проникновения РЗА	1.Какие основные особенности асимметричного метода криптографической защиты информации 2.Какие основные отличия симметричного и ассиметричного методов криптографической защиты информации

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Из каких документов складывается нормативно-правовое регулирование в сфере безопасности объектов КИИ Электроэнергетики 2. Классификация криптографических алгоритмов

Процедура проведения

Проводится в письменной и устной форме по билетам в виде решения задачи и изложения развернутого ответа. Время на выполнение экзаменационного задания/подготовку ответа – 60 минут

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

1. Компетенция/Индикатор: ИД-1$_{ПК-2}$ Демонстрирует знание протоколов информационного обмена

Вопросы, задания

1.

1. Раскрыть понятие Информационная безопасность
2. Раскрыть понятие целостности данных. Привести примеры теоретических способов мер защиты для протокола GOOSE

2.

1. Раскрыть понятие Кибербезопасность
2. Раскрыть понятие идентификация, аутентификация, авторизация. Привести классификацию. Привести основные способы реализации

3.

1. Свойства информации в контексте обеспечения информационной безопасности
2. Классификация криптографических алгоритмов

4.

1. Объяснить структуру нормативно-правого регулирования в сфере защиты информации
2. Электронная цифровая подпись. Функция хэширования

5.

1. Объяснить структуру нормативно-правого регулирования в сфере защиты информации
2. Асимметричные криптосистемы шифрования

Материалы для проверки остаточных знаний

1. **По методам анализа СОВ бывают следующих видов**

   Ответы:

a. Сигнатурный
b. Статистический
c. Реального времени
d. Активные

Верный ответ: a. Сигнатурный b. Статистический

2. **Что в переводе с греческого языка означает слово «криптография»**

Ответы:

a. Шифр
b. Тайнопись
c. Преобразование
d. Расшифровка

Верный ответ: b. Тайнопись

3. **Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства**

Ответы:

a. Шифр Маркова
b. Шифр Цезаря
c. Шифр Энигма
d. Шифр Бэбиджа

Верный ответ: b. Шифр Цезаря

4.**Какие ключи используются в системах с открытым ключом**

Ответы:

a. Открытый
b. Закрытый
c. Секретный
d. Нет правильного ответа

Верный ответ: a. Открытый b. Закрытый

5. **Отметьте, что используется для создания цифровой подписи**

Ответы:

1. Отметьте, что используется для создания цифровой подписи
a. Закрытый ключ отправителя
b. Закрытый и открытый ключи отправителя
c. Общий секретный ключ отправителя и получателя
d. Открытый ключ отправителя

Верный ответ: Закрытый ключ отправителя

2. Компетенция/Индикатор: ИД-2$_{ПК-2}$ Демонстрирует знание нормативно-технической документации

Вопросы, задания

1.

1. Раскрыть понятие Защита информации
2. Понятие и классификация атак на информационные системы Традиционная и распределенная атака. APT – атака

2.

1. Раскрыть понятие комплексности требований для систем класса IIoT в Электроэнергетике

2. Симметричные криптосистемы шифрования

3.

1. Раскрыть понятие нормативно-правого и нормативно-технического регулирования
2. Объяснить роль и место SOC в анализе защищенности, обнаружении и реагировании на компьютерные атаки в в автоматизированных системах управления, системах релейной защиты и противоаварийной автоматики активно-адаптивных сетей (Smart Grid)

4.

1. Из каких документов складывается нормативно-правовое регулирование в сфере безопасности объектов КИИ Электроэнергетики
2. Раскрыть сущность методологического подхода к моделированию угроз MITRE’s Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK™)

5.

1. Представить общую информацию о структуре нормативно-технического регулирования кибербезопасности SmartGrid
2. Привести примеры применения СОА/СОВ на ЦПС. На примере любого варианта структурной схемы

Материалы для проверки остаточных знаний

1. **Дайте полное определение что такое межсетевой экран**

   Ответы:

a. Специализированное аппаратное устройство со встроенной ОС
b. Аппаратно-программное устройство для фильтрации трафика
c. Локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей и/или выходящей из автоматизированной системы, и обеспечивает защиту посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении
d. технологический барьер, предназначенный для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостами

   Верный ответ: c. Локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей и/или выходящей из автоматизированной системы, и обеспечивает защиту посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении

2. **В каком исполнении могут быть межсетевые экраны**

   Ответы:

a. Только программное
b. Только аппаратно-программное
c. В зависимости от типа исполнение может быть как программным, так и аппаратно-программным

   Верный ответ: c. В зависимости от типа исполнение может быть как программным, так и аппаратно-программным

3. **Межсетевые экраны для защиты отдельных конечных точек (настольных компьютеров, ноутбуков и серверов) являются**

   Ответы:

a. Исключительно программными
b. Аппаратно-программными средствами защиты
c. Не могут быть встроенными в ОС, которую они защищают; всегда реализованы внешними производителями
Всегда встроены в ОС, которую они защищают; не могут быть реализованы внешними производителями
Верный ответ: a. Исключительно программными

4. **При использовании СОВ появляются следующие преимущества**
Ответы:

a. Возрастает возможность фильтрования трафика
b. Возрастает возможность определения оптимального маршрута для каждого кадра
c. Возрастает возможность определения преамбулы атаки
d. Возрастает возможность раскрытия осуществленной атаки
Верный ответ: c. Возрастает возможность определения преамбулы атаки d. Возрастает возможность раскрытия осуществленной атаки

5. **СОВ может обеспечивать следующие возможности**
Ответы:

a. Возможность аутентификации пользователей
b. Возможность определения внутренних угроз
c. Возможность сканирования портов
d. Возможность блокировать атаку, если есть функционал предотвращения вторжений
Верный ответ: b. Возможность определения внутренних угроз d. Возможность блокировать атаку, если есть функционал предотвращения вторжений

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

Промежуточная аттестация по итогам освоения дисциплины: средняя оценка по всем оценочным средствам на каждой контрольной неделе. Оценки за все контрольные недели используется при допуске к экзамену