МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

Подписан: ФГБОУ ВО «КГЭУ», КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСИЙ УНИВЕРСИТЕТ
Владелец: Гибадуллин Рамил Рифатович, Директора института электроэнергетики и электроники,
Сертификат: 141EBA4A321BD0AF4F90D509019D90D0
Действителен с 15.04.2026 по 18.04.2027

УТВЕРЖДАЮ
Директор
Института электроэнергетики и электроники

_____Р.Р. Гибадуллин

« 24 » февраля 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.01.01.01 Кибербезопасность

Направление подготовки 13.04.02 Электроэнергетика и электротехника

Направленность (профиль) Цифровая автоматизация и роботизация в энергетике

Квалификация Магистр

г. Казань, 2026

Программу разработал(и):

Наименование кафедры	Должность, уч.степень, уч.звание	ФИО разработчика
ТОЭ	Доцент, к.т.н.	Вассунова Ю.Ю.

Согласование	Наименование подразделения	Дата	№ протокола	Подпись
Одобрена	Кафедра – разработчик «Теоретические основы электротехники»	28.01.2026	№7	Зав. кафедрой, д.т.н, профессор Садыков М.Ф.
Согласована	Выпускающая кафедра – «Теоретические основы электротехники»	28.01.2026	№7	Зав. кафедрой, д.т.н, профессор Садыков М.Ф.
Согласована	Учебно-методический совет ИЭЭ	24.02.2026	№5	Директор ИЭЭ, к.т.н., доцент Гибадуллин Р.Р.
Одобрена	Ученый совет ИЭЭ	24.02.2026	№6	Директор ИЭЭ, к.т.н., доцент Гибадуллин Р.Р.

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины является формирование у студентов комплекса теоретических знаний и практических навыков по обеспечению кибербезопасности объектов критической информационной инфраструктуры в электроэнергетике, включая цифровые подстанции, АСУ ТП и системы автоматизации

Задачами дисциплины являются:

- изучение нормативно-правовой базы и стандартов (включая серию ISO/IEC 27000, приказы ФСТЭК) в области защиты КИИ ;
- анализ архитектуры, основных угроз и уязвимостей киберфизических систем в энергетике;
- освоение методов и средств защиты (криптография, межсетевое экранирование, обнаружение вторжений) для АСУ ТП и устройств РЗА ;
- формирование способности проектировать сегменты защищенных сетей и оценивать риски информационной безопасности на объектах энергетики

Компетенции и индикаторы, формируемые у обучающихся:

Код и наименование компетенции	Код и наименование индикатора
ПК-1 Способен осуществлять эксплуатацию, развитие и цифровую трансформацию систем автоматизации и управления технологическими процессами (АСУ ТП) энергообъектов	ПК-1.6 Демонстрирует понимание построения и обеспечения кибербезопасной эксплуатации сетевой инфраструктуры систем управления и контроля энергообъектов

2. Место дисциплины в структуре ОП

Предшествующие дисциплины (модули), практики, НИР, др.

Б1.В.03 Эксплуатация и техническое обслуживание систем автоматизации

Б1.В.02 Программируемые логические контроллеры автоматизированных систем

Последующие дисциплины (модули), практики, НИР, др.

Б1.В.04 Виртуальное проектирование и цифровые двойники

Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Для очной формы обучения

Вид учебной работы	Всего ЗЕ	Всего часов	Семестр(ы)		
			1		
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	3	108	108		
КОНТАКТНАЯ РАБОТА*	-	32	32		
АУДИТОРНАЯ РАБОТА	0,7	24	24		
Лекции	0,2	8	8		
Практические (семинарские) занятия	0,5	16	16		
Лабораторные работы	-	-	-		
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	2,3	84	84		

Проработка учебного материала	2,3	84	84		
Курсовой проект					
Курсовая работа					
Подготовка к промежуточной аттестации					
Промежуточная аттестация:			З		
			-		

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	Всего часов	Распределение трудоемкости				Формы и вид контроля	Индексы индикаторов формируемых компетенций
		лекции	лаб. раб.	пр. зан.	сам. раб.		
Раздел 1. Введение в кибербезопасность энергосистем	30	2	-	4	24	ТК1	**ПК-1.6.З** **ПК-1.6.У** **ПК-1.6.В**
Раздел 2. **Технические средства и архитектура защиты**	46	4	-	8	34	ТК2	**ПК-1.6.З** **ПК-1.6.У** **ПК-1.6.В**
Раздел 3. **Организационное обеспечение и управление инцидентами**	32	2	-	4	26	ТК3	**ПК-1.6.З** **ПК-1.6.У** **ПК-1.6.В**
Зачет	0				0	**ОМ**	**ПК-1.6.З** **ПК-1.6.У** **ПК-1.6.В**
ИТОГО	**108**	**8**	-	16	**84**		

3.3. Содержание дисциплины

РАЗДЕЛ 1. Введение в кибербезопасность энергосистем

Тема 1.1. Цифровая трансформация и киберфизические системы в энергетике. Понятие киберфизических систем (КФС). Архитектура цифровой подстанции и АСУ ТП как объектов кибербезопасности. Взаимосвязь информационных и физических процессов. Особенности обеспечения безопасности в энергетике по сравнению с корпоративным сектором.

Тема 1.2. Нормативно-правовое регулирование. Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»: субъекты и объекты КИИ, обязанности субъектов. Приказы ФСТЭК (№31, №239 и др.): требования к организации и техническим мерам защиты. Обзор стандартов ISO/IEC 27001 и серии IEC 62443.

РАЗДЕЛ 2. Технические средства и архитектура защиты

Тема 2.1. Уязвимости протоколов и архитектура АСУ ТП. Стек протоколов МЭК 61850 (GOOSE, MMS, SV): особенности, достоинства и проблемы безопасности. Протокол Modbus: отсутствие аутентификации и шифрования. Типовые архитектурные ошибки при построении сетей АСУ ТП.

Тема 2.2. Средства криптографической защиты информации. Основы криптографии для АСУ ТП: шифрование каналов связи, электронная подпись для команд управления. Понятие встраиваемых СКЗИ. Особенности внедрения криптографии в промышленные сети с жесткими требованиями к задержкам.

Тема 2.3. Сетевые средства защиты. Межсетевые экраны промышленного исполнения (NGFW) с функцией глубокого анализа трафика (DPI) промышленных протоколов. Системы обнаружения и предотвращения вторжений (IDS/IPS) для АСУ ТП. Выделение демилитаризованных зон (DMZ). Технологии VLAN и списки доступа (ACL) для сегментации.

РАЗДЕЛ 3. Организационное обеспечение и управление инцидентами

Тема 3.1. Управление рисками информационной безопасности на объектах ТЭК. Понятие и методы оценки рисков ИБ (количественные и качественные оценки). Этапы управления рисками: идентификация, анализ, оценка, обработка. Критерии приемлемости риска для объектов энергетики.

Тема 3.2. Реагирование на инциденты и социальная инженерия. Жизненный цикл реагирования на инциденты: обнаружение, сдерживание, устранение, восстановление. Особенности расследования инцидентов в АСУ ТП (компьютерная криминалистика/форензика). Социальная инженерия как угроза: методы атак и методы противодействия персоналу.

3.4. Тематический план практических занятий

1. Анализ технического задания на АСУ ТП типового энергообъекта (распределенная подстанция, микрогрид). Выбор аппаратной платформы ПЛК.
2. Разработка программы управления на языке FBD/LD в среде CODESYS. Управление схемой собственных нужд подстанции.
3. Создание простой SCADA-страницы (HMI). Визуализация мнемосхемы управления, настройка аварийных сигналов.

4. Моделирование работы цифровой системы в целом. Запуск проекта (ПЛК + HMI), тестирование логики, анализ реакции на аварийные ситуации.

3.5. Тематический план лабораторных работ

«Данный вид работы не предусмотрен учебным планом».

3.6. Курсовой проект /курсовая работа

«Данный вид работы не предусмотрен учебным планом».

4. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности индикатора компетенции			
			Высокий	Средний	Ниже среднего	Низкий
			от 85 до 100	от 70 до 84	от 55 до 69	от 0 до 54
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено			не зачтено
ПК-1	ПК-1.6	знать:				
		Знает теоретические и нормативные основы кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Свободно владеет теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	В основном знает теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Частично знает теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Не знает теоретическим и нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты
		уметь:				

		Умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для выявления и расследования инцидентов	Свободно умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов)	В основном умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов)	Не всегда умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов)	Не умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов
		владеть:				
		Владеет **инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).**	Уверенно владеет **инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).**	Владеет **инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).**	Частично владеет **инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).**	Не владеет **инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и**

Оценочные материалы для проведения текущего контроля и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины.

Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре разработчика.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Учебно-методическое обеспечение

5.1.1. Основная литература

1. Баланов, А. Н. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 680 с. — ISBN 978-5-507-52709-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/457463.
2. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 280 с. — ISBN 978-5-507-56255-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/514704.
3. Краковский Ю. М. Методы и средства защиты информации : учебное пособие / Ю. М. Краковский. - 2-е изд., стер. - Санкт-Петербург : Лань, 2025. - 271 с. - URL: https://e.lanbook.com/book/463013. - ISBN 978-5-507-52958-2. - Текст : электронный.
4. Крылов, Г. О. Базовые понятия информационной безопасности : учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва : Русайнс, 2025. — 257 с. — ISBN 978-5-466-09255-4. — URL: https://book.ru/book/958467. — Текст : электронный.

5.1.2. Дополнительная литература:

1. Рацеев С. М. Криптография. Безопасные многосторонние вычисления : учебное пособие / С. М. Рацеев. - 2-е изд., испр. и доп. - Санкт-Петербург : Лань, 2025. - 538 с. - URL: https://e.lanbook.com/book/505598. - ISBN 978-5-507-53156-1. - Текст : электронный.

2. Бабаш А. В. Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. - Москва : Кнорус, 2026. - 189 с. - URL: https://book.ru/books/959208. - ISBN 978-5-406-14904-1. - Текст : электронный.

3. Нестеров С. А. Основы информационной безопасности : учебник / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 321 с. - URL: https://e.lanbook.com/book/370967. - ISBN 978-5-507-49077-6. - Текст : электронный.

5.1.3. Нормативные документы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Стандарты серии ГОСТ Р МЭК 62443 «Сети и системы связи на подстанциях»

5.2. Информационное обеспечение

5.2.1. Электронные и интернет-ресурсы

1. Электронно-библиотечная система «Лань» (https://e.lanbook.com/)
2. ДК размещенный в LMS Moodle 3.03. Интернет тренажеры: www.i-exam.ru.

5.2.2. Профессиональные базы данных / Информационно-справочные системы

1. Международная реферативная база данных (http:// link.springer.com).
2. Научная электронная библиотека "eLIBRARY.RU" (http://elibrary.ru/defaultx.asp).
3. Российская государственная библиотека (http://www.rsl.ru)
4. Энциклопедии, словари, справочники (URL: http://www.rubricon.com).

5.2.3. Лицензионное и свободно распространяемое программное обеспечение дисциплины

1. Пользовательская операционная система Windows 10.
2. ПО для эффективного онлайн- взаимодействия преподавателя и студента LMS Moodle. Современное программное обеспечение. https://download.moodle .org/releases/latest/
3. Система поиска информации в сети интернет Браузер Chrome
4. Пакет программ для создания и просмотра файлов формата PD Adobe Acrobat "ИРБИС 64 (модульная поставка): АРМ «Читатель», АРМ "Книговыдача

6. Материально-техническое обеспечение дисциплины

Наименование вида учебной работы	Наименование учебной аудитории, специализтрованной лаборатории	Перечень необходимого оборудования и технических средств обучения
Лекции	Учебная аудитория для проведения занятий лекционного типа	Специализированная учебная мебель, технические средства обучения, служащие для представления учебной информации большой аудитории (мультимедийный проектор, компьютер (ноутбук), экран), демонстрационное оборудование, учебно-наглядные пособия
Практические занятия	Учебная аудитория для проведения занятий семинарского типа, групповых и индивиду-альных консультаций, текущего контроля и	Специализированная учебная мебель, технические средства обучения (мультимедийный проектор, компьютер (ноутбук), экран) и др.
Самостоятельная работа	Компьютерный класс с выходом в Интернет В-600а	Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультиме-дийный проектор, компьютер (ноутбук), экран), видеокамеры, программное

	Читальный зал библиотеки	Специализированная мебель, компьютерная техника с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, экран, мультимедийный проектор, программное обеспечение

6. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно- двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию

устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

7. Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися.

Методическое обеспечение процесса воспитания обучающихся выступает одним из определяющих факторов высокого качества образования. Преподаватель вуза, демонстрируя высокий профессионализм, эрудицию, четкую гражданскую позицию, самодисциплину, творческий подход в решении профессиональных задач, в ходе образовательного процесса способствует формированию гармоничной личности.

При реализации дисциплины преподаватель может использовать следующие методы воспитательной работы:

- методы формирования сознания личности (беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, самоконтроль, рассказ, совет, убеждение и др.);
- методы организации деятельности и формирования опыта поведения (задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение, и др.);
- методы мотивации деятельности и поведения (одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально-нравственных переживаний, соревнование и др.)

При реализации дисциплины преподаватель должен учитывать следующие направления воспитательной деятельности:

Гражданское и патриотическое воспитание:

- формирование у обучающихся целостного мировоззрения, российской идентичности, уважения к своей семье, обществу, государству, принятым в семье и обществе духовно-нравственным и социокультурным ценностям, к национальному, культурному и историческому наследию, формирование стремления к его сохранению и развитию;
- формирование у обучающихся активной гражданской позиции, основанной на традиционных культурных, духовных и нравственных ценностях российского общества, для повышения способности ответственно реализовывать свои конституционные права и обязанности;
- развитие правовой и политической культуры обучающихся, расширение конструктивного участия в принятии решений, затрагивающих их права и интересы, в том числе в различных формах самоорганизации, самоуправления, общественно-значимой деятельности;
- формирование мотивов, нравственных и смысловых установок личности, позволяющих противостоять экстремизму, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам, межэтнической и межконфессиональной нетерпимости, другим негативным социальным явлениям.

Духовно-нравственное воспитание:

- воспитание чувства достоинства, чести и честности, совестливости, уважения к родителям, учителям, людям старшего поколения;
- формирование принципов коллективизма и солидарности, духа милосердия и сострадания, привычки заботиться о людях, находящихся в трудной жизненной ситуации;
- формирование солидарности и чувства социальной ответственности по отношению к людям с ограниченными возможностями здоровья, преодоление психологических барьеров по отношению к людям с ограниченными возможностями;
- формирование эмоционально насыщенного и духовно возвышенного отношения к миру, способности и умения передавать другим свой эстетический опыт.

Культурно-просветительское воспитание:

- формирование эстетической картины мира;
- формирование уважения к культурным ценностям родного города, края, страны;

- повышение познавательной активности обучающихся.

Научно-образовательное воспитание:

- формирование у обучающихся научного мировоззрения;
- формирование умения получать знания;
- формирование навыков анализа и синтеза информации, в том числе в профессиональной области.

Вносимые изменения и утверждения на новый учебный год

№	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» Зав. каф. реализующей	«Согласовано» председатель УМК института (факультета), в состав которого входит выпускающая
1	2	3	4	5	6
1					
2					
3					

Приложение к рабочей программе дисциплины

К Г Э У

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине

Б1. В.ДЭ.01.01.01 Кибербезопасность

Направление подготовки 13.04.02 Электроэнергетика и электротехника

Направленность (профиль) Цифровые системы автоматизации в электроэнергетике

Квалификация Магистр

г. Казань, 2026

Оценочные материалы по дисциплине «**Кибербезопасность**», предназначены для оценивания результатов обучения на соответствие индикаторам достижения компетенций.

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля (ТК) и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

1.Технологическая карта

Семестр 1 (зачет)

Наименование раздела	Формы и вид контроля	Рейтинговые показатели							
		I текущий контроль	Дополнительные баллы к	II текущий контроль	Дополнительные баллы к	III текущий контроль	Дополнительные баллы к	Итого	Промежуточная аттестация
Раздел 1. Введение в кибербезопасность энергосистем	**ТК1**	**10**	**0-15**					**10-25**	**10-25**
Тест		10							
Раздел 2. Технические средства и архитектура защиты	**ТК2**			**20**	**0-15**			**20-35**	**20-35**
Тест				20					
Раздел 3. Организационное обеспечение и управление инцидентами	**ТК3**					**25**	**0-15**	**25-40**	**25-40**
Тест						15			
Реферат (Рфр)						10			
Промежуточная аттестация (зачет)	**ОМ 1**								**0-45**
Задание (вопросы) промежуточной аттестации									0-45

1. Оценочныематериалытекущегоконтроляи промежуточнойаттестации

Шкала оценки результатов обучения по дисциплине:

Код компе-тенции	Код индикатора компетенции	Заплани-рованные результаты обучения по дисциплине	Уровень сформированности индикатора компетенции			
			Высокий	Средний	Ниже среднего	Низкий
			от 85 до 100	от 70 до 84	от 55 до 69	от 0 до 54
			Шкала оценивания			
			отлично	хорошо	удовлет-ворительно	неудов-летвори-тельно
			зачтено			не зачтено
ПК-1 Способен осуществлять эксплуатацию, развитие и цифровую трансформацию систем автоматизации и управления технологическим и процессами (АСУ ТП) энергообъектов	ПК-1.6. Демонстрирует понимание построения и обеспечения кибербезопасной эксплуатации сетевой инфраструктуры систем управления и контроля энергообъектов	знать:				
		Знает теоретические и нормативные основы кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Свободно владеет теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	В основном знает теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Частично знает теоретическими нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты	Не знает теоретическим и нормативными основами кибербезопасности сетей АСУ ТП энергообъектов: архитектуру и протоколы (МЭК 61850, Modbus), актуальные угрозы и уязвимости, средства защиты (межсетевые экраны, IDS/IPS, СКЗИ), а также требования ФЗ-187 и приказов ФСТЭК к безопасной эксплуатации и реагированию на инциденты
		уметь:				

		Умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для выявления и расследования инцидентов	Свободно умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для выявления и	В основном умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для выявления и	Не всегда умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для выявления и	Не умеет проводить комплексный инжиниринг кибербезопасной сетевой инфраструктуры АСУ ТП энергообъектов, включая анализ конфигураций и промышленного трафика (МЭК 61850) для выявления уязвимостей и признаков атак, проектирование сегментации сетей (DMZ, зоны безопасности) с обоснованным выбором средств защиты, настройку сетевого оборудования (коммутаторы, межсетевые экраны) для реализации политик фильтрации, а также интерпретацию журналов событий (логов) IDS/IPS для
		владеть:				

		Владеет инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).	Уверенно владеет инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).	Владеет инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).	Частично владеет инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).	Не владеет инструментально-методическим аппаратом обеспечения кибербезопасности сетевой инфраструктуры АСУ ТП энергообъектов, включая навыки работы со специализированными программными средствами (анализаторы трафика, сканеры уязвимостей, симуляторы сетей), применения методик оценки защищенности и моделирования угроз для выделенных сегментов сети, а также разработки организационно-распорядительной документации (политики безопасности, регламенты настройки и реагирования на инциденты).

Оценка **«Отлично»** выставляется студенту, который обладает всесторонними, систематизированными и глубокими знаниями материала учебной программы, умеет свободно выполнять задания, предусмотренные учебной программой, усвоил основную и ознакомился с дополнительной литературой.

Оценка **«Хорошо»** выставляется студенту, обнаружившему полное знание материала учебной программы, успешно выполняющему предусмотренные учебной программой задания, усвоившему материал основной литературы, рекомендуемой учебной программой.

Оценка **«Удовлетворительно»** выставляется студенту, который показал знание основного материала учебной программы в объеме, достаточном и необходимом для дальнейшей учебы, справился с выполнением заданий, знаком с основной литературой.

Оценка **«Неудовлетворительно»** выставляется студенту, не знающему основной части материала учебной программы, допускающему

принципиальные ошибки в выполнении заданий, неуверенно с большими затруднениями выполняющему практические работы

2. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного	Краткая характеристика оценочного средства	Описание
Реферат (Рфр)	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы	Темы рефератов
Тест (Тест)	Система стандартизированных заданий, позволяющая автоматизировать процедуру	Комплект тестовых заданий

3. Перечень контрольных заданий или иные материалы, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Текущий контроль ТК1:

Проверяемая компетенция: **ПК-1.6.З , ПК-1.6.У, ПК-1.6.В**

ТЕСТ

Вопрос 1.

Какой базовый недостаток протокола Modbus TCP/IP делает его наиболее уязвимым для перехвата и модификации данных при передаче между ПЛК и SCADA-сервером?

A. Отсутствие механизмов аутентификации и шифрования, передача данных в открытом виде.

B. Высокая требовательность к вычислительным ресурсам контроллеров.

C. Использование только последовательного интерфейса RS-485.

D. Сложность настройки таблиц регистров.

Правильный ответ: A

Вопрос 2.

Согласно стандарту IEC 62351, какой уровень безопасности является обязательным, а какой опциональным при использовании протоколов МЭК 61850 для обмена данными между подстанцией и центром управления?

A. Конфиденциальность обязательна, целостность и аутентификация опциональны.

B. Аутентификация и целостность информации обязательны, конфиденциальность опциональна.

C. Все три параметра (конфиденциальность, целостность, аутентификация) являются обязательными.

D. Безопасность обеспечивается исключительно на физическом уровне.

Правильный ответ: B

Вопрос 3.

Какова основная функция DMZ (демилитаризованной зоны) в архитектуре АСУ ТП энергообъекта, построенной на базе модели Purdue?

A. Размещение серверов, непосредственно управляющих технологическим процессом, для ускорения доступа.

B. Обеспечение буферной зоны для безопасного обмена данными между корпоративной сетью (уровень 4) и технологической сетью (уровень 3), исключая прямое соединение.

C. Организация беспроводного доступа для полевых устройств (уровень 0).

D. Хранение резервных копий конфигураций ПЛК.

Вопрос 4.

Какая угроза для GOOSE-сообщений стандарта МЭК 61850 является наиболее критичной из-за их природы (мультикастовая рассылка без встроенной безопасности)?

A. Спуфинг (подмена) команд и Replay-атаки (повторная отправка перехваченных команд).

B. Чрезмерное увеличение размера Ethernet-кадра.

C. Неправильная настройция времени на IED (Intelligent Electronic Device).

D. Невозможность передачи сигналов защит.

Правильный ответ: A

Вопрос 5.

Применение технологии виртуального патчинга (virtual patching) на промышленном межсетевом экране наиболее оправдано в сценарии, когда:

A. Обнаружена уязвимость в ПЛК, но его остановка для установки официального патча невозможна из-за непрерывности техпроцесса.

B. Необходимо увеличить пропускную способность сети.

C. Требуется настроить новый VPN-доступ для удаленного вендора.

D. Производится замена вышедшего из строя коммутатора.

Правильный ответ: A

Вопрос 6.

Какой российский нормативный правовой акт устанавливает требования по обеспечению безопасности значимых объектов

критической информационной инфраструктуры (КИИ), включая создание систем безопасности?

A. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

B. Приказ ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

C. Приказ Минцифры № 123.

D. Регламент IEC 61850-90-2.

Правильный ответ: B

Вопрос 7.

Для выявления признаков атаки типа Man-in-the-Middle (перехват управления) в трафике МЭК 61850 инженеру по кибербезопасности необходимо в первую очередь анализировать:

A. Общую загрузку процессора на коммутаторах.

B. Журналы авторизации в домене Active Directory.

C. Аномалии в последовательности и времени доставки GOOSE-сообщений или появление "неизвестного" IED, публикующего данные.

D. Уровень напряжения в первичной цепи.

Правильный ответ: C

Вопрос 8.

При проектировании сегментации сети энергообъекта на каком уровне модели Purdue целесообразно применять "незначительную границу принуждения" (minor enforcement boundary) с использованием простых списков контроля доступа (ACL)?

A. Между корпоративной сетью (Уровень 4) и DMZ.

B. Между DMZ и диспетчерским уровнем (Уровень 3).

C. Между диспетчерским уровнем (Уровень 3) и уровнем локального управления (Уровень 2).

D. Между уровнем полевых устройств (Уровень 0) и контроллерами (Уровень 1).

Правильный ответ: C

Вопрос 9.

При расследовании инцидента, связанного с подозрительной активностью на инженерной рабочей станции АСУ ТП, какие журналы событий в первую очередь позволят проследить цепочку действий злоумышленника и использованные им инструменты?

A. Только журналы событий межсетевого экрана.

B. Журналы системы резервного копирования.

C. Журналы EDR-агента (Endpoint Detection and Response), установленного на рабочей станции, в совокупности с журналами IDS/IPS.

D. Журналы изменений конфигурации ПЛК.

Правильный ответ: C

Вопрос 10.

Какое сочетание методов оценки защищенности и инструментов наиболее эффективно для первичного моделирования угроз и выявления уязвимостей в выделенном сегменте сети с протоколом Modbus?

A. Только анализ организационно-распорядительной документации.

B. Сканирование портов (Nmap) для обнаружения устройств с открытым портом 502 и перехват трафика (Wireshark) для проверки передачи данных в открытом виде.

C. Анализ кода ПЛК на предмет логических ошибок.

D. Стресс-тестирование высоким напряжением.

Правильный ответ: B

Текущий контроль ТК2:

Проверяемая компетенция: **ПК-1.6.З , ПК-1.6.У, ПК-1.6.В**

ТЕСТ

Вопрос 1.

При проектировании архитектуры защиты АСУ ТП энергообъекта применение технологии однонаправленной передачи данных (data diode) наиболее оправдано в сценарии, когда:

A. Требуется обеспечить двустороннюю синхронизацию времени по протоколу PTP между технологической и корпоративной сетью.

B. Необходимо гарантировать физическую изоляцию технологического контура от внешних сетей при сохранении возможности мониторинга технологических параметров в диспетчерском центре.

C. Требуется организовать удаленный доступ вендора для диагностики оборудования.

D. Необходимо обеспечить резервирование каналов связи по технологии PRP.

Правильный ответ: B

Вопрос 2.

Какой функционал промышленного межсетевого экрана (Industrial Firewall) позволяет обнаружить попытку несанкционированной перепрошивки ПЛК или изменения его уставок через анализ промышленного протокола?

A. Stateful packet inspection (проверка состояния сессии).

B. Технология глубокого анализа трафика (DPI) на уровне приложений промышленных протоколов (Modbus, МЭК 61850).

C. Традиционная фильтрация по IP-адресам и портам.

D. Виртуальное патчинг (virtual patching).

Правильный ответ: B

Вопрос 3.

При обнаружении в журналах IDS/IPS события с атрибутами: источник — IP-адрес из корпоративной сети (192.168.1.10), получатель

— IP-адрес ПЛК (10.0.0.1), протокол — Modbus TCP, функциональный код — 90 (0x5A) (зарезервирован и не используется в стандартной спецификации), какой вывод должен сделать инженер по кибербезопасности?

A. Производится штатный сбор данных с ПЛК SCADA-сервером.

B. Зафиксирована попытка эксплуатации уязвимости или аномальная активность, требующая расследования (возможно, фаззинг или атака с использованием нестандартных функциональных кодов).

C. Выполняется успешная аутентификация пользователя.

D. Система резервного копирования создает архив конфигурации.

Правильный ответ: B

Вопрос 4.

Какой тип средств защиты (класс устройств) в архитектуре АСУ ТП предназначен для создания "песочницы" (sandbox) — изолированной виртуальной среды для безопасного запуска и анализа подозрительных файлов из внешних источников (например, со съемных носителей) перед их передачей в технологическую сеть?

A. Межсетевой экран следующего поколения (NGFW).

B. SIEM-система.

C. Средства защиты конечных точек (EDP/EPP) с функцией динамического анализа угроз.

D. Система обнаружения вторжений (IDS).

Правильный ответ: C

Вопрос 5.

Какие два протокола сетевого резервирования, согласно требованиям к ЛВС для объектов энергетики, обеспечивают бесшовное (seamless) переключение при обрыве связи с нулевым временем восстановления, что критично для GOOSE-сообщений МЭК 61850?

A. RSTP (Rapid Spanning Tree Protocol) и MSTP.

B. PRP (Parallel Redundancy Protocol) и HSR (High-availability Seamless Redundancy).

C. OSPF и BGP.

D. LACP и PAgP.

Правильный ответ: B

Вопрос 6.

При анализе конфигурации правил межсетевого экрана для сегментации сети энергообъекта (модель Purdue) обнаружено правило: "Разрешить любой трафик от ANY к ANY из сети Уровня 3 (операционный уровень) в сеть Уровня 0/1 (полевые устройства)". Данное правило является:

A. Приемлемым, так как операторам необходим полный доступ к оборудованию.

B. Допустимым при наличии системы обнаружения вторжений (IDS).

C. Грубым нарушением политики безопасности, реализующим избыточные права и потенциально позволяющим

скомпрометированному узлу верхнего уровня бесконтрольно воздействовать на технологический процесс.

D. Корректным, если это требование технологического регламента.

Правильный ответ: C

Вопрос 7.

Какую функцию выполняет SIEM-система в архитектуре кибербезопасности АСУ ТП при обработке журналов событий (логов) от различных источников (межсетевые экраны, IDS/IPS, серверы)?

A. Непосредственную блокировку сетевых атак в реальном времени.

B. Централизованный сбор, нормализацию, корреляцию событий и выявление инцидентов, требующих реагирования.

C. Шифрование всего сетевого трафика.

D. Резервное копирование конфигураций сетевых устройств.

Правильный ответ: B

Вопрос 8.

При проведении оценки защищенности сегмента сети с протоколом МЭК 61850 наиболее безопасной методикой тестирования, исключающей риск нарушения технологического процесса, является:

A. Запуск сканера уязвимостей общего назначения (Nessus) с максимальным профилем атак.

B. Пассивный мониторинг и анализ трафика с последующим применением протокол-ориентированного фаззинга в изолированной тестовой среде (копии сегмента).

C. Непосредственная отправка случайных (fuzzed) пакетов на работающие IED (Intelligent Electronic Devices).

D. Проведение стресс-тестирования путем генерации максимального потока широковещательных рассылок.

Правильный ответ: B

Вопрос 9.

Для синхронизации времени компонентов АСУ ТП с высокой точностью (субмикросекунды), требуемой для векторных измерений (синхрофазоры) по стандарту IEEE C37.118, какой протокол должен применяться?

A. NTP (Network Time Protocol).

B. SNTP (Simple Network Time Protocol).

C. PTP (Precision Time Protocol, IEEE 1588v2).

D. HTTP.

Правильный ответ: C

Вопрос 10.

Какой метод защиты периметра сети АСУ ТП предполагает создание отдельной подсети (буферной зоны) для размещения серверов, доступных как из корпоративной сети, так и из технологической, но исключающей прямое соединение между ними?

A. Виртуальная частная сеть (VPN).

B. Технология виртуальных локальных сетей (VLAN).

C. Демилитаризованная зона (DMZ).

D. Система предотвращения вторжений (IPS).

Правильный ответ: C

Текущий контроль ТКЗ:

Проверяемая компетенция: **ПК-1.6.З , ПК-1.6.У, ПК-1.6.В**

ТЕСТ

Вопрос 1.

Согласно требованиям ФСТЭК России к значимым объектам КИИ (Приказ № 239), какой из перечисленных этапов входит в обязанность субъектов КИИ по реагированию на инциденты?

A. Только уведомление вышестоящих организаций о факте инцидента.

B. Незамедлительное информирование ФСБ России о каждом подозрительном событии.

C. Проведение мероприятий по реагированию на инциденты, включая анализ причин и условий возникновения инцидента, устранение последствий и принятие мер по недопущению повторения.

D. Публичное раскрытие информации о всех выявленных уязвимостях АСУ ТП.

Вопрос 2.

При разработке регламента реагирования на инциденты для АСУ ТП энергообъекта, какой фактор в первую очередь должен отличать действия персонала при подозрении на целевое кибератаку (APT) от реагирования на отказ оборудования?

A. Скорость перезагрузки серверов.

B. Необходимость сохранения криминалистически значимой информации (логов, дампов памяти) для расследования до начала восстановительных работ.

C. Немедленное отключение электропитания на объекте.

D. Вызов только технического персонала, без привлечения службы безопасности.

Правильный ответ: B

Вопрос 3.

Какой документ из состава организационно-распорядительной документации в первую очередь определяет цели, задачи, обязанности сотрудников и общие принципы обеспечения кибербезопасности на энергообъекте?

A. Инструкция по настройке межсетевого экрана.

B. Регламент резервного копирования.

C. Политика информационной безопасности (высокоуровневый документ).

D. Журнал учета съемных носителей информации.

Правильный ответ: C

Вопрос 4.

При моделировании угроз для сегмента сети с протоколом Modbus, питающего ПЛК управления турбиной, какова должна быть первичная цель идентификации активов и построения модели угроз согласно методике ФСТЭК?

A. Оценка рыночной стоимости оборудования.

B. Определение критических бизнес-процессов и установление возможных последствий от нарушения их функционирования (останов турбины, авария).

C. Подготовка документации для закупки нового оборудования.

D. Классификация сотрудников по уровням доступа к интернету.

Правильный ответ: B

Вопрос 5.

В журналах IDS/IPS зафиксирована аномалия: единичное GOOSE-сообщение с "0" во всех полях данных, широковещательно отправленное от устройства с незнакомым MAC-адресом, после чего один из выключателей на подстанции изменил состояние. Действия инженера согласно регламенту реагирования:

A. Проигнорировать событие как ошибочное.

B. Квалифицировать событие как инцидент, инициировать расследование, изолировать подозрительный сегмент сети для анализа и сохранения доказательств.

C. Немедленно перезагрузить все коммутаторы на подстанции.

D. Отправить отчет в конце месяца.

Правильный ответ: B

Вопрос 6.

Какой элемент регламента реагирования на инциденты для АСУ ТП должен содержать четкий порядок взаимодействия с оперативным персоналом (дежурными диспетчерами, начальниками смены) при подозрении на кибератаку?

A. Только технические детали анализа трафика.

B. Перечень формализованных команд и процедур (например, "стоп-кран" или перевод на ручное управление) для безопасной остановки технологического процесса при подтверждении атаки.

C. Список IP-адресов всех ПЛК.

D. Инструкция по замене сетевых кабелей.

Правильный ответ: B

Вопрос 7.

Согласно ФЗ-187 «О безопасности КИИ», в какой срок субъект КИИ обязан проинформировать ФСТЭК России об инцидентах, повлекших негативные последствия (например, нарушение технологического процесса)?

A. В течение 24 часов с момента обнаружения.

B. В течение 3 дней с момента ликвидации последствий.

C. Незамедлительно (не позднее 24 часов) и дополнительно предоставить информацию по результатам расследования.

D. Субъект КИИ не обязан информировать государственные органы о таких инцидентах.

Правильный ответ: C

Вопрос 8.

При разработке политики безопасности для сетей АСУ ТП, использование каких паролей (согласно приказам ФСТЭК) категорически запрещено для учетных записей привилегированных пользователей (администраторов АСУ ТП)?

A. Пароли длиной не менее 8 символов.

B. Пароли, совпадающие с логином пользователя, а также пароли, устанавливаемые по умолчанию (заводские) и не измененные после ввода в эксплуатацию.

C. Пароли с использованием только латинских букв.

D. Пароли, содержащие символы верхнего и нижнего регистра.

Правильный ответ: B

Вопрос 9.

Какой методологический подход (методика) должен применяться при разработке организационно-распорядительной документации для определения достаточного набора средств защиты в конкретных сегментах сети АСУ ТП энергообъекта?

A. Метод "максимальной стоимости" (установка всех возможных средств защиты).

B. Метод "минимальной функциональности" (установка только того, что уже есть в наличии на складе).

C. Стратификация (разбиение на уровни/зоны) на основе модели Purdue и риск-ориентированный подход (оценка угроз и уязвимостей для каждой зоны).

D. Копирование документации с аналогичного объекта без изменений.

Правильный ответ: C

Вопрос 10.

При расследовании инцидента, связанного с несанкционированным изменением уставок защит на микропроцессорном терминале РЗА, какие журналы событий в дополнение к сетевым логам (IDS/IPS) необходимо в первую очередь запросить и проанализировать для определения ответственного лица?

A. Журналы событий операционной системы и приложений самого терминала РЗА (если доступно) и журналы доступа оперативного персонала (СКУД, система сбора технологической информации).

B. Только журналы работы систем кондиционирования.

C. Журналы изменений в корпоративной почте.

D. Журналы электропотребления здания.

Правильный ответ: А

Темы рефератов

1. Сравнительный анализ архитектурных моделей АСУ ТП энергообъектов: от классической иерархии к модели Purdue и концепции «зоны и каналы» стандарта IEC 62443.
2. Протоколы промышленной автоматизации в энергетике: анализ уязвимостей Modbus TCP/IP и МЭК 61850 (GOOSE, MMS, SV).
3. Актуальные угрозы и векторы атак на АСУ ТП энергообъектов: анализ инцидентов (Industryer, BlackEnergy, Triton) и тактики по MITRE ATT&CK для ICS.
4. Нормативно-правовое регулирование кибербезопасности КИИ в энергетике РФ: анализ требований ФЗ-187, Приказов ФСТЭК (№ 31, 239) и их практическая реализация.
5. Стандартизация кибербезопасности в электроэнергетике: сравнительный обзор международных стандартов (IEC 62351, NIST SP 800-82) и их адаптация в РФ.
6. Принципы сегментации сетей АСУ ТП энергообъектов: проектирование DMZ, зон безопасности и границ принуждения на основе модели угроз.
7. Средства защиты периметра и внутренних сегментов АСУ ТП: специализированные межсетевые экраны и системы обнаружения вторжений (IDS/IPS) для промышленных протоколов.
8. Криптографическая защита информации (СКЗИ) в АСУ ТП энергообъектов: проблемы внедрения и практические решения для аутентификации и шифрования трафика (ГОСТ, IEC 62351).
9. Технологии безопасного удаленного доступа к компонентам АСУ ТП энергообъектов: анализ рисков, модели реализации (VEN, jump host, многофакторная аутентификация).
10. Резервирование и отказоустойчивость сетей связи на энергообъектах: применение протоколов PRP/HSR для критичных сервисов (GOOSE) и их влияние на кибербезопасность.
11. Методика анализа промышленного трафика (МЭК 61850) с использованием Wireshark и TShark: выявление аномалий и признаков атак.
12. Применение сканеров уязвимостей для оценки защищенности АСУ ТП: особенности, риски и методология безопасного тестирования компонентов энергообъектов.
13. Моделирование угроз и оценка рисков для сегмента сети АСУ ТП энергообъекта: практическое применение методик ФСТЭК и построение модели нарушителя.
14. Симуляция сетей АСУ ТП как инструмент тестирования средств защиты: построение виртуального полигона с эмуляцией протоколов Modbus/МЭК 61850 в GNS3/EVE-NG.

15. Интерпретация журналов событий (логов) систем обнаружения вторжений для выявления и расследования инцидентов в АСУ ТП.

16. Разработка политики информационной безопасности для АСУ ТП энергообъекта: структура, ключевые разделы и требования к парольной защите и антивирусной защите.

17. Регламент реагирования на инциденты кибербезопасности для АСУ ТП энергообъекта: процедуры обнаружения, сдерживания,

18. Организация взаимодействия с государственными органами (ФСТЭК, НКЦКИ) при инцидентах на объектах КИИ: порядок и сроки информирования.

19. Роль криминалистики (ICS Forensics) в расследовании киберинцидентов на энергообъектах: сбор, сохранение и анализ цифровых доказательств.

20. Повышение осведомленности и обучение персонала энергообъектов основам кибербезопасности: разработка программы и ключевых тем для технического и оперативного персонала.

Для промежуточной аттестации:

ОМ1

1. Раскройте содержание иерархической модели Purdue применительно к архитектуре АСУ ТП энергообъектов. Охарактеризуйте основные уровни от 0 до 4 и поясните, какие компоненты на них располагаются.

2. Проведите сравнительный анализ протоколов Modbus TCP/IP и МЭК 61850 (GOOSE, MMS) с точки зрения кибербезопасности. В чем заключаются основные уязвимости каждого из них?

3. Охарактеризуйте стандарт IEC 62351. Какие требования к безопасности протоколов МЭК 61850 он устанавлиет? Какие механизмы защиты (аутентификация, целостность, конфиденциальность) являются обязательными, а какие опциональными?

4. Назовите и классифицируйте актуальные угрозы и векторы атак на АСУ ТП энергообъектов. Приведите примеры известных инцидентов (Industryer, BlackEnergy, Triton) и опишите тактики злоумышленников.

5. Раскройте содержание Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Какие субъекты подпадают под его действие и какие обязанности на них возлагаются?

6. Охарактеризуйте ключевые требования приказов ФСТЭК России № 31 и № 239 к обеспечению безопасности значимых объектов КИИ в части создания систем защиты и реагирования на инциденты.

7. Какие требования предъявляются к парольной защите и управлению доступом в АСУ ТП согласно нормативным документам

ФСТЭК? Какие пароли категорически запрещены?

8. Опишите структуру и содержание матрицы MITRE ATT&CK для промышленных систем (ICS). Как она может применяться для моделирования угроз и анализа тактик нарушителей?

9. В чем заключается специфика обеспечения безопасности систем реального времени (СРВ) в энергетике по сравнению с классическими информационными системами? Какие требования к временным задержкам критичны?

10. Раскройте понятие "киберустойчивость" (cyber resilience) применительно к энергообъектам. Чем это понятие отличается от традиционной информационной безопасности?

11. Охарактеризуйте принципы сегментации сетей АСУ ТП энергообъектов. Что такое DMZ (демилитаризованная зона), какова ее роль и какие компоненты в ней размещаются?

12. Опишите функциональные возможности промышленных межсетевых экранов (Industrial Firewall). В чем отличие технологии DPI (Deep Packet Inspection) от классической фильтрации по IP-адресам и портам?

13. Проведите сравнительный анализ систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS). Каковы особенности их применения в АСУ ТП?

14. Что такое технология "песочницы" (sandbox) и как она применяется для защиты АСУ ТП от угроз нулевого дня (zero-day attacks)?

15. Охарактеризуйте средства криптографической защиты информации (СКЗИ) в АСУ ТП. Какие проблемы возникают при внедрении шифрования в промышленных сетях с жесткими требованиями к временным задержкам?

16. Опишите технологию однонаправленной передачи данных (data diode). В каких сценариях защиты энергообъектов ее применение наиболее оправдано?

17. Какие протоколы сетевого резервирования (PRP, HSR, RSTP) применяются в сетях цифровых подстанций? В чем преимущества PRP/HSR для передачи критичных GOOSE-сообщений?

18. Охарактеризуйте функциональные возможности NGFW (Next-Generation Firewall) на примере российских решений (ViPNet Coordinator HW, UserGate и др.). Какие функции безопасности объединяют такие устройства?

19. Что такое виртуальное патчинг (virtual patching) и в каких сценариях его применение наиболее оправдано при эксплуатации АСУ ТП?

20. Опишите архитектуру защищенного удаленного доступа к компонентам АСУ ТП энергообъекта. Какие модели реализации (VPN, jump host, многофакторная аутентификация) могут применяться?

21. Опишите методику анализа промышленного трафика МЭК 61850

с использованием Wireshark. Какие признаки могут свидетельствовать о наличии аномалий или атак (спуфинг, replay-атаки)?

22. Какие функциональные коды протокола Modbus являются наиболее критическими с точки зрения безопасности? Обнаружение каких кодов в трафике должно вызывать тревогу?

23. Охарактеризуйте особенности применения сканеров уязвимостей (например, Nessus для ICS) для оценки защищенности АСУ ТП. Какие риски связаны с активным сканированием и как их минимизировать?

24. Опишите процесс интерпретации журналов событий (логов) IDS/IPS для выявления и расследования инцидентов. На какие атрибуты событий следует обращать внимание в первую очередь?

25. Какие инструменты симуляции сетей (GNS3, EVE-NG) могут применяться для тестирования политик безопасности и сценариев реагирования без риска для реального оборудования энергообъекта?

26. Опишите методику моделирования угроз для выделенного сегмента сети АСУ ТП. Какие этапы включает этот процесс согласно рекомендациям ФСТЭК?

27. Как проводится криминалистический анализ (ICS Forensics) компонентов АСУ ТП при расследовании инцидентов? Какие цифровые доказательства необходимо сохранить и как обеспечить их юридическую силу?

28. Охарактеризуйте процесс анализа конфигураций сетевого оборудования (коммутаторов, межсетевых экранов) на предмет выявления ошибок и избыточных правил фильтрации.

29. Какие метрики и показатели могут применяться для оценки уровня защищенности АСУ ТП энергообъекта? Что такое KPI кибербезопасности?

30. Опишите процесс разработки модели нарушителя для энергообъекта. Какие типы нарушителей (внешние/внутренние, мотивированные/случайные) выделяются и как их потенциал влияет на выбор средств защиты?

31. Какова структура и содержание политики информационной безопасности для АСУ ТП энергообъекта? Какие разделы обязательно должны присутствовать в этом документе?

32. Опишите пошаговый регламент реагирования на инциденты кибербезопасности для АСУ ТП. Каковы этапы обнаружения, сдерживания, ликвидации и восстановления?

33. Каков порядок и сроки информирования государственных органов (ФСТЭК России, НКЦКИ) об инцидентах на объектах КИИ? Что должно содержаться в первичном уведомлении?

34. Как организовать процесс взаимодействия с оперативным персоналом (дежурными диспетчерами) при подозрении на кибератаку? Какие формализованные команды и процедуры должны быть разработаны?

35. Охарактеризуйте принципы организации антивирусной защиты в

АСУ ТП. В чем заключается специфика обновления антивирусных баз на промышленных объектах?

36. Какие требования предъявляются к резервному копированию и восстановлению компонентов АСУ ТП с точки зрения кибербезопасности? Как часто должны создаваться резервные копии конфигураций?

37. Опишите процесс разработки программы повышения осведомленности и обучения персонала энергообъекта основам кибербезопасности. Какие темы должны быть включены в программу для технического и оперативного персонала?

38. Как организовать процесс управления уязвимостями в АСУ ТП? Каков порядок получения информации об уязвимостях, их оценки и устранения (патчинга)?

39. Охарактеризуйте понятие "безопасность на этапе проектирования" (Security by Design) применительно к АСУ ТП энергообъектов. Почему важно закладывать меры защиты на ранних этапах создания системы?

40. Какие требования предъявляются к безопасности цепочки поставок (supply chain) для компонентов АСУ ТП энергообъектов? Как минимизировать риски, связанные с закладками и недоверенным программным обеспечением?