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 автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Защита технологической информации в АСУ ТП

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Дратвяк А.В. Идентификатор: R1a0ecc29-DratviakAV-b9b11303	А.В. Дратвяк
(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-2 Готов к внедрению систем защиты информации автоматизированных систем
   ПК-2.1 Устанавливает и настраивает средства защиты информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 2 (Контрольная работа)
3. Контрольное мероприятие № 3 (Контрольная работа)
4. Контрольное мероприятие № 4 (Контрольная работа)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Раздел 1. Понятие АСУ ТП и принципы её функционирования					
Вводная лекция.		+			
Тема 1. Нормативно-правовые основы организации функционирования и защиты АСУ ТП.		+			
Тема 2. Принципы сбора, обработки и хранения информации в АСУ ТП.		+			
Тема 3. Классификация программно-технических уровней АСУ ТП.				+	+
Тема 4. Идентификация и оценивание состояния технологических объектов управления для построения комплексной системы защиты информации.				+	+
Тема 5. Администрирование подсистем информационной безопасности на объектах критической инфраструктуры.				+	+
Раздел. 2. Защита информации в программных и технических компонентах АСУ ТП					
Тема 6. Сегментация локально вычислительных сетей АСУ ТП.					+
Тема 7. Программно-аппаратные решения для построения системы защиты на типовых промышленных объектах.					+

Тема 8. Программное обеспечение верхнего уровня АСУ ТП.		+		
Тема 9. Центр управления информационной безопасностью АСУ ТП.		+		
Тема 10. Комплексный подход к обеспечению информационной безопасности на промышленных объектах, оснащенных АСУ ТП.		+		
Раздел 3. Построение комплексной системы защиты АСУ ТП на предприятии.				
Тема 11. Методы декомпозиции общей задачи защиты информации в АСУ ТП на частные задачи меньшей размерности.		+		
Тема 12. Разработка и реализация политики информационной безопасности на объектах АСУ ТП.			+	
Тема 13. Требования руководящих документов по технической и программной защите информации в АСУ ТП.	+			
Тема 14. Регламентация деятельности персонала по защите информации в АСУ ТП.		+		
Тема 15. Анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.		+		
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	ПК-2.1$_{ПК-2}$ Устанавливает и настраивает средства защиты информации в автоматизированных системах	Знать: порядок администрирования программных компонентов АСУ ТП нормативные документы, регламентирующие создание, применение и защиту АСУ ТП порядок применения и реализации стандартных политик информационной безопасности применительно к АСУ ТП в соответствии с требованиями руководящих документов регуляторов методы поиска технической информации и иных исходных данных для проведения анализа защищенности информации в АСУ ТП Уметь:	Контрольное мероприятие № 1 (Контрольная работа) Контрольное мероприятие № 2 (Контрольная работа) Контрольное мероприятие № 3 (Контрольная работа) Контрольное мероприятие № 4 (Контрольная работа)

		анализировать полноту и целостность программных элементов АСУ ТП выбирать средства защиты информации для типовых подсистем АСУ ТП осуществлять поиск, анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных решений	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольное мероприятие № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: методы поиска технической информации и иных исходных данных для проведения анализа защищенности информации в АСУ ТП</td>
<td>1.Контрольное мероприятие № 1 по дисциплине Б1.В.04 Защита технологической информации в АСУ ТП
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>1</td><td>Опишите общую структуру и типовые компоненты АСУ ТП.</td><td>Какие виды рисков возникают в АСУ ТП? Объяснить причину возникновения.</td></tr>
<tr><td>2</td><td>Как применяется в КСУ принцип защиты в глубину для обеспечения ИБ и для обеспечения ФБ?</td><td>Каким образом взаимосвязаны и какие группы требований предъявляются ИБ и ФБ?</td></tr>
<tr><td>3</td><td>В соответствии с положениями ГОСТ Р МЭК о функциональная безопасность систем Э/Э/ЭП раскройте суть определений:
→ "вред",
→ "опасная ситуация",
→ "причиняющее вред событие",
→ "управляемое оборудование",
→ "полнота безопасности".</td><td>В соответствии с положениями ГОСТ Р МЭК о функциональная безопасность систем Э/Э/ЭП раскройте суть определений:
→ "опасность",
→ "опасное событие",
→ "безопасное состояние",
→ "окружение",
→ "режим работы".</td></tr>
<tr><td>4</td><td>Что включает в себя концепция продукта?</td><td>Что включает в себя устав проекта по сертификации?</td></tr>
<tr><td>5</td><td>Что решается в ходе инициирующего собрания?</td><td>Как рассчитывается бюджет проекта сертификации?</td></tr>
</table>
</td>
</tr>
<tr>
<td>Уметь: осуществлять поиск,</td>
<td>1.</td>
</tr>
</table>

<table>
<tr>
<td>анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП</td>
<td></td>
<td>
<table>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>6</td><td>Кратко составьте концепцию продукта в формате mind-схемы для программируемого логического контроллер ПЛК100-220.Р-М ОВЕН</td><td>Кратко составьте концепцию продукта в формате mind-схемы для программируемого логического контроллер 110-24.30.К-М ОВЕН</td></tr>
</table>
</td>
</tr>
</table>

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Студент ответил на все вопросы. Ответы на вопросы полные, содержательные, правильные и логически обоснованные.

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Студент не ответил только на 1 вопрос или дал неполные ответы на все вопросы. Ответы на вопросы достаточно полные, обстоятельные, частично правильные, содержат незначительные логические нарушения.

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Студент ответил на половину вопросов. Ответы на вопросы неполные, плохо обоснованные, частично неправильные, нарушена логическая последовательность ответа.

КМ-2. Контрольное мероприятие № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: порядок администрирования программных компонентов АСУ ТП</td>
<td></td>
<td>
1.Контрольное мероприятие № 1 по дисциплине Б1.В.04 Защита технологической информации в АСУ ТП
<table>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>1</td><td>Какую структуру должен иметь план управления ФБ (FSMP) для соответствия требованиям МЭК 61508?</td><td>Какую структуру должен иметь план управления персоналом (HRMP) для соответствия требованиям МЭК 61508?</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>2</td><td>Какие атрибуты ФБ определяет МЭК 61508? Раскройте определение данных атрибутов.</td><td>Составьте перечень и раскройте суть методов анализа надёжности в соответствии с МЭК 61508 Вам известны? (RBD, FTA, MT).</td></tr>
<tr><td>3</td><td>Опишите структуру методов обеспечения ФБ согласно МЭК 61508. Дайте характеристику организационным методам обеспечения ИБ и ФБ в АСУ ТП.</td><td>Опишите структуру методов обеспечения ФБ согласно МЭК 61508. Дайте характеристику техническим методам обеспечения ИБ и ФБ в АСУ ТП.</td></tr>
<tr><td>4</td><td>Каким образом должны применяться таблицы, содержащие требования к защите от
отказов аппаратных средств в КСУ АСУ ТП?</td><td>Каким образом должны применяться таблицы, содержащие требования к защите от
отказов ПО в КСУ АСУ ТП?</td></tr>
<tr><td>5</td><td>Дайте характеристику полевого уровня и уровня присоединения ПТК АСУ ТП. Приведите примеры устройств каждого из уровней.</td><td>Дайте характеристику станционного уровня и уровня демилитаризованной зоны ПТК АСУ ТП. Раскройте суть и назначение демилитаризованной зоны в АСУ ТП.</td></tr>
</table>
</td></tr>
<tr><td>Уметь: анализировать полноту и целостность программных элементов АСУ ТП</td><td></td><td>1.
<table>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>6</td><td>Какова взаимосвязь между требованиями к ИБ и ФБ?</td><td>В чем состоят отличия КСУ от информационных систем?</td></tr>
<tr><td>7</td><td>Какие типы моделей и каким образом применяются для оценивания и обеспечения ИБ и ФБ КСУ?</td><td>Какое описание следует составить для КСУ с точки зрения оценивания и обеспечения ИБ?</td></tr>
<tr><td>8</td><td>Опишите структуру фрейворка ИБ согласно положениям NIST SP 800-53</td><td>Дайте характеристику уровням ИБ (Security Level) согласно положениям ISA/IEC 62443</td></tr>
</table>
</td></tr>
<tr><td>Уметь: применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных</td><td></td><td>1.
<table>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>7</td><td>Составить модель угроз функциональной и информационной</td><td>Составить модель угроз функциональной и информационной</td></tr>
</table>
</td></tr>
</table>

решений			безопасности для программируемого логического контроллера REGUL R500	безопасности для программируемого логического контроллера REGUL R400

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Студент ответил на все вопросы. Ответы на вопросы полные, содержательные, правильные и логически обоснованные.

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Студент не ответил только на 1 вопрос или дал неполные ответы на все вопросы. Ответы на вопросы достаточно полные, обстоятельные, частично правильные, содержат незначительные логические нарушения.

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Студент ответил на половину вопросов. Ответы на вопросы неполные, плохо обоснованные, частично неправильные, нарушена логическая последовательность ответа.

КМ-3. Контрольное мероприятие № 3

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: нормативные документы, регламентирующие создание, применение и защиту АСУ ТП

1.Контрольное мероприятие № 1 по дисциплине Б1.В.04 Защита технологической информации в АСУ ТП

№ п/п	1 Вариант	2 Вариант
1	Опишите структуру общего жизненного цикла безопасности КСУ в соответствии со стандартом МЭК 61508-1	Опишите структуру V-образного жизненного цикла информационной и функциональной безопасности
2	Дайте характеристику тестирования «засевом» дефектов (Fault Insertion Testing)	Дайте характеристику интеграционного и валидационного тестирования

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>ПО КСУ</td><td>(Integration Testing and Validation Testing) ПО КСУ</td></tr>
<tr><td>3</td><td>Что такое спецификация требований по безопасности? (для мировой практики раскрыть суть SRS, для отечественной - суть и отличие технического задания (ТЗ) и технического условия (ТУ)</td><td>Что такое проект архитектуры системы (SAD) и какова его структура?</td></tr>
<tr><td>4</td><td>Назовите суть и назначение стандартов:
- Profibus DP и PA,
- Foundation Fieldbus,
- Modbus RTU,
- HART,
- DeviceNet.</td><td>Назовите суть и назначение стандартов:
- Profinet,
- EtherCAT,
- Ethernet Powerlink,
- Ether/IP.</td></tr>
<tr><td>5</td><td>Что такое сеть CAN? Что такое протокол CANopen? Что такое CANopenNode?</td><td>Что такое As-Interface? Каковы его преимущества и недостатки?</td></tr>
</table>
</td></tr>
<tr><td>Уметь: выбирать средства защиты информации для типовых подсистем АСУ ТП</td><td></td><td>1.
<table>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>1</td><td>Провести анализ информации, передаваемой по протоколу Modbus RTU в АСУ ТП электрической подстанции, для выявления наличия конфиденциальной и технической информации на примере предложенного файла перехваченных пакетов программы WireShark</td><td>Провести анализ информации, передаваемой по протоколу EtherCAT в АСУ ТП электрической подстанции, для выявления наличия конфиденциальной и технической информации на примере предложенного файла перехваченных пакетов программы WireShark</td></tr>
</table>
</td></tr>
</table>

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Студент ответил на все вопросы. Ответы на вопросы полные, содержательные, правильные и логически обоснованные.

Оценка: 4

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Студент не ответил только на 1 вопрос или дал неполные ответы на все вопросы. Ответы на вопросы достаточно полные, обстоятельные, частично правильные, содержат незначительные логические нарушения.

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Студент ответил на половину вопросов. Ответы на вопросы неполные, плохо обоснованные, частично неправильные, нарушена логическая последовательность ответа.

КМ-4. Контрольное мероприятие № 4

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: нормативные документы, регламентирующие создание, применение и защиту АСУ ТП</td>
<td>1.
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>6</td><td>Произведите первичное подключение и настройку SCADA-системы стенда АСУ ТП. Дайте краткую характеристику отображаемым в интерфейсе SCADA-системы параметрам</td><td>Произведите первичное подключение и настройку SCADA-системы стенда АСУ ТП. Сформируйте краткую модель нарушителя информационной безопасности для SCADA-системы</td></tr>
</table></td>
</tr>
<tr>
<td>Знать: порядок применения и реализации стандартных политик информационной безопасности применительно к АСУ ТП в соответствии с требованиями руководящих документов регуляторов</td>
<td>1.Контрольное мероприятие № 1 по дисциплине Б1.В.04 Защита технологической информации в АСУ ТП
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>1</td><td>По каким категориям требований происходит сравнительный анализ характеристик IT-систем и КСУ?</td><td>Дайте характеристику СМИБ в соответствии с NIST SP 800-53. Кратко охарактеризуйте возможность применения данного стандарта и NIST CSF к отечественным реалиям ИБ.</td></tr>
<tr><td>2</td><td>Какова общая структура содержания NIST SP 800-82 «Guide</td><td>Каково общее содержание и назначение ISA/IEC</td></tr>
</table></td>
</tr>
</table>

			to Industrial Control Systems (ICS) Security»? Переведён ли документ на русский язык?	62443? Какие части документа переведены на русский язык?
		3	В виде таблицы или графического отображения кратко опишите уровни ИБ (Security Level, SL) в соответствии со стандартом ISA/IEC 62443.	Раскройте суть аббревиатуры ПЛИС и её назначение. Дайте краткую характеристику двум типам современных ПЛИС с точки зрения ИБ.
		4	Опираясь на ТТХ и физические свойства ПЛИС предложите перечень достоинств их применения в АСУ ТП исключительно с точки зрения обеспечения ИБ.	Опираясь на ТТХ и физические свойства ПЛИС составьте перечень недостатков их применения в АСУ ТП исключительно с точки зрения обеспечения информационной безопасности.
		5	Какова цель проведения квалификационных испытаний оборудования в АСУ ТП с использованием рекомендация EPRI TR-107330?	В общем виде сформулируйте виды тестов, применяемых для квалификационных испытаний ПЛИС в соответствии с EPRI TR-107330?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Студент ответил на все вопросы. Ответы на вопросы полные, содержательные, правильные и логически обоснованные.

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Студент не ответил только на 1 вопрос или дал неполные ответы на все вопросы. Ответы на вопросы достаточно полные, обстоятельные, частично правильные, содержат незначительные логические нарушения.

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Студент ответил на половину вопросов. Ответы на вопросы неполные, плохо обоснованные, частично неправильные, нарушена логическая последовательность ответа.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра: *Безопасности и информационных технологий* Дисциплина: «Защита технологической информации в автоматизированных системах управления технологическими процессами»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю. Невский* *Протокол кафедры № 3* *«16» декабря 2020г.*
1. Основные нормативно-правовые акты в области информационной и функциональной безопасности АСУ ТП. 2. Назначение и содержание спецификации требований по безопасности (SRS) и проекта архитектуры системы (SAD) АСУ ТП. 3. Рассчитать показатели функциональной безопасности и надёжности для одного из предложенных преподавателем компонентов АСУ ТП.		

Процедура проведения

Устный экзамен с практической письменной частью на листах установленного администрацией образца

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

1. Компетенция/Индикатор: ПК-2.1$_{ПК-2}$ Устанавливает и настраивает средства защиты информации в автоматизированных системах

Вопросы, задания

1.Перечислить основные нормативно-правовые акты в области информационной и функциональной безопасности АСУ ТП
2.Описать назначение и функциональные возможности SCADA-систем. Операции, доступные оперативному персоналу, через интерфейс SCADA-системы
3.Дать характеристику порядка работы и обновления программного обеспечения компонентов АСУ ТП и антивирусного программного обеспечения в КСУ ТП
4.Сформировать перечень техник атак на SCADA-системы АСУ ТП на основе матрицы MITRE ATT&CK
5.Перечислить требования к функциональной безопасности АСУ ТП в соответствии с ГОСТ Р МЭК 61508 и её взаимосвязь с информационной безопасностью КИИ
6.Описать требования к обеспечению безопасности АСУ ТП, представленных в ФЗ № 187 и Приказе ФСТЭК России № 239
7.Дать характеристику назначения и содержания ГОСТ Р МЭК 60870 и ГОСТ Р МЭК 62443 в контексте обеспечения сетевой безопасности АСУ ТП
8.Сформировать перечень вариантов реализации требований к мерам защиты информации в АСУ ТП в соответствии с Приказом № 31 ФСТЭК России
9.Перечислить характеристики системы управления функциональной и информационной безопасностью в соответствии с ГОСТ Р МЭК 61508

10.Описать реализацию принципов многорубежности и эшелонирования средств защиты информации в соответствии со структурными элементами типовой архитектуры компьютерной системы управления
11.Дать характеристику различим принципам построения вычислительных сетей в АСУ ТП электрической подстанции в зависимости от применяемого на объекте типа архитектуры
12.Сформировать порядок применения организационных и технических решений по сегментации локальной вычислительной сети АСУ ТП
13.Перечислить классификацию и способы оценки эффективности инструментальных средств для обеспечения функциональной безопасности АСУ ТП
14.Описать понятия релейной техники, релейной защиты автоматики и противоаварийной автоматики, а также обеспечение безопасности полевого уровня АСУ ТП
15.Дать характеристику уровней программно-технического комплекса АСУ ТП, характеристика их назначения и подходы к обеспечению информационной безопасности на примере электрической подстанции
16.Сформировать принципы применения системы обнаружения вторжений на шинах станции, управления и демилитаризованной зоны в АСУ ТП

Материалы для проверки остаточных знаний

1.1. Опишите общую структуру и компоненты типовой КСУ

Ответы:

Деление системы на компоненты следует производить исходя из функциональных задач технологического процесса, отраслевой принадлежности, а также наивысшего грифа обрабатываемой в КСУ информации

Верный ответ: В производственных АСУ ТП системы обычно строятся по трехуровневому принципу. Нижний уровень (полевой уровень, field) АСУ ТП представляет собой различные датчики (сенсоры) и исполнительные механизмы. Средний уровень (уровень контроллеров) состоит из программируемых логических контроллеров (ПЛК, в англоязычной литературе - PLC). Он как раз принимает полевые данные и выдает команды управления на нижний уровень. Управление в ПЛК осуществляется по заранее разработанному алгоритму, который исполняется циклически (прием данных – обработка – выдача управляющих команд). Верхний уровень - это уровень визуализации, диспетчеризации (мониторинга) и сбора данных. На этом уровне задействован человек, т.е. оператор (диспетчер). Если он осуществляет контроль локального агрегата (машины), то для его осуществления используется так называемый человеко-машинный интерфейс (HMI, Human-Machine Interface). Если оператор осуществляет контроль за распределенной системой машин, механизмов и агрегатов, то для таких диспетчерских систем часто применим термин SCADA (Supervisory Control And Data Acqusition - диспетчерское управление и сбор данных, англ.) В обоих случаях верхний уровень АСУ ТП обеспечивает сбор, а также архивацию важнейших данных от ПЛК, их визуализацию, т.е. наглядное (в виде мнемосхем, часто анимированных) представление на экране существо и параметры происходящего процесса.

2.2. Как распределяются отказы между компонентами КСУ?

Ответы:

Отказы системы неразрывно связаны с понятием “надежности” и трактуются в отношении отказоустойчивости объекта к техногенным и информационным угрозам

Верный ответ: Средняя наработка между отказами – математическое ожидание наработки объекта от окончания восстановления его работоспособного состояния после отказа до возникновения следующего отказа. Вычисляется как отношение суммарной наработки объекта между отказами за рассматриваемый период к числу

отказов за тот же период. Теория надёжности предполагает следующие четыре основных допущения: Отказ рассматривается как случайное событие. Причины отказов, соотношения между отказами (за исключением того, что вероятность отказа есть функция времени) задаются функцией распределения. Инженерный подход к надёжности рассматривает вероятность безотказной работы как оценку на определённом статистическом доверительном уровне. Надёжность системы тесно связана с понятием «заданная функция системы». В основном, рассматривается режим работы без отказов. Однако, если в отдельных частях системы нет отказов, но система в целом не выполняет заданных функций, то это относится к техническим требованиям к системе, а не к показателям надёжности. Надёжность системы может рассматриваться на определённом отрезке времени. На практике это означает, что система имеет шанс (вероятность) функционировать это время без отказов. Характеристики (показатели) надёжности гарантируют, что компоненты и материалы будут соответствовать требованиям на заданном отрезке времени. Поэтому иногда надёжность в широком смысле слова означает свойство «гарантоспособности»[источник не указан 606 дней]. В общем случае надёжность относится к понятию «наработка», которое в зависимости от назначения системы и условий её применения определяет продолжительность или объём работы. Наработка может быть как непрерывной величиной (продолжительность работы в часах, километраж пробега в милях или километрах и т. п.), так и целочисленной величиной (число рабочих циклов, запусков, выстрелов оружия и т. п.). Согласно определению, надёжность рассматривается относительно заданных режимов и условий применения. Это ограничение необходимо, так как невозможно создать систему, которая способна работать в любых условиях. Внешние условия функционирования системы должны быть известны на этапе проектирования. Например, Марсоход создавался совершенно для других условий эксплуатации, чем семейный автомобиль.

3.3. Какие существуют типы и архитектуры КСУ? Являются ли они киберфизическими системами?

Ответы:

В ответе на вопрос необходимо раскрыть понятие компьютерной системы управления и киберфизических систем

Верный ответ: Компьютерные системы управления подразделяются на два основных типа: • КСУ технологическими процессами; • компьютерные системы организационно-экономического управления. В основе такого деления лежат объект управления и форма передачи информации об управляемом объекте. Да, так как киберфизические системы (Cyber-Physical System, CPS) представляют собой системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое

4.4. Опишите классы для каждого из существующих типов АСУ.

Ответы:

В ответе на вопрос необходимо показать связь АСУ с технологическим процессом производства на предприятии

Верный ответ: Различают АСУ следующих классов: • О ГАС — общегосударственная автоматизированная система сбора и обработки информации для учета, планирования и управления народным хозяйством страны в целом. Перерабатываемая информация здесь носит экономический характер, причем решение задач планирования увязано с социальными аспектами развития общества. Технической базой ОГАС является государственная сеть вычислительных центров (ГСВЦ), взаимодействующая с единой автоматизированной системой связи страны (ЕАСС); • ОАСУ — отраслевая автоматизированная система управления, объектом

которой является определенная отрасль народного хозяйства страны; • АСУП — автоматизированная система управления предприятием на основе применения ЭВМ и экономико-математических методов для решения основных задач производственно-хозяйственной деятельности. Цель АСУП заключается в обеспечении неуклонного увеличения выпуска продукции путем непрерывного повышения технического я организационного уровня производства; • АСУТП — автоматизированная система управления технологическим процессом, предназначенная для выработки и реализации управляющих воздействий на технологический объект управления (ТОУ) в соответствии с принятым критерием оптимальности. Здесь ТОУ оказывается совокупностью технологического оборудования и реализованного на нем по соответствующим технологическим инструкциям или регламентам технологического процесса производства.

5.5. Какие виды рисков возникают в АСУ, и какова природа каждого из этих рисков?

Ответы:

Для ответа на вопрос можно использовать как качественные так и количественные метрики оценки рисков информационной безопасности

Верный ответ: Риски могут быть существенны: 1. Остановка производства Из-за обычного шифровальщика, запущенного в корпоративную сеть автопроизводителя Honda с целью получения выкупа, компании пришлось на целый день остановить производство на нескольких заводах. После такого вмешательства у компании уйдет немало сил, чтобы вернуться к нормальной работе и обеспечить дальнейшее полноценное функционирование технологических и бизнес-систем, а также не допустить повторного вторжения. 2. Нарушение технологических процессов В мае 2021 года в результате атаки вируса-шифровальщика была нарушена работа Colonial Pipeline — крупнейшего в США поставщика топлива. Из-за недельного простоя компьютерных систем компании закрылась половина заправочных станций в нескольких юго-восточных штатах, выросли оптовые цены на бензин, возник ажиотажный спрос на топливо. В 2020 году злоумышленники пытались атаковать системы водоснабжения и очистки воды в Израиле. А в феврале 2021 года одному хакеру удалось получить доступ к системам водоочистных сооружений в небольшом городе США и изменить химический состав воды. 3. Нарушение бизнес-процессов В феврале 2020 года в результате хакерской атаки хорватская нефтяная компания INA не могла выставлять счета-фактуры, фиксировать использование карт лояльности, выпускать новые мобильные ваучеры и принимать от клиентов плату за топливо. Причиной нарушения бизнес-процессов стала программа-вымогатель Clop, зашифровавшая данные на внутренних серверах компании.

6.6. Как применяется в КСУ принцип защиты в глубину для обеспечения ИБ и для обеспечения ФБ?

Ответы:

Для ответа на вопрос необходимо дать определение термина “защита в глубину” и вспомнить суть принципа “эшелонирование” и “равнопрочность рубежа”

Верный ответ: Принцип защиты в глубину (глубокоэшелонированная защита) Этот принцип занимает особое место среди основных принципов безопасности АЭС. Он предполагает создание ряда последовательных уровней защиты от вероятных от технических средств и ошибок персонала, включая: – установление последовательных физических барьеров на пути распространен радиоактивных продуктов в окружающую среду; –готовность к проведению технических и организационных мероприятий по сохранению целостности и эффективности этих барьеров; –готовность к проведению мероприятий по защите населения и окружающей среды в случае разрушения барьеров. В основе данного принципа лежит установление ряда последовательных физических барьеров (барьеров безопасности), обеспечивающих надежное удержание радиоактивных веществ в

заданных объемах или границах сооружений АЭС (рис. 2.2). Система барьеров включает в себя: –Топливную матрицу (топливную таблетку). –Оболочку тепловыделяющих элементов. –Корпус реактора и границы 1—го контура теплоносителя, выполненные из высокопрочной легированной стали. Радиоактивность в помещениях 1—го контура в 108 раз меньше радиоактивности в топливной таблетке. – Герметичное ограждение локализующих систем безопасности, например, защитную гермооболочку, в которой размещается реактор, оборудование и трубопроводы первого контура. – Биологическую защиту. Основным материалом биологической защиты служат бетон, вода и серпентиновый песок.

7.7. Каким образом взаимосвязаны ИБ и ФБ?

Ответы:

Для ответа на вопрос необходимо верно перевести на русский язык понятия "safety" и “security”

Верный ответ: При выполнении сертификации на соответствие требованиям МЭК 61508 к тому или иному уровню SIL (Safety Integrity Level), важно продемонстрировать, что, во-первых, в продукт заложен необходимый и достаточный механизм обеспечения функциональной безопасности (ФБ), а, во-вторых, что необходимый и достаточный набор методов обеспечения ФБ применялся в процессе разработки. Исходя из этого, условно разделим методы обеспечения ФБ на технические и организационные. Методы обеспечения ФБ направлены на защиту от случайных отказов аппаратных средств, вызванных физическим старением элементов, а также на защиту от систематических отказов, вызванных несовершенством процессов проектирования. Поскольку в современном мире ФБ немыслимо рассматривать в отрыве от информационной безопасности (ИБ), то методы обеспечения ФБ также, в большинстве своем, обеспечивают и защиту от кибератак.

8.8. Как распределяются ошибки проектирования КСУ между этапами жизненного цикла?

Ответы:

Для ответа на вопрос необходимо дать краткое описание жизненного цикла АСУ ТП

Верный ответ: Две основные ошибки при проектировании и программировании АСУ для оборудования такого типа. Первая ошибка – неправильное проектирование релейной части управления главного привода или критичного механизма. Вторая ошибка – недостаток программы в части обработки фатальных ошибок ПЛК.

9.9. Какие вызовы с точки зрения ИБ и ФБ создает быстрый рост количества подключенных к интернету устройств?

Ответы:

Для ответа на вопрос необходимо обратиться к модели угроз ФСТЭКа для КИИ

Верный ответ: Вопросы обеспечения ИБ АСУТП становятся все более актуальными как в связи с ростом интереса зло-умышленников к АСУТП, так и в связи с развитием самих АСУТП, включая: 1. рост потребностей интеграции АСУТП в еди-ную корпоративную систему, связанных, например, со сбором исторических данных, мониторингом со-стояния АСУТП, передачей производственных пара-метров, с созданием центров управления производ-ством уровня завода; 2. передача обслуживания инфраструктуры АСУТП на инсорс/аутсорс, в том числе с возможностью удален-ного подключения через Internet; 3. постепенный переход на использование стан-дартных протоколов на базе Ethernet на «низком» уровне автоматизации; 4. развитие полевого уровня АСУТП: повышение «интеллекта» полевых устройств, использование ра-диоканала на полевом уровне.

10.10. Для каких промышленных отраслей разработаны отдельные стандарты по ФБ?

Ответы:

В ответе необходимо перечислить нормативно-правовые акты в области функциональной и информационной безопасности

Верный ответ: Федеральный закон от 21.11.1995 №170-ФЗ «Об использовании атомной энергии» Федеральный закон от 21.07.1997 №116-ФЗ «О промышленной безопасности опасных производственных объектов» Федеральный закон от 21.07.1997 №117-ФЗ «О безопасности гидротехнических сооружений» Федеральный закон от 09.02.2007 г. №16-ФЗ «О транспортной безопасности» Федеральный закон от 21.07.2011 г. №256-ФЗ «О безопасности объектов топливно-энергетического комплекса» Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

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

III. Правила выставления итоговой оценки по курсу

Для оценки используется только результаты промежуточной аттестации