

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФИЗИКО- МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

УТВЕРЖДАЮ

Руководитель образовательной программы

И.о декана физико-математического
факультета

_____/М.Х. Мальсагов
«20» мая 2024г.

_____/Б.С.Кульбужев
«23» мая 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 Безопасность АСУ ТП

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Технологии искусственного интеллекта и анализа данных

Квалификация выпускника

Бакалавр

Форма обучения

Очная, очно-заочная

Магас, 2024г.

Рабочая программа дисциплины **«Безопасность АСУ ТП»** составлена в соответствии с требованиями ФГОСВО по направлению подготовки 09.03.02- «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 926.

Программу составили:

ассистент кафедры «Информационные системы и технологии» Угурчиева М. А.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол №9 от «20» мая 2024 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол № 9 от «22» мая 2024 года

1. Цели и задачи освоения дисциплины «Безопасность АСУ ТП»

Основной целью изучения дисциплины «Безопасность АСУ ТП» является формирование у обучающегося компетенций для следующих видов деятельности: - проектная; - организационно-управленческая. Задача дисциплины «Обеспечение информационной безопасности АСУ ТП» – получение основополагающих знаний о методах обеспечения безопасности информации на различных объектах за счет руководящих и нормативных документов, а так же внутренних документов организации, и о каналах утечки защищаемой информации.

Целью курса является изучение:

- основных направлений деятельности по обеспечению безопасности АСУ ТП и Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;
- основных понятий в области безопасности АСУ ТП и Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры(КИИ);
- основных угроз, уязвимостей, рисков в области безопасности АСУ ТП и Интернета вещей, киберфизических систем в составе объектов КИИ;
- технологий реализации угроз сетевой безопасности, а также механизмов противодействия сетевым атакам;
- основных требований нормативно-правовых документов по категорированию и защите объектов КИИ;
- особенностей проектирования систем безопасности объектов КИИ.

Формируемые дисциплиной знания и умения готовят выпускника данной образовательной программы к выполнению следующих обобщенных трудовых функций (трудовых функций):

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Уровень квалификации	Наименование	Код	Уровень (подуровень) квалификации
06.015 Специалист по информационным системам	С	Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.	6	Определение первоначальных требований заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ	С/01.6	6
				Документирование существующих бизнес-процессов организации заказчика (реверс-инжиниринг бизнес-процессов организации)	С/07.6	6
				Разработка модели бизнес-процессов заказчика	С/08.6	6
				Разработка архитектуры ИС	С/14.6	6
				Проектирование и дизайн ИС	С/16.6	6

2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «**Безопасность АСУ ТП**» относится к базовой части Б1. До начала ее изучения студенту необходимо **освоить** содержание учебных дисциплин: «Информатика», «Операционные системы», «Администрирование в информационных системах».

Код дисциплины	Дисциплины, следующие за дисциплиной «Теория информационных процессов и систем»	Семестр
Б1.О.06	Информатика	2
Б1.В.03	Операционные системы	3
Б1.В.08	Администрирование в информационных системах	7

Дисциплина «**Безопасность АСУ ТП**» является **предшествующей дисциплинам:** «Методы и средства проектирования информационных систем и технологий», «Программирование промышленных логических контроллеров», «Проектирование информационного обеспечения САПР»

Код дисциплины	Дисциплины, следующие за дисциплиной «Теория информационных процессов и систем»	Семестр
Б1.В.11	Методы и средства проектирования информационных систем и технологий	8
Б1.В.05	Программирование промышленных логических контроллеров	8
Б1.В.ДВ.03.01	Проектирование информационного обеспечения САПР	8

3. Результаты освоения дисциплины «Безопасность АСУ ТП»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Универсальные компетенции (УК) и индикаторы их достижения:

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
УК-1	УК-1. Способен осуществлять поиск, критический анализ информации, применять системный подход для решения поставленных задач.	ИУК-1.1.Анализирует задачу, выделяя ее базовые составляющие. ИУК-1.2.Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи. ИУК-1.3. Осуществляет поиск информации для решения поставленной задачи по различным типам запросов. ИУК-1.4. При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения ИУК-1.5. Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки.	УК-1.1. Знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа.
			УК-1.2. Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач.
			УК-1.3. Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.

Общепрофессиональные компетенции (ОПК) и индикаторы их достижения для программ бакалавриата:

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине

ОПК-5	ОПК-5: Способность объективно оценивать результаты исследований и разработок, выполненных другими специалистами в других научных учреждениях	ИОПК-5.1. Использует современные информационные технологии при решении задач профессиональной деятельности ИОПК-5.2. Использует программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ОПК-5.1. Знать: научные проблемы в выбранной области исследования и основные нормы общения, принятые в научных кругах ОПК-5.2. Уметь: критически оценивать результаты исследований и разработок, выполненных другими специалистами и в других научных учреждениях ОПК-5.3. Владеть: способностью критически оценивать научные достижения в рассматриваемой области
-------	--	---	---

4. Структура и содержание дисциплины «Безопасность АСУ ТП»

4.1. Структура дисциплины «Безопасность АСУ ТП»

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часов.

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости (по неделям семестра)						
			Контактная работа					Самостоятельная работа				Форма промежуточной аттестации (по семестрам)						
			Всего	Лекции	Практические занятия	Лабораторные занятия	Др. виды контакт. работы	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельной-работы	Собеседование	Коллоквиум	Проверка тестов	Проверка контрол.н. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект) др.
1.	Модуль 1 Угрозы и уязвимости безопасности АСУ ТП																	
1.1.	Тема 1.1. Основные понятия и определения ИБ АСУ ТП	5	4	2		2		4					2					
1.2.	Тема 1.2. Угрозы безопасности киберфизических систем	5	6	4		2		4					2					
1.3.	Тема 1.3. Сетевые технологии и протоколы связи и аутентификации для киберфизических систем	5	6	4		2		6					4	2				
1.4.	Тема 1.4. Обеспечение безопасности сетевой инфраструктуры объектов АСУ ТП	5	6	2		4		6					4	2				
1.5.	Тема 1.5. Средства управления и конфигурирования ПО АСУ ТП	5	4	2		2		6					4	2				
1.6.	Тема 1.6. Методы сохранности информации при авариях	5	8	4		4		4					4					
2.	Модуль 2 Обеспечение безопасности АСУ ТП и КИИ																	
2.1.	Тема 2.1. Методики и руководящие документы по категорировании объектов АСУ ТП	5	8	4		4		4					4					
2.2.	Тема 2.2. Проектирование безопасной инфраструктуры объектов АСУ ТП	5	8	4		4		4					4					

2.3.	Тема 2.3. Защита информации АСУ ТП от несанкционированного доступа	5	10	6		4	4					4				
2.4	Тема 4.4. Методы безопасного управления изменениями в ПО и сетевом оборудовании объектов АСУ ТП	5	8	4		4	9					4	5			
	<i>Курсовая работа (проект)</i>															
	<i>Подготовка к экзамену</i>															
	Общая трудоемкость, в часах															
	Промежуточная аттестация															
	Форма		144	36		32	49									
	Зачет															
	Зачет с оценкой															
	Экзамен															

4.3 Содержание учебного материала

Раздел 1. Основные понятия и определения ИБ АСУ ТП.

Киберфизические системы и «Интернет-вещей» соотношение понятий. Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интернет-вещей»: основные стандарты, понятия, определения.

Раздел 2. Угрозы безопасности киберфизических систем.

Угрозы, уязвимости, риски АСУ ТП. АСУ ТП в сфере здравоохранения – риски и проблемы. «Умный дом» риски и проблемы. Юридические инциденты – примеры. Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан. Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибербезопасностью; основные угрозы и уязвимости в сфере кибербезопасности. Регулирование вопросов кибербезопасности в «Интернет-вещей»: международное, в РФ.

Раздел 3. Сетевые технологии и протоколы связи и аутентификации для киберфизических систем.

Сетевые технологии и протоколы – модель OSI, проблемы безопасности. Протоколы связи и аутентификации для киберфизических систем и «Интернет-вещей»: обзор, особенности, проблемы безопасности.

Раздел 4. Обеспечение безопасности сетевой инфраструктуры объектов АСУ ТП.

Основные подсистемы обеспечения ИБ объектов КИИ. Средства обеспечения кибербезопасности (обзор). «Умный город»: состав систем (категории систем, классификация), зрелость Smart City: понятие, критерии оценки, угрозы, риски и проблемы, модель угроз (структура, особенности), обзор стандартов по направлению «Умный город» (Smart City). «Интернет-вещей» и его применение в Smart Grid, проблемы кибербезопасности.

Раздел 5. Средства управления и конфигурирования ПО АСУ ТП.

Функциональная безопасность: основные стандарты, понятия и определения. Обзор основных стандартов в сфере функциональной безопасности.

Раздел 6. Методы сохранности информации при авариях.

Архитектура, обеспечивающая сохранность баз данных, файлов данных на файловых серверах. Методы и средства и регламенты восстановления данных. Построение системы долговременного архивирования данных и файлов для обеспечения сохранности в случае инцидентов ИБ, пожаров, стихийных бедствий.

Раздел 7. Методики и руководящие документы по категорированию объектов АСУ ТП.

Критическая информационная инфраструктура, основные понятия, стандарты. Критическая информационная инфраструктура РФ, основные понятия, НПА, требования. Категорирование объектов КИИ РФ, порядок и критерии

Раздел 8. Проектирование безопасной инфраструктуры объектов АСУ ТП.

Проектирование систем безопасности значимых объектов КИИ. Требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры. Построение СМИБ для объектов КИИ на промышленных объектах: Обзор стандартов семейства ISO / ГОСТ 27К. Состав СМИБ. Особенности создания СМИБ для объектов КИИ на промышленных объектах

Раздел 9. Защита информации АСУ ТП от несанкционированного доступа.

Киберфизические системы и «Интернет-вещей» в промышленности: понятие «Индустриальный Интернет-вещей», соотношение с понятием «киберфизическая система», классификация продуктов «Интернет-вещей», соотношение с понятиями АСУ ТП, ICS; угрозы, уязвимости, риски.

Раздел 10. Методы безопасного управления изменениями в ПО и сетевом оборудовании объектов АСУ ТП.

Силы обеспечения кибербезопасности объектов КИИ. Ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК

5. Образовательные технологии

Для успешного освоения дисциплины применяются различные образова-

тельные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме.

Для изучения дисциплины предлагается сочетание традиционных образовательных технологий в форме лекций с интерактивными элементами, информационными технологиями при выполнении лабораторных работ и проведении контрольных мероприятий.

По дисциплине предусмотрены следующие варианты активные формы обучения:

- лекции-визуализации – с использованием презентационного материала;
- лабораторные работы, реализующие проектный метод.

Наряду с традиционными образовательными технологиями, для реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологий в электронной информационно-образовательной среде Южного федерального университета. Лекционные занятия и другие формы контактной работы обучающихся с преподавателем могут проводиться с использованием платформ Microsoft Teams, Cisco, Moodle (BigBlueButton) и др., что позволяет обеспечить онлайн и офлайн взаимодействие преподавателя с обучающимися в рамках дисциплины.

Основными методами текущего контроля являются электронный учёт и контроль учебных достижений студентов (использование средств сервиса балльно-рейтинговой системы; ведение электронного журнала успеваемости, проведение электронного тестирования и применение других средств контроля с использованием системы электронного обучения).

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1.1	Тема 1.1. Основные понятия и определения ИБ АСУ ТП	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4

			материал		
1.2	Тема 1.2. Угрозы безопасности киберфизических систем	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
1.3	Тема 1.3. Сетевые технологии и протоколы связи и аутентификации для киберфизических систем	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
1.4.	Тема 1.4. Обеспечение безопасности сетевой инфраструктуры объектов АСУ ТП	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
1.5.	Тема 1.5. Средства управления и конфигурирования ПО АСУ ТП	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	6
1.6.	Тема 1.6. Методы сохранности информации при авариях	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	6
2.1.	Тема 2.1. Методики и руководящие документы по категорированию объектов АСУ ТП	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
2.2.	Тема 2.2. Проектирование безопасной инфраструктуры объектов АСУ ТП	Тест	Подготовиться к тесту, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
2.3.	Тема 2.3. Защита информации АСУ ТП от несанкционированного доступа	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изучить пройденный материал	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	4
2.4.	Тема 4.4. Методы безопасного управления изменениями в ПО	Коллоквиум	Подготовиться к коллоквиуму, разобрать и изу-	[1]-[4](ол) [1]-[2](дл) Интернет-ресурсы	9

	и сетевом оборудовании объектов АСУ ТП		чить пройденный материал		
	Итого:				49

6.2. Методические указания по организации самостоятельной работы студентов

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, практические занятия, самостоятельную работу студента, консультации.

- а. При изучении тем студентам необходимо повторить лекционный учебный материал, изучить рекомендованную литературу, а также учебный материал, находящийся в указанных информационных ресурсах.

На завершающем этапе изучения каждого модуля необходимо, воспользовавшись предложенными вопросами для самоконтроля, размещенными в электронной информационной образовательной среде (ЭИОС), проверить качество усвоения учебного материала.

В случае затруднения в ответах на поставленные вопросы рекомендуется повторить учебный материал.

- б. После изучения каждого модуля дисциплины необходимо ответить на вопросы контрольного теста по данному модулю с целью оценивания знаний и получения баллов.
- с. После изучения всех модулей приступить к выполнению контрольной работы, руководствуясь методическими рекомендациями по ее выполнению.
- д. По завершению изучения учебной дисциплины в семестре студент обязан пройти промежуточную аттестацию. Вид промежуточной аттестации определяется рабочим учебным планом. Форма проведения промежуточной аттестации - компьютерное тестирование с использованием автоматизированной системы тестирования знаний студентов в ЭИОС.
- е. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов.

Контрольная работа № 1. Варианты тестовых вопросов

- 1) Угроза информационной безопасности:

- * Все вышеперечисленное
- * То же самое, что компьютерная атака
- * Потенциальное нарушение требований к свойствам информации
- * Является причиной уязвимости

2) Какое из следующих утверждений верно для промышленных систем?

- * Большинство атак на промышленные системы являются целевыми атаками
- * Случайный или направленный характер атаки зависит от географического расположения промышленного объекта
- * Большинство атак на промышленные системы являются ненаправленными, случайными атаками
- * Случайный или направленный характер атаки зависит от принадлежности промышленного объекта к критической инфраструктуре

3) Особенности угроз информационной безопасности для промышленных автоматизированных систем управления:

- * Особо важными последствиями реализации угрозы часто являются нарушения целостности и доступности информационного сигнала.
- * Возможен несанкционированный доступ к системе
- * Возможно нарушение работы оборудования
- * Последствия реализации угрозы не только в информационном, но и в физическом окружении системы.

4) Следующие факторы определяют подверженность промышленной системы компьютерным атакам

- * Плохая осведомленность людей, имеющих доступ к системе, об актуальных угрозах информационной безопасности
- * Все перечисленные варианты верны
- * Высокая связность сетей, подсистем и компонентов промышленной системы, и связанная с этим сложность
- * Количество сценариев доступа к системе

5) По статистике, промышленные системы наиболее часто подвергаются атакам с использованием вредоносных программ

- * Через съемные носители, подключаемые к промышленному компьютеризованному оборудованию
- * Через сетевые папки и облачные хранилища, используемые в сети промышленного предприятия
- * Через почтовые клиенты в сети промышленного предприятия
- * Через Интернет, к которому на постоянной или периодической основе подключаются системы и сети промышленного предприятия

6) Какое из следующих утверждений верно для промышленных систем?

- * Проблемы информационной безопасности важнее, чем проблемы функциональной безопасности
- * Информационная и функциональная безопасность должны рассматриваться независимо, т.к. они не связаны между собой
- * Проблемы функциональной безопасности важнее, чем проблемы информационной безопасности
- * Информационная и функциональная безопасность не важны для систем промышленных систем

7) По мнению специалистов, в последнее время угрозы информационной безопасности промышленной автоматизации

- * Похожи на угрозы в корпоративных системах, за исключением угроз для вебтехнологий
- * В основном обусловлены уязвимостью веб-технологий
- * Становятся все более похожими на угрозы в корпоративных системах
- * Становятся все более специфичными и непохожими на угрозы в корпоративных системах

8) Уязвимости в корпоративных приложениях

- * Могут приводить к успешным атакам на эти приложения, но не опасны для промышленных систем
- * Могут приводить к успешным атакам на корпоративные и подключенные к ним промышленные системы
- * Могут приводить к успешным атакам на корпоративные и подключенные к ним промышленные системы
- * Могут приводить к успешным атакам на промышленные системы, но не представляют угрозы для их функциональной безопасности

9) Вирусы для программируемых логических контроллеров (ПЛК)

- * Существуют и успешно подавляются специализированным антивирусным ПО для ПЛК
- * Существуют и свободно распространяются в промышленных системах (in-the-wild)
- * Не существуют
- * Существуют в виде экспериментальных образцов, представленных исследователями

10) Различия между корпоративными сетями и системами промышленной автоматизации с точки зрения информационной безопасности обусловлены различием

- * Рисков безопасности, связанных со схожими угрозами в этих системах
- * Целей обеспечения безопасности и их приоритетов

- * Возможных типов уязвимостей в программном коде
- * Доступных методов обеспечения безопасности

11) Защита от вредоносных программ в любой промышленных системе может быть Реализована

- * При помощи комплекса мер, включая антивирусное ПО, специализированное или общего назначения
- * Исключительно при помощи специализированного антивирусного ПО
- * При помощи комплекса мер, включающего в отдельных случаях специализированное антивирусное ПО
- * При помощи антивирусного ПО, специализированного или общего назначения

12) Управление обновлениями в промышленной системе затруднено следующими факторами

- * Необходимость синхронизации с графиком технического обслуживания и предварительным тестированием обновлений
- * Широкое распространение поддельных обновлений
- * Высокая стоимость возможного отказа после установки обновления
- * Высокая стоимость остановки процесса и простоя оборудования

13) Срок службы технологий информационной безопасности

- * Не имеет значения, т.к. время не влияет на стойкость технологий информационной безопасности
- * Может быть продлен с помощью переконфигурации и замены ключей на срок службы технологий промышленной автоматизации
- * Как правило меньше срока службы технологий промышленной автоматизации, но это не является проблемой, так как при необходимости могут быть внедрены новые технологии защиты
- * Как правило меньше срока службы технологий промышленной автоматизации, и это является проблемой для обеспечения их безопасности

14) Управление изменениями в информационной системе – это

- * Внедрение новых технологий и компонентов
- * Регулярное обновление программного обеспечения
- * Переконфигурация, настройка системы и компонентов, управление учетными записями
- * Процесс, связанный с поддержкой вышеперечисленных мероприятий и управлением их зависимостями и возможными последствиями

15) Какой из следующих вопросов следует рассмотреть в первую очередь при обновлении компонентов промышленных систем?

- * Предоставил ли производитель исходный текст обновления?

- * Как поддерживается непрерывность промышленного процесса в процессе обновления?
- * Какие криптографические средства встроены в новые компоненты?
- * Присутствует ли представитель производителя при установке обновления?

16) Особенности расследования инцидентов в промышленных системах

- * Трудность сбора данных из-за скудных средств мониторинга информационной среды
- * Трудность обнаружения инцидентов вплоть до наступления последствий
- * Необходимость наличия собственной команды для расследования
- * Необходимость совместной работы специалистов разного профиля

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

- 1.Итоговый контрольный тест доступен студенту только во время тестирования, согласно расписанию занятий или в установленное деканатом время.
- 2.Студент информируется о результатах текущей успеваемости.
- 3.Студент получает информацию о текущей успеваемости и допуске к процедуре итогового тестирования от преподавателя или в ЭИОС.
- 4.Производится идентификация личности студента.
- 5.Студентам, допущенным к промежуточной аттестации, открывается итоговый контрольный тест.
- 6.Тест закрывается студентом лично по завершении тестирования или автоматически по истечении времени тестирования.

Опрос устный

Опрос устный - диалог преподавателя со студентом, цель которого - систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.

Устный опрос по основным терминам может проводиться в начале/конце лекционного или практического занятия в течение 15 -20 мин. Либо устный опрос проводится в течение всего практического занятия по заранее выданной тематике. Выбранный преподавателем студент может отвечать с места либо у доски.

Критериями оценки устного опроса являются: правильность ответа на вопросы, степень раскрытия сущности вопроса.

Оценка «**отлично**» — дан полный, всесторонний ответ на вопрос. Точность в определениях. Приведение примеров из практики.

Оценка «**хорошо**» — дан неполный ответ на вопрос. Допущены неточности при ответе. Допущены неточности в основных определениях.

Оценка «**удовлетворительно**» — имеются существенные недочеты при ответе. Вопрос раскрыт частично. Незнание базовых определений курса.

Оценка «**неудовлетворительно**» — вопрос не раскрыт или дан неверный ответ.

Тесты

Тесты - инструмент, с помощью которого педагог оценивает степень достижения студентом требуемых знаний, умений, навыков. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.

Критерии оценки теста: Оценка «**отлично**» выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий;

Оценка «**хорошо**» выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий;

Оценка «**удовлетворительно**» выставляется при условии правильного ответа студента не менее 51 %; .

Оценка «**неудовлетворительно**» выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Контрольная работа

Контрольная работа - средство промежуточного контроля остаточных знаний и умений, состоит из вопросов или заданий, которые студент должен решить, выполнить. Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме.

Критерии оценки контрольной работы для студентов заочного отделения: Оценка «**зачтено**» ставится за полные ответы на все вопросы.

Оценка «**не зачтено**» ставится, если освещены не все вопросы требуемого материала или не описано главное в содержании вопросов, или письменная работа не сдана.

Коллоквиум

Коллоквиум (в переводе с латинского «беседа, разговор») – форма текущего контроля знаний студентов, которая проводится в виде собеседования преподавателя и студента по самостоятельно подготовленной студентом теме.

Он применяется для проверки знаний по определенному разделу (или объемной теме) и принятия решения о том, можно ли переходить к изучению нового материала. Коллоквиум — это беседа со студентами, целью которой является выявление уровня овладения новыми знаниями. В отличие от семинара главное на коллоквиуме — это проверка знаний с целью их систематизации.

Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы.

На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Коллоквиум может проводиться по вопросам, обсуждавшимся на семинарах. Конкретные вопросы для коллоквиума студентам не сообщаются, однако заранее формулируются преподавателем. Предполагаемый объем ответа не должен быть большим (примерно 1,5-2 минуты), чтобы преподаватель мог успеть опросить всех студентов.

От студента требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Коллоквиум — это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника.

Задача коллоквиума добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной экономической литературы.

Подготовка к проведению коллоквиума.

Подготовка к коллоквиуму предполагает несколько этапов:

1. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума.

2. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3–4 недели. Подготовка включает в себя изучение рекомендованной литературы и (по указанию преподавателя) конспектирование важнейших источников.

3. Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (3–5 человек).

4. Преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, контролирует конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания.

5. По итогам коллоквиума выставляется дифференцированная оценка, имеющая большой удельный вес в определении текущей успеваемости студента.

Особенности и порядок сдачи коллоквиума. Студент может себя считать готовым к сдаче коллоквиума по избранной работе, когда у него есть им лично составленный и обработанный конспект сдаваемой работы, он знает структуру работы в целом, содержание работы в целом или отдельных ее разделов (глав); умеет раскрыть рассматриваемые проблемы и высказать свое отношение к прочитанному и свои сомнения, а также знает, как убедить преподавателя в правоте своих суждений.

Проведение коллоквиума позволяет студенту приобрести опыт работы над первоисточниками, что в дальнейшем поможет с меньшими затратами времени работать над литературой по курсовой работе и при подготовке к экзаменам.

Экзамен

Экзамен - итоговая форма оценки знаний.

Проводится в заданный срок, согласно графику учебного процесса.

Критерии оценки при проведении экзамена:

Оценка "отлично" ставится, если студент обнаружил полное знание учебно-программного материала, успешно выполняет предусмотренные в

программе задания, усвоил основную литературу, рекомендованную в программе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Студент уверенно отвечает на дополнительные вопросы

Оценка «хорошо» ставится в том случае, когда студент обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком. При этом могут допускаться некоторые погрешности в ответе на зачете, если студент обладает необходимыми знаниями для их устранения под руководством преподавателя.

Оценка «удовлетворительно» ставится в том случае, когда студент обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. Студент испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему проблемы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала или допущен ряд существенных ошибок, которые студент не может исправить при наводящих вопросах экзаменатора. Студент подменил научное обоснование проблем рассуждением бытового плана. Ответ носит поверхностный характер; наблюдаются неточности в использовании научной терминологии.

6.5. Экзаменационные вопросы по дисциплине «Безопасность АСУ ТП»

1. Основные понятия в области кибербезопасности АСУ ТП и Интернета вещей.
2. Основные угрозы, риски и уязвимости в сфере кибербезопасности АСУ ТП и критической информационной инфраструктуры.
3. Основные протоколы передачи данных и аутентификации, используемые в АСУ ТП и Интернете вещей.
4. Основные понятия в сфере функциональной безопасности.
5. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации.
6. Архитектура основных подсистем обеспечения ИБ объектов КИИ.
7. Основные определения системы обеспечения ИБ и особенности построения системы обеспечения ИБ для объектов КИИ на промышленных объектах.
8. Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
9. Основные средства обеспечения кибербезопасности (архитектура, принципы построения).
10. Принципы проектирования безопасной инфраструктуры объектов АСУ ТП и значимых объектов КИИ.
11. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ.
12. Основные требования к специалистам в области кибербезопасности АСУ ТП и Интернета вещей, критической информационной инфраструктуры.
13. Цели обеспечения кибербезопасности в АСУ ТП и Интернете вещей для граждан.
14. Классификация и примеры продуктов «Интернет-вещей» для граждан, примеры угроз, уязвимостей, рисков.
15. Основные риски и проблемы кибербезопасности АСУ ТП в сфере здравоохранения.
16. Основные риски и проблемы кибербезопасности для «Умного дома».
17. Состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз.
18. Основные риски и проблемы кибербезопасности в Smart Grid.
19. Основные риски и проблемы кибербезопасности в АСУ ТП.

20. Примеры юридических инцидентов в области регулирования кибербезопасности АСУ ТП.
21. Методы и средства обеспечения безопасности сетевой инфраструктуры объектов АСУ ТП.
22. Примеры инцидентов ИБ в АСУ ТП (kill-chain, скомпрометированная инфраструктура, последствия).
23. Методы сохранности информации при авариях.
24. Методики и руководящие документы по категорированию объектов АСУ ТП.
25. Защита информации АСУ ТП от несанкционированного доступа.
26. Методы безопасного управления изменениями в ПО и сетевом обслуживании объектов АСУ ТП.

7. Учебно-методическое и материально-техническое обеспечение дисциплины

8.

7.1. Учебная литература:

Основная литература.

1. Петренко С. А., Смирнов М. Б. Безопасность АСУТП и критической информационной инфраструктуры // СПб.: ООО «ИД «Афина». – 2018. ISBN 978-5-9909868-1-7. Учебно-методическое пособие [<https://avtoritet.net/library/books/bezopasnostasutp-i-kriticheskoy-informacionnoy-infrastruktury>].
2. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении. (СПб.: ООО «ИД «Афина». – 2017. ISBN 978-5-99098680-0). [<https://www.elibrary.ru/item.asp?id=29402725>].
3. Petrenko, Sergei (2018) Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation [<https://www.springer.com/gp/book/9783319790350>].
4. Ginter Andrew, Secure Operation Technology // Abterra Technology – 2018. ISBN13 9780995298439 [<https://waterfall-security.com/secure-operations-technology-the-missing-link-to-a-secure-industrial-site/>]

Дополнительная литература.

5. Что такое Интернет вещей (Internet of Things, IoT) [Электронный ресурс]. Режим доступа: <http://tadviser.ru/a/135141> (дата обращения 25.06.2018).
6. ОБСЕ. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства. 5 марта 2013 г.
7. <http://www.osce.org/ru/secretariat/110472>
8. Обеспечение безопасности АСУТП – краткий обзор семейства стандартов IEC 62443 <http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiyobzorsemeystva-standartov-iec-62443>
9. Европейское агентство по кибербезопасности ENISA опубликовало анализ стандартов, касающихся поставщиков услуг доверия. 22.07.2016 <http://rusrim.blogspot.ru/2016/07/enisa.html> Документ доступен по адресу https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport
10. Substation Communications Design Legacy to IEC 61850 Best Practices <http://info.belden.com/substation-design-wp1-lp-bc>
11. Коммуникации между подстанциями и центрами управления – в соответствии с МЭК 61850 <http://digitalsubstation.ru/blog/2015/11/10/kommunikatsii-mezhdupodstantsiyami-itsentrami-upravleniya-v-sootvetstvii-s-mek-nbsp-61850/>
12. Cyber Security for Power Utilities. How to Protect Your Network in a Hyper-Connected Environment http://www.rad.com/21/Cyber-Security-for-Power-Utilities-WhitePaper/30757/?utm_source=google&utm_medium=cpc&utm_campaign=utilities-firewall

7.2. Интернет-ресурсы

Название ресурса	Ссылка/доступ
Электронная библиотека онлайн «Единое окно к образовательным ресурсам»	http://window.edu.ru
«Образовательный ресурс России»	http://school-collection.edu.ru
Федеральный образовательный портал: учреждения, программы, стандарты, ВУЗы, тесты ЕГЭ, ГИА	http://www.edu.ru
Федеральный центр информационно-образовательных ресурсов (ФЦИОР)	http://fcior.edu.ru
Русская виртуальная библиотека	http://rvb.ru
Кабинет русского языка и литературы	http://ruslit.ioso.ru
Национальный корпус русского языка	http://ruscorpora.ru
Научная электронная библиотека «e-Library»	http://elibrary.ru/defaultx.asp

Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
Электронно-библиотечная система ИнГУ	https://lib.inggu.ru/
Информационно-правовая система «Гарант»	Сетевая версия, доступна со всех компьютеров в корпоративной сети ИнГУ

7.3. Программное обеспечение

- 1.1. Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10
- 1.2. Microsoft Windows server 2003, 2008, 2012, 2016
- 1.3. Microsoft Office 2007, 2010, 2016

7.4. Материально-техническое обеспечение

1. Мультимедийные аудитории.
2. Библиотека.
3. Справочно-правовая система «Гарант».
4. Электронная информационно-образовательная среда университета.
5. Локальная сеть с выходом в Интернет.
6. Виртуальные аналоги специализированных кабинетов и лабораторий.

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедр- ры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедр- рой