

**Федеральное государственное бюджетное учреждение науки
Институт машиноведения им. А.А. Благонравова
Российской академии наук
(ИМАШ РАН)**

УТВЕРЖДАЮ
Заместитель директора по вопросам
подготовки кадров высшей
квалификации ИМАШ РАН
И.Ф.-м.н. Жданов Э.Р.
« 01 » _____ 2026 года
М.П.



**Комплект оценочных материалов
по дисциплине «Защищенные системы управления промышленными
объектами»**

Направление подготовки:	09.04.03 Прикладная информатика
Профиль подготовки:	Цифровые двойники и автоматизированные системы управления технологическими процессами
Квалификация:	Магистр
Форма обучения	Очная

Содержание

1. Общие положения.....	3
2. Результаты освоения дисциплины, подлежащие проверке.....	3
3. Контроль и оценка освоения учебной дисциплины.....	5
4. Оценочные материалы для проведения текущего контроля успеваемости.....	5
5. Оценочные материалы для проведения промежуточной аттестации.....	7

1. Общие положения

Комплект оценочных материалов (далее - ОМ) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу дисциплины «Защищенные системы управления промышленными объектами».

ОМ включают контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации в форме зачета.

ОМ разработаны на основании:

- основной профессиональной образовательной программы по направлению подготовки 09.04.03 Прикладная информатика;
- рабочей программы дисциплины «Защищенные системы управления промышленными объектами».

2. Результаты освоения дисциплины, подлежащие проверке

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями

ПК-1	Способен руководить процессами разработки и реализации проекта автоматизированной системы управления технологическими процессами
ПК-1.1	Разрабатывает концепции и техническое задание на проектирование автоматизированной системы управления технологическими процессами
ПК-1.2	Контролирует разработку проекта автоматизированной системы управления технологическими процессами
ПК-2	Способен управлять цифровой трансформацией документированных сфер деятельности организации
ПК-2.1	Развивает цифровую трансформацию документированных сфер деятельности организации

Код индикатора компетенции	Планируемые результаты обучения по дисциплине
ПК-1.1	<i>Знать:</i> - специфику угроз информационной безопасности для промышленных объектов, включая векторы атак на полевой уровень (ПЛК, датчики), сети и системы верхнего уровня (SCADA); - принципы построения эшелонированной (Defense-in-Depth) и зональной защиты, а также архитектурные модели (например, Purdue/ISA-95) для обеспечения безопасности АСУ ТП; - нормативно-правовую базу и отраслевые стандарты (включая требования регуляторов РФ), регламентирующие проектирование и эксплуатацию защищенных систем управления; - требования к выбору программно-аппаратных средств защиты (межсетевые экраны, IDS/IPS, средства защиты конечных узлов) с учетом специфики промышленных протоколов. <i>Уметь:</i> - анализировать объект автоматизации с точки зрения выявления критических активов и потенциальных угроз их безопасности; - формулировать требования по информационной безопасности в составе технического задания, включая требования к архитектуре сети, средствам защиты и организационным мерам; - применять принципы сегментации сети и проектирования демилитаризованных зон (DMZ) при разработке концепции системы; - оценивать риски безопасности и определять необходимые меры по их минимизации на этапе формирования концепции проекта. <i>Иметь практический опыт:</i> - разработки раздела «Информационная безопасность» для технического

	задания на проектирование фрагмента АСУ ТП; - проектирования архитектуры защищенной сети для условного промышленного объекта с разделением на уровни.
ПК-1.2	<i>Знать:</i> - требования нормативных документов и стандартов в области защиты информации критической информационной инфраструктуры (КИИ) и АСУ ТП, применимые к проектной документации; - принципы организации и проведения контроля за соблюдением требований информационной безопасности на всех этапах жизненного цикла разработки проекта (от технического задания до ввода в эксплуатацию); - методики анализа проектной документации на предмет соответствия утвержденным архитектурным решениям и политикам безопасности; <i>Уметь:</i> - проверять проектную документацию (разделы по ИБ, схемы сетей, спецификации на оборудование) на соответствие требованиям технического задания и нормативным актам; - выявлять несоответствия и уязвимости в проектных решениях, связанных с архитектурой сети, настройками средств защиты и логикой управления доступом; - организовывать взаимодействие с разработчиками и смежными подразделениями для согласования изменений в проекте, направленных на устранение выявленных недостатков в части безопасности. <i>Иметь практический опыт:</i> - разработки замечаний и рекомендаций по результатам анализа проектной документации для внесения изменений, повышающих уровень защищенности системы.
ПК-2.1	<i>Знать:</i> - роль и место информационной безопасности как фундаментального элемента стратегии цифровой трансформации промышленных предприятий; - специфические киберриски, возникающие при внедрении новых цифровых технологий (Интернет вещей, облачные вычисления, цифровые двойники) в традиционные производственные процессы; - методы оценки влияния угроз информационной безопасности на непрерывность технологических процессов и экономическую эффективность предприятия; - принципы интеграции систем защиты информации в единую экосистему цифрового предприятия для обеспечения безопасного обмена данными. <i>Уметь:</i> - анализировать существующие бизнес-процессы и технологические цепочки с целью выявления точек, где внедрение цифровых решений требует первоочередного усиления мер кибербезопасности; - аргументировать необходимость инвестиций в информационную безопасность как в инструмент обеспечения стабильности и эффективности цифровой трансформации; - оценивать зрелость процессов обеспечения информационной безопасности в организации и определять их готовность к переходу на новые цифровые модели управления; - разрабатывать предложения по модернизации систем защиты в соответствии с меняющимися требованиями цифровой среды. <i>Иметь практический опыт:</i> - выполнения анализа кейса по цифровой трансформации предприятия с подготовкой отчёта, включающего оценку киберрисков и предложения по созданию системы защиты для новых цифровых активов; - разработки дорожной карты (в рамках учебного проекта) по внедрению элементов кибербезопасности в стратегию цифровизации конкретного производственного подразделения.

3. Контроль и оценка освоения учебной дисциплины

Элемент учебной дисциплины	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые идк	Форма контроля	Проверяемые идк
Тема 1. Введение в кибербезопасность АСУ ТП / КФС	Дидактическая игра	ПК-1.1 ПК-2.1		
Тема 2. Архитектура безопасности промышленных сетей	Отчет по практикуму по решению задач	ПК-1.1 ПК-1.2		
Тема 3. Средства и методы технической защиты	Отчет по практикуму по решению задач	ПК-1.1 ПК-1.2		
Тема 4. Управление доступом и мониторинг безопасности	Отчет по практикуму по решению задач	ПК-1.1 ПК-1.2		
Тема 5. Нормативно-правовое регулирование и управление рисками	Отчет по практикуму по решению задач/	ПК-1.1 ПК-1.2 ПК-2.1		
			Зачет	ПК-1.1 ПК-1.2 ПК-2.1

4. Оценочные материалы для проведения текущего контроля успеваемости

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Практикум по решению задач
20-15 – работа и отчет выполнены в срок, самостоятельно, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 14-9– работа и отчет выполнены в срок, самостоятельно, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 8-3 – работа и отчет выполнены в срок, в основном самостоятельно, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 2-1 – обучающийся подготовил работу и отчет самостоятельно и/или не завершил в срок, описание содержит ошибки, выводы и ответы на вопросы отсутствуют.
Дидактическая игра
20-18 – студент принимает активное участие в работе группы, предлагает собственные варианты решения проблемы, выступает от имени группы с рекомендациями по рассматриваемой проблеме либо дополняет ответчика; демонстрирует предварительную информационную готовность в игре; 17-12 - студент принимает активное участие в работе группы, участвует в обсуждениях, высказывает типовые рекомендации по рассматриваемой проблеме, готовит возражения оппонентам, однако сам не выступает и не дополняет ответчика; демонстрирует информационную готовность к игре 11-5- студент принимает участие в обсуждении, однако собственной точки зрения не высказывает, не может сформулировать ответов на возражения оппонентов, не выступает от имени рабочей группы и не дополняет ответчика; демонстрирует слабую информационную подготовленность к игре 4-1 – студент принимает участие в работе группы, однако предлагает не аргументированные, не

подкрепленные фактическими данными решения; демонстрирует слабую информационную готовность

0 – студент не принимает участия в работе группы, не высказывает никаких суждений, не выступает от имени группы; демонстрирует полную неосведомленность, по сути, изучаемой проблемы

Порядок начисления баллов

Если студент набрал достаточное количество баллов ТКУ по дисциплине (более 70 баллов) в течение семестра, он может отказаться от сдачи зачета, и результат будет выставлен автоматически по его согласию.

Типовые контрольные задания и иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и(или) опыта деятельности

Типовые задания практикумов по решению задач

Тема 2. Архитектура безопасности промышленных сетей

Задача: Разработка архитектуры сегментации сети для условного завода с выделением уровней управления, контроля и полевых устройств.

Тема 3. Средства и методы технической защиты

Задача: Анализ логов промышленного межсетевого экрана для выявления аномальной активности (сканирование портов, попытки неавторизованного доступа).

Тема 4. Управление доступом и мониторинг безопасности

Задача: Разработка матрицы доступа для операторов, инженеров и администраторов SCADA-системы. Анализ сценария инцидента на основе данных SIEM.

Тема 5. Нормативно-правовое регулирование и управление рисками

Задача: Проведение экспресс-оценки рисков для предложенного фрагмента АСУ ТП (например, система управления насосной станцией). Разработка плана мероприятий по минимизации рисков.

Типовое задание дидактической игры

Формат: «Киберучения: Атака на завод»

Цель: сформировать у студентов понимание ключевых различий между ИТ-безопасностью и безопасностью ОТ (операционных технологий), а также научиться идентифицировать критические активы и потенциальные векторы атак на промышленном объекте.

Вводная часть:

Презентация: Краткий обзор темы. Ключевой тезис: «В ИТ главное — конфиденциальность данных. В ОТ (АСУ ТП) главное — доступность и целостность процесса».

Разбор примера: Демонстрация реального кейса (например, атака Stuxnet или инцидент с Colonial Pipeline). Обсуждение: как кибератака привела к физическому ущербу и остановке производства.

Основной блок: Деловая игра

Сценарий: Студенты делятся на 2 команды.

Команда 1: «Злоумышленники» (Red Team)

Задача: разработать план атаки на условный «Химический завод по производству реагента Х».

Вводные данные: у команды есть план-схема объекта (можно раздать упрощенную схему с ПЛК, SCADA, сетевыми коммутаторами, Wi-Fi роутером в офисе, USB-портами на станциях операторов).

Задание: выбрать цель атаки (например, «изменить температуру в реакторе», «остановить конвейер», «украсть формулу реагента») и описать 3-4 вектора атаки.

Примеры векторов:

1. Внешний: Фишинговое письмо инженеру с зараженной флешкой.
2. Сетевой: Поиск незащищенного порта RDP или VPN.
3. Физический: Проникновение на территорию и подключение к сети через розетку в цеху.
4. Цепочка поставок: Взлом обновления ПО для ПЛК.

Команда 2: «Защитники» (Blue Team)

Задача: разработать концепцию эшелонированной обороны для защиты того же завода.

Вводные данные: Та же схема объекта.

Задание: предложить меры защиты для каждого уровня, основываясь на модели Purdue:

1. Уровень 3 (MES/Business Network): Межсетевой экран, сегментация, запрет на использование личных USB-устройств.
2. Уровень 2 (Control/SCADA): Защищенные шлюзы (OPC UA с аутентификацией), антивирусное ПО на серверах.
3. Уровень 1 и 0 (Field Devices/PLCs): Отключение ненужных сетевых служб на ПЛК, физическая защита шкафов управления.

Подведение итогов и обсуждение

Представители команд представляют свои решения.

Модератор (преподаватель) проводит анализ:

- насколько реалистичны были векторы атаки «Злоумышленников»?
- смогли ли «Защитники» закрыть эти векторы?
- обсуждение главного вопроса: «Почему нельзя просто поставить обычный антивирус и межсетевой экран, как в офисе?».

5. Оценочные материалы для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Зачет представляет собой выполнение обучающимся заданий билета, включающего в себя:

Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающегося принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними.

Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности.

Задание №3 – задания на проверку умений и навыков, полученных в результате освоения дисциплины.

Выполнение обучающимся заданий билета оценивается по следующей балльной шкале:

Задание 1: 0-30 баллов

Задание 2: 0-30 баллов

Задание 3: 0-40 баллов

«Зачтено»

– 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат.

– 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный.

Обучающийся в целом правильно интерпретирует полученный результат.

– 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично.

«Не зачтено»

– менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания 1-го типа

1. В чем заключается ключевое различие в приоритетах информационной безопасности для ИТ-систем и для автоматизированных систем управления технологическими процессами (АСУ ТП)?

2. Опишите архитектуру модели Purdue (ISA-95). Как принципы этой модели используются для построения эшелонированной защиты и сегментации промышленной сети?

3. Перечислите основные векторы атак на промышленные объекты. В чем заключается специфика атак на полевой уровень (ПЛК, датчики) по сравнению с атаками на корпоративный сегмент?

4. Каковы основные уязвимости промышленных протоколов передачи данных (например, Modbus, DNP3)? Какие методы защиты применяются для обеспечения их безопасности?

5. Раскройте концепцию эшелонированной обороны (Defense-in-Depth) применительно к защите АСУ ТП. Какие уровни защиты она включает?

6. Опишите назначение и принципы работы межсетевых экранов прикладного уровня (DPI) и систем обнаружения/предотвращения вторжений (IDS/IPS) в промышленных сетях.

7. Каковы основные принципы управления доступом в АСУ ТП? Опишите ролевую модель доступа для различных категорий пользователей (оператор, инженер, администратор).

8. Для решения каких задач в промышленных сетях применяются системы мониторинга и управления событиями информационной безопасности (SIEM)?

9. Каковы основные положения Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и как он влияет на проектирование защищенных систем?

10. Какие основные группы требований предъявляет ФСТЭК России к созданию систем безопасности значимых объектов критической информационной инфраструктуры (КИИ)?

11. Опишите методику анализа и оценки рисков информационной безопасности для АСУ ТП. Какие этапы включает в себя этот процесс?

12. Какие технологии и архитектурные решения используются для организации безопасного удаленного доступа к компонентам АСУ ТП (например, к SCADA-системе или ПЛК)?

13. В чем заключаются угрозы безопасности цепочки поставок (Supply Chain Security) для промышленных систем? Какие меры позволяют минимизировать эти риски?

14. Как обеспечивается информационная безопасность на различных этапах жизненного цикла АСУ ТП, от разработки технического задания до вывода системы из эксплуатации?

15. Опишите алгоритм действий персонала при реагировании на инцидент информационной безопасности, который может привести к нарушению или остановке технологического процесса.

Задания 2-го типа

1. Дайте определение и объясните ключевое различие между понятиями

«Информационная безопасность» (ИТ-контекст) и «Кибербезопасность АСУ ТП» (ОТ-контекст). Как это различие влияет на выбор мер защиты?

2. Что такое «Эшелонированная оборона» (Defense-in-Depth) в контексте защиты АСУ ТП? Опишите, как этот принцип реализуется на практике на примере защиты насосной станции.

3. Объясните взаимосвязь между моделью Purdue (ISA-95) и принципом сегментации сети. Почему сегментация является критически важным элементом защиты промышленных систем?

4. Сравните понятия «Надежность» и «Отказоустойчивость» применительно к компонентам АСУ ТП. Как меры кибербезопасности могут влиять на каждый из этих параметров?

5. Что такое «Объект критической информационной инфраструктуры» (КИИ)? Каковы критерии его отнесения к значимому объекту и как это влияет на требования к его защите?

6. Опишите взаимосвязь между понятиями «Угроза», «Уязвимость» и «Риск». Приведите пример, где одна и та же уязвимость может порождать разные риски для разных активов в рамках одного завода.

7. В чем заключается принципиальное отличие межсетевого экрана для корпоративной сети (ИТ-файрвол) от межсетевого экрана для промышленной сети (ОТ-файрвол, DPI)?

8. Объясните разницу между системами обнаружения вторжений (IDS) и системами предотвращения вторжений (IPS) в контексте их применения в реальном времени на производстве. Каковы риски использования IPS в контуре управления?

9. Что такое «Зона» и «Канал связи» в терминологии модели Purdue? Как концепция «Глубокой обороны» применяется для защиты каналов связи между зонами?

10. Как связаны понятия «Цифровой двойник» и «Поверхность атаки» промышленного объекта? Почему внедрение цифровых двойников требует пересмотра модели угроз?

11. Опишите взаимосвязь между требованиями Федерального закона № 187-ФЗ и приказами ФСТЭК России. Какова роль каждого из этих документов в процессе проектирования защищенной системы?

12. В чем заключается разница между «Аудитом безопасности» и «Тестированием на проникновение» (пентестом) для АСУ ТП? Как эти процессы дополняют друг друга?

13. Объясните, как понятие «Целостность данных» (Integrity) трансформируется при переходе от офисных систем к промышленным. Почему нарушение целостности команды управления опаснее, чем утечка данных о температуре?

14. Что такое «Событие ИБ», «Инцидент ИБ» и как они связаны с понятием «Реагирование на инцидент»? Опишите базовый алгоритм реагирования.

15. Опишите взаимосвязь между жизненным циклом АСУ ТП (проектирование -> внедрение -> эксплуатация) и процессом обеспечения информационной безопасности. Почему безопасность нельзя «добавить» в уже работающую систему?

Задания 3-го типа

1. Дана простая схема сети: один коммутатор, к которому подключены офисный ПК, сервер SCADA и программируемый логический контроллер (ПЛК).

Задача: нарисовать новую схему, реализующую базовую сегментацию. Нужно разделить сеть на два сегмента (Офис и Производство) с помощью виртуальных сетей (VLAN) и показать, где должен стоять межсетевой экран для контроля трафика между ними.

2. Описан процесс: оператор меняет скорость конвейера через HMI-панель.

Задача: описать 3 разных способа, как злоумышленник может несанкционированно увеличить скорость конвейера (например, через USB на HMI, атаку на сеть, кражу пароля). Для каждого способа предложить одну меру защиты.

3. SCADA-сервер (IP 192.168.1.10) должен только считывать данные с датчика (IP 192.168.1.50) по протоколу Modbus/TCP (порт 502).

Задача: написать одно правило для межсетевого экрана в формате «[Действие] [Протокол] [Порт] [Источник] -> [Назначение]», которое разрешает только эту операцию и блокирует всё остальное.

4. В системе есть три роли: «Оператор», «Инженер» и «Администратор». Есть три действия: «Просмотр данных», «Изменение уставок», «Обновление прошивки ПЛК».

Задача: заполнить матрицу доступа (таблицу), указав, какие роли имеют право на какие действия.

5. Предоставлен короткий лог событий:

12:00 Подключение к ПЛК с IP-адреса администратора.

12:05 Изменение уставки температуры в печи.

12:10 Администратор сообщает, что был на обеде и не подключался.

Задача: описать, какой инцидент произошел, и назвать первое действие, которое должен предпринять инженер по безопасности.

6. На заводе есть два актива:

А) База данных с финансовыми отчетами за 5 лет.

Б) Система управления клапаном, который перекрывает подачу горючего газа.

Задача: объяснить, какой актив является более критичным для безопасности АСУ ТП и почему (используя понятия доступности и целостности).

7. Инженеру нужно удаленно подключаться к SCADA-серверу для диагностики, но прямое подключение из интернета опасно.

Задача: описать архитектуру из двух шагов для организации безопасного доступа (например, сначала подключение к офисной сети через VPN, а затем к SCADA).

8. Описана ситуация: «На HMI-панели оператора установлен пароль '12345', а антивирус отключен для 'повышения производительности'».

Задача: описать две угрозы, которые создает эта конфигурация, и предложить по одному способу их устранения.

9. Нужно повысить осведомленность персонала.

Задача: составить список из 3 правил для оператора АСУ ТП по работе с электронной почтой и USB-накопителями на рабочем месте.

10. У вас есть бюджет на покупку одного средства защиты для защиты сети управления.

Задача: выбрать между «Межсетевым экраном нового поколения (NGFW)» и «Системой обнаружения вторжений (IDS)». Обосновать свой выбор в 2-3 предложениях, описав основную задачу этого средства в промышленной сети.