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
_____ к.ф-м.н. Жданов Э.Р.
«_01_» _____ 2026 года
м.п.

Рабочая программа дисциплины

«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

Москва, 2026 г.

1. Аннотация к дисциплине

1.1.	Составлена в соответствии с ФГОС ВО - магистратура по направлению подготовки 09.04.03 Прикладная информатика, утвержденным приказом Минобрнауки от 19.09.2017 г. N 916.
1.2.	Посвящена изучению методологии, технологий и стандартов обеспечения кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) и киберфизических систем.
1.3.	Рассматривает специфику угроз для промышленных объектов, архитектурные принципы построения эшелонированной обороны и методы защиты на всех уровнях: от физического оборудования и сетевой инфраструктуры до прикладного программного обеспечения и систем верхнего уровня (SCADA, MES). Особое внимание уделяется интеграции требований безопасности в жизненный цикл проектирования систем, анализу рисков и соответствию нормативным требованиям РФ.

2. Место дисциплины в структуре ООП

2.1.	Цикл (раздел) ООП: Б1.В.ОД.10
2.2.	2 курс, 3 семестр

3. Цель освоения дисциплин

3.1.	Формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы

4. Задачи освоения дисциплины

4.1.	- сформировать знания о специфике угроз и векторов атак на промышленные системы управления (АСУ ТП/КФС), включая атаки на физический уровень, протоколы и персонал; - сформировать знания о принципах построения эшелонированной (многоуровневой) защиты промышленных объектов; - сформировать знания о методах и средствах защиты на сетевом, хостовом и прикладном уровнях (сегментация, межсетевое экранирование, системы обнаружения вторжений); - сформировать знания о нормативно-правовой базе и отраслевых стандартах в области защиты информации критической информационной инфраструктуры (КИИ) и АСУ ТП; - сформировать знания о методиках анализа рисков, оценки защищенности и проведения аудита безопасности промышленных систем; - сформировать навыки применять принципы сегментации сети (модель Purdue) для изоляции критических узлов АСУ ТП; - сформировать навыки конфигурировать средства защиты информации (межсетевые экраны прикладного уровня, системы обнаружения вторжений) для контроля трафика в промышленной сети; - сформировать навыки проводить базовый анализ защищенности промышленных протоколов (Modbus, Profinet, OPC UA) и выявлять их уязвимости; - сформировать навыки разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности (политики, инструкции, регламенты) для промышленного предприятия; - сформировать умение интегрировать требования по кибербезопасности в техническое задание и проектную документацию на всех этапах жизненного цикла создания АСУ ТП; - сформировать умение применять риск-ориентированный подход для выбора адекватных мер защиты, исходя из критичности защищаемых активов.

5. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

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	*Знать:* - специфику угроз информационной безопасности для промышленных объектов, включая векторы атак на полевой уровень (ПЛК, датчики), сети и системы верхнего уровня (SCADA); - 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. *Уметь:* - 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. *Иметь практический опыт:* - 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	*Знать:* - 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; *Уметь:* - 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. *Иметь практический опыт:* - разработки замечаний и рекомендаций по результатам анализа проектной документации для внесения изменений, повышающих уровень защищенности системы.
ПК-2.1	*Знать:* - 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. *Уметь:* - 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. *Иметь практический опыт:* - выполнения анализа кейса по цифровой трансформации предприятия с подготовкой отчёта, включающего оценку киберрисков и предложения по созданию системы защиты для новых цифровых активов.

6. Тематический план

Наименование темы/раздела	**Виды занятий и трудоемкость (в часах)**					**Формы контроля Форма ПА**
	Всего	Л	ПЗ	ЛЗ	СР	
Тема 1. Введение в кибербезопасность АСУ ТП / КФС	**18**	2	4	-	12	Дидактическая игра/20
Тема 2. Архитектура безопасности промышленных сетей	**22**	4	6	-	12	Отчет по практикуму по решению задач/20
Тема 3. Средства и методы технической защиты	**22**	2	6	-	14	Отчет по практикуму по решению задач/20
Тема 4. Управление доступом и мониторинг безопасности	**22**	2	6	-	14	Отчет по практикуму по решению задач/20
Тема 5. Нормативно-правовое регулирование и управление рисками	**24**	4	6	-	14	Отчет по практикуму по решению задач/20
Всего часов	**108**	**14**	**28**	**-**	**66**	100 ТКУ
Контроль, час	-					Зачет
Объем дисциплины (в ак. час.)	108					
Объем дисциплины (в зач. ед.)	3					

7. Содержание дисциплины

Наименование темы/раздела	Краткое содержание	Лекции (часов)
Тема 1. Введение в кибербезопасность АСУ ТП / КФС	Специфика промышленных систем: доступность, целостность, безопасность. Отличия от IT-безопасности. Основные угрозы и модели нарушителя (внешние, внутренние, APT-группировки). Концепция эшелонированной обороны (Defense-in-Depth).	2
Тема 2. Архитектура безопасности промышленных сетей	Сетевая сегментация на основе модели Purdue/ISA-95. Создание демилитаризованных зон (DMZ). Промышленные протоколы и их уязвимости (Modbus, DNP3, S7, OPC UA).	4
Тема 3. Средства и методы технической защиты	Межсетевые экраны прикладного уровня (Deep Packet Inspection) для АСУ ТП. Системы обнаружения/предотвращения вторжений (IDS/IPS) в промышленных сетях. Защита конечных узлов (серверы SCADA, рабочие станции операторов, ПЛК).	2
Тема 4. Управление доступом и мониторинг безопасности	Идентификация и аутентификация в АСУ ТП. Управление учетными записями. Системы сбора и корреляции событий безопасности (SIEM). Мониторинг инцидентов.	2
Тема 5. Нормативно-правовое регулирование и управление рисками	Законодательство РФ в области КИИ (ФЗ-187), требования ФСТЭК и ФСБ России. Методики анализа рисков для АСУ ТП. Оценка возможного ущерба от реализации угроз.	4

8. Самостоятельная работа студентов

Наименование темы/раздела	Виды самостоятельной работы	Трудоемкость в часах
Тема 1. Введение в кибербезопасность АСУ ТП / КФС	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	12
Тема 2. Архитектура безопасности промышленных сетей	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	12
Тема 3. Средства и методы технической защиты	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	14
Тема 4. Управление доступом и мониторинг безопасности	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	14
Тема 5. Нормативно-правовое регулирование и управление рисками	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	14

9. Тематика практических и лабораторных занятий

Наименование темы/раздела	Вид занятия	Краткое содержание занятия	Объем часов
Тема 1. Введение в кибербезопасность АСУ ТП / КФС	Практикум по решению задач	Дидактическая игра	4
Тема 2. Архитектура	Практикум	Разработка архитектуры сегментации сети	6

безопасности промышленных сетей	по решению задач	для условного завода с выделением уровней управления, контроля и полевых устройств.	
Тема 3. Средства и методы технической защиты	Практикум по решению задач	Анализ логов промышленного межсетевого экрана для выявления аномальной активности (сканирование портов, попытки неавторизованного доступа).	6
Тема 4. Управление доступом и мониторинг безопасности	Практикум по решению задач	Разработка матрицы доступа для операторов, инженеров и администраторов SCADA-системы. Анализ сценария инцидента на основе данных SIEM.	6
Тема 5. Нормативно-правовое регулирование и управление рисками	Практикум по решению задач	Проведение экспресс-оценки рисков для предложенного фрагмента АСУ ТП (например, система управления насосной станцией). Разработка плана мероприятий по минимизации рисков.	6

10. Фонд оценочных средств

Оценочные материалы для проведения текущего контроля успеваемости, промежуточной аттестации, а также порядок начисления баллов и критерии оценивания представлены в комплекте оценочных материалов (КОМ) по дисциплине

11. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература			
Авторы	**Заглавие**	**Издательство, год**	**Эл. адрес**
Щеглов, А. Ю.	Защита информации: основы теории: учебник для вузов	Москва: Издательство Юрайт, 2025	urait.ru
Казарин, О. В.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов	Москва: Издательство Юрайт, 2026	urait.ru
Суворова, Г. М.	Информационная безопасность: учебное пособие для вузов	Москва: Издательство Юрайт, 2021	urait.ru
Козырь, Н. С.	Информационные технологии в кибербезопасности: учебник для вузов / Н. С. Козырь, А. М. Левченко	Москва: Издательство Юрайт, 2026	urait.ru
9.2. Дополнительная литература			
Козырь, Н. С	Оценка рисков и аудит информационной безопасности: учебник для вузов / Н. С. Козырь, В. Н. Хализев	Москва: Издательство Юрайт, 2026	urait.ru
Козырь, Н. С.	Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян	Москва: Издательство Юрайт, 2026	urait.ru
Андык, В. С.	Автоматизированные системы управления технологическими процессами на ТЭС: учебник для вузов	Москва: Издательство Юрайт, 2025	urait.ru

12. Материально-техническое обеспечение дисциплины

Наименование помещения	Перечень основного оборудования
Учебная аудитория для проведения лекционных и практических занятий,	Мультимедийное оборудование (проектор, экран), маршрутизатор/роутер, мебель

консультаций, текущего контроля, промежуточной аттестации.	
Компьютерный класс для проведения лабораторных занятий, консультаций, текущего контроля, промежуточной аттестации.	Компьютерная техника с возможностью подключения к Интернету, маршрутизатор/роутер, мультимедийное оборудование (проектор, экран), мебель.
Помещения для самостоятельной работы обучающихся	Мебель, компьютерная техника с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, маршрутизатор/роутер.