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

«Основы информационной безопасности»

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.	формирует у магистрантов системное представление о современных угрозах, методах и средствах защиты информации в условиях цифровизации промышленного производства. Особое внимание уделяется специфике обеспечения безопасности цифровых двойников, распределённых информационных систем и автоматизированных систем управления технологическими процессами (АСУ ТП). Курс охватывает нормативно-правовые основы, методы анализа рисков, технологии криптографической защиты, а также принципы построения защищённых архитектур для критически важных объектов.

2. Место дисциплины в структуре ООП

2.1.	Цикл (раздел) ООП: Б1.Б.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 об основных понятиях, принципах и целях информационной безопасности в контексте промышленных систем; - сформировать знания о современных угрозах, моделях нарушителя и специфике атак на автоматизированные системы управления технологическими процессами; - сформировать знания о нормативно-правовой базе и стандартах, регламентирующих защиту информации на критически важных объектах; - сформировать знания о методах анализа рисков информационной безопасности для производственных предприятий; - сформировать знания о принципах построения защищённых архитектур распределённых информационных систем и цифровых двойников; - сформировать навыки применения методов идентификации и оценки угроз информационной безопасности для объектов АСУ ТП; - сформировать навыки использования базовых средств защиты информации (криптографические инструменты, средства сетевой защиты) для решения типовых задач безопасности; - сформировать навыки разработки организационно-распорядительной документации (политик, инструкций) по обеспечению информационной безопасности на предприятии; - сформировать навыки проведения аудита защищённости компонентов автоматизированных систем управления; - сформировать умение анализировать архитектуру информационных систем предприятия с целью выявления потенциальных уязвимостей и точек отказа; - сформировать умение выбирать и обосновывать применение адекватных методов и средств защиты информации в зависимости от модели угроз и специфики производственного процесса; - сформировать умение интегрировать требования информационной безопасности в процессы проектирования, внедрения и эксплуатации цифровых двойников и АСУ ТП.

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

ОПК-5	**Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем**
ОПК-5.1	Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-5.2	Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач

Код индикатора компетенции	Планируемые результаты обучения по дисциплине
ОПК-5.1	*Знать:* - архитектуру и состав современных программно-аппаратных комплексов, используемых в информационных системах и автоматизированных системах управления технологическими процессами (АСУ ТП); - принципы работы и особенности аппаратных платформ (контроллеры, серверы, IoT-устройства) и системного программного обеспечения, применяемого для построения цифровых двойников и промышленных сетей. *Уметь:* - идентифицировать и классифицировать основные компоненты программно-аппаратного обеспечения информационной системы; - анализировать технические характеристики аппаратных средств и программного окружения для оценки их применимости в задачах промышленной автоматизации. *Иметь практический опыт:* - работы с современными образцами аппаратного обеспечения (контроллеры, модули ввода-вывода, сетевое оборудование) и их настройки в составе лабораторных стендов; - установки, конфигурирования и диагностики операционных систем и специализированного ПО, используемого в АСУ ТП.
ОПК-5.2	*Знать:* - методы и технологии модернизации аппаратных платформ и программного обеспечения, включая обновление микропрограмм (firmware), драйверов и системного ПО для обеспечения совместимости и повышения производительности; - принципы обратной совместимости и миграции данных при обновлении компонентов автоматизированных систем управления. *Уметь:* - планировать и реализовывать мероприятия по модернизации аппаратного и программного обеспечения с учётом требований информационной безопасности и непрерывности производственного процесса; - выполнять установку, настройку и интеграцию новых версий ПО и оборудования в существующую инфраструктуру АСУ ТП. *Иметь практический опыт:* - проведения апгрейда аппаратных компонентов (например, замена контроллеров, модулей ввода-вывода) на лабораторных стендах или в симулированной среде; - обновления версий системного и прикладного ПО, а также драйверов устройств в составе автоматизированной системы.

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	**24**	2	4	2	16	Отчет по лабораторному

информационную безопасность						практикуму/10 Практикум по решению задач/10
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	**28**	4	6	2	16	Отчет по лабораторному практикуму/10 Практикум по решению задач/10
Тема 3. Методы и средства защиты информации	**34**	4	6	6	18	Отчет по лабораторному практикуму/10 Практикум по решению задач/10
Тема 4. Управление информационной безопасностью	**30**	4	6	2	18	Отчет по лабораторному практикуму/10 Практикум по решению задач/10
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	**28**	-	6	2	20	Отчет по лабораторному практикуму/10 Практикум по решению задач/10
Всего часов	**144**	**14**	**28**	**14**	**88**	100 ТКУ
Контроль, час	**36**					Экзамен
Объем дисциплины (в академических часах)	180					
Объем дисциплины (в зачетных единицах)	5					

7. Содержание дисциплины

Наименование темы/раздела	Краткое содержание	Лекции (часов)
Тема 1. Введение в информационную безопасность	Основные понятия и определения: информация, информационная безопасность, конфиденциальность, целостность, доступность (CIA). Цели и задачи обеспечения информационной безопасности в современных условиях. Классическая триада информационной безопасности и её применение к промышленным системам. Классификация угроз информационной безопасности: естественные и искусственные, преднамеренные и случайные. Нормативно-правовая база РФ в области защиты информации (обзор ФЗ-149, ФЗ-187 «О КИИ», требования регуляторов ФСТЭК и ФСБ).	2
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	Специфика промышленных систем управления (АСУ ТП, SCADA) как объекта защиты. Классификация уязвимостей в программном и аппаратном обеспечении АСУ ТП (протоколы, ПЛК, человеко-машинные интерфейсы). Анализ актуальных векторов атак на промышленные объекты (на примере инцидентов Stuxnet, Industroyer). Угрозы целостности и доступности данных цифрового двойника. Моделирование угроз и нарушителя для производственных информационных систем.	4
Тема 3. Методы и средства защиты информации	Криптографические методы защиты: симметричное и асимметричное шифрование, электронная подпись, управление ключами. Сетевая безопасность: межсетевое экранирование (Firewalls), системы обнаружения/предотвращения вторжений (IDS/IPS), сегментация сетей (создание демилитаризованных зон). Защита конечных узлов: контроль доступа, антивирусная защита, управление обновлениями (patch management). Средства	4

	защиты промышленного сетевого трафика (глубокий анализ промышленных протоколов).	
Тема 4. Управление информационной безопасностью	Политика информационной безопасности предприятия: цели, структура, порядок разработки и внедрения. Организация процессов мониторинга событий безопасности и реагирования на инциденты (концепция SOC/COB). Планирование непрерывности бизнеса (BCP) и аварийного восстановления (DRP) для критически важных систем. Аудит информационной безопасности: внутренний и внешний, методы оценки соответствия требованиям стандартов.	4
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	Обеспечение достоверности данных: методы верификации и валидации информации, поступающей от физического объекта. Защита каналов передачи данных между физическим объектом, цифровой моделью и системами поддержки принятия решений. Управление доступом к данным цифрового двойника: ролевые модели, разграничение прав. Интеграция систем защиты информации в жизненный цикл цифрового двойника (от проектирования до вывода из эксплуатации).	-

8. Самостоятельная работа студентов

Наименование темы/раздела	Виды самостоятельной работы	Трудоемкость в часах
Тема 1. Введение в информационную безопасность	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	16
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	16
Тема 3. Методы и средства защиты информации	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	18
Тема 4. Управление информационной безопасностью	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	18
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	Проработка лекционного материала, изучение рекомендуемой литературы, работа с ЭБС	20

9. Тематика практических и лабораторных занятий

Наименование темы/раздела	Вид занятия	Краткое содержание занятия	Объем часов
Тема 1. Введение в информационную безопасность	Практикум по решению задач	Решение задач.	4
Тема 1. Введение в информационную безопасность	Лабораторный практикум	Выполнение заданий в лабораторных условиях.	2
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	Практикум по решению задач	Решение задач.	6
Тема 2. Угрозы и уязвимости в АСУ ТП и цифровых двойников	Лабораторный практикум	Выполнение заданий в лабораторных условиях.	2
Тема 3. Методы и средства защиты информации	Практикум по решению задач	Решение задач.	6
Тема 3. Методы и средства защиты информации	Лабораторный практикум	Выполнение заданий в лабораторных условиях.	6

Тема 4. Управление информационной безопасностью	Практикум по решению задач	Решение задач.	6
Тема 4. Управление информационной безопасностью	Лабораторный практикум	Выполнение заданий в лабораторных условиях.	2
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	Практикум по решению задач	Решение задач.	6
Тема 5. Практические аспекты обеспечения ИБ в цифровых двойниках	Лабораторный практикум	Выполнение заданий в лабораторных условиях.	2

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**
Козырь, Н. С.	Анализ и оценка рисков информационной безопасности: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/590420
Козырь, Н. С.	Оценка рисков и аудит информационной безопасности: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/590417
Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Организационное и правовое обеспечение информационной безопасности: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/583236
9.2. Дополнительная литература			
Козырь, Н. С.	Гуманитарные аспекты информационной безопасности: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/589310
Рабчевский, А. Н.	Основы информационного противоборства: сетевая наука: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/589700
Чернова, Е. В.	Информационная безопасность человека: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/587699

12. Материально-техническое обеспечение дисциплины

Наименование помещения	Перечень основного оборудования
Учебная аудитория для проведения лекционных и практических занятий, консультаций, текущего контроля, промежуточной аттестации.	Мультимедийное оборудование (проектор, экран), маршрутизатор/роутер, мебель
Компьютерный класс для проведения лабораторных занятий, консультаций,	Компьютерная техника с возможностью подключения к Интернету,

текущего контроля, промежуточной аттестации.	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.