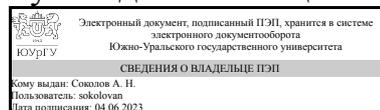


УТВЕРЖДАЮ:
Руководитель специальности



А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.43 Киберфизические системы
для специальности 10.05.03 Информационная безопасность автоматизированных систем

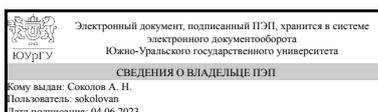
уровень Специалитет

форма обучения очная

кафедра-разработчик Защита информации

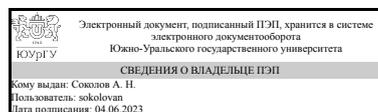
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
к.техн.н., доц., заведующий
кафедрой



А. Н. Соколов

1. Цели и задачи дисциплины

Знакомство с общей концепцией и принципами построения киберфизических систем (КФС) как новой технологической платформы формирования универсальной информационно-управляющей среды, объединяющей ключевые тренды развития сквозных информационных и информационно-прикладных технологий, и предназначенной для решения широкого класса задач промышленной автоматизации, управления и кибербезопасности

Краткое содержание дисциплины

Киберфизические системы: основные понятия. Теория автоматического управления и информационно-управляющие системы. Индустриальные киберфизические системы. Кибербезопасность

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	Знает: базовые понятия и определения киберфизической системы, базовые принципы теории управления системами, формирования целей, методов и критериев качества управления, формализованных стратегий управления; основы, понятия и определения информационно-управляющих систем; основы теории сетевой организации информационно-вычислительных распределенных систем и компьютерных сетей, архитектуры и иерархии сетевой организации; основы модели знаний, базовые понятия теории формирования баз данных и баз знаний; подходы к построению платформы киберфизической системы как гибридной сетевой среды с интегрированными вычислительными и физическими возможностями Умеет: анализировать подходы к построению гибридной информационно-управляющей среды, ориентированной на решение широкого класса прикладных задач, в том числе связанных с обеспечением информационной безопасности; ставить задачи формирования архитектуры, принципов построения и функционирования киберфизической системы; ставить задачи проведение аналитики киберугроз и оценки уязвимостей и рисков киберфизической системы

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.34 Комплексное обеспечение защиты информации объектов информатизации,	Не предусмотрены

1.О.31 Защита информации от утечки по техническим каналам, 1.О.33 Программно-аппаратные средства защиты информации, 1.О.24 Введение в графические системы общего и специализированного назначения	
---	--

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.О.31 Защита информации от утечки по техническим каналам	Знает: типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации, классификацию и количественные характеристики технических каналов утечки информации; способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности; организацию защиты информации от утечки по техническим каналам на объектах информатизации Умеет: проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального контроля показателей эффективности технической защиты информации Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек по техническим каналам
1.О.24 Введение в графические системы общего и специализированного назначения	Знает: основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков Умеет: применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), применять методы построения компьютерных моделей изделий Имеет практический опыт: разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементарных геометрических построений при помощи средств компьютерной графики; построения двухмерных и трехмерных (3D) изображений изделий
1.О.34 Комплексное обеспечение защиты информации объектов информатизации	Знает: принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности

	<p>организации, принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p> <p>Умеет: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации, определять комплекс мер для обеспечения защиты информации объектов информатизации</p> <p>Имеет практический опыт: анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации</p>
1.О.33 Программно-аппаратные средства защиты информации	<p>Знает: программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях</p> <p>Умеет: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности</p> <p>Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа</p>

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	
Общая трудоёмкость дисциплины	72	72	
<i>Аудиторные занятия:</i>	32	32	
Лекции (Л)	16	16	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	35,75	35,75	
Подготовка к зачету	8	8	
Подготовка к контрольным работам	11,75	11.75	
Подготовка к практическим занятиям	16	16	
Консультации и промежуточная аттестация	4,25	4,25	

Вид контроля (зачет, диф.зачет, экзамен)	-	зачет
--	---	-------

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Киберфизические системы: основные понятия	6	4	2	0
2	Теория автоматического управления и информационно-управляющие системы	18	8	10	0
3	Индустриальные киберфизические системы. Кибербезопасность	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие киберфизической системы (КФС). Области применения киберфизических систем. Концептуальная модель КФС	2
2	1	Основные принципы организации и функционирования КФС. Системный подход к анализу и синтезу структур КФС	2
3	2	Базовые понятия теории автоматического управления (ТАУ). Формализация постановки задачи и выбора стратегий управления	2
4	2	Информационно-управляющие системы: понятия, определения, особенности	2
5	2	Информационно-вычислительные распределенные системы: принципы сетевой организации, архитектура и иерархия	2
6	2	Инженерия знаний: модели знаний, базовые понятия теории формирования баз данных и баз знаний	2
7	3	Индустриальные КФС (ИКФС), сферы применения ИКФС. подходы к разработке и анализу, оперативное планирование и управление	2
8	3	Кибербезопасность КФС	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие КФС. Примеры киберфизических систем и объектов. Уровни концептуальной модели КФС. Функциональные признаки модели	2
2	2	Базовые понятия ТАУ: объект управления, алгоритмы и критерии качества управления	2
3	2	Постановка задачи и выбора стратегий управления. Целевые функции при синтезе КФС	2
4	2	Примеры информационно-управляющих систем. Анализ особенностей	2
5	2	Архитектура и иерархия сетевой организации вычислительной распределенной системы	2
6	2	Модели знаний	2
7	3	Интеллектуальные фабрики. Промышленные интеллектуальные данные и сервисы	2
8	3	Подходы к разработке и анализу интеллектуальных производственных систем с позиций кибербезопасности	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к зачету	Основная и дополнительная литература	9	8
Подготовка к контрольным работам	Основная и дополнительная литература	9	11,75
Подготовка к практическим занятиям	Основная и дополнительная литература	9	16

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	9	Текущий контроль	Контрольная работа 1	1	18	Работа включает 6 вопросов. Каждый максимально оценивается в 3 балла. 3 балла – дан верный и развернутый ответ. 2 балла – дан верный, недостаточно полный ответ. 1 балл – дан верный, односложный ответ. 0 баллов – нет ответа.	зачет
2	9	Текущий контроль	Контрольная работа 2	1	36	Работа включает 12 вопросов. Каждый максимально оценивается в 3 балла. 3 балла – дан верный и развернутый ответ. 2 балла – дан верный, недостаточно полный ответ. 1 балл – дан верный, односложный ответ. 0 баллов – нет ответа.	зачет
3	9	Текущий контроль	Контрольная работа 3	1	27	Работа включает 9 вопросов. Каждый максимально оценивается в 3 балла. 3 балла – дан верный и развернутый ответ. 2 балла – дан верный, недостаточно полный ответ. 1 балл – дан верный, односложный ответ. 0 баллов – нет ответа.	зачет
4	9	Текущий контроль	Реферат	4	19	Оценивание реферата: 1. Оформление: 2 балла – оформление соответствует всем требованиям; 1 балл – есть несущественный погрешности в оформлении; 0 баллов – оформление не	зачет

						<p>соответствует требованиям</p> <p>2. Раскрытие темы: 2 балла – тема раскрыта полностью; 1 балл – тема раскрыта не полностью; 0 баллов – тема не раскрыта.</p> <p>3. Новизна: 2 балла – представленный материал является новым; 1 балл – представленный материал не является новым, но переработан автором ; 0 баллов – представленный материал не является новым.</p> <p>4. Степень научности: 1 балл – изложенный материал содержит научную составляющую; 0 баллов – изложенный материал не содержит научную составляющую.</p> <p>5. Объем: 2 балла – свыше 20 страниц; 1 балл – от 10 до 19 страниц ; 0 баллов – до 10 страниц .</p> <p>6. Количество источников: 2 балла – число источников более 10, включая статьи; 1 балл – число источников от 5 до 10, статей нет ; 0 баллов – число источников до 5.</p> <p>7. Наличие ссылок на источники: 2 балла – в тексте есть ссылки на все источники; 1 балл – в тексте есть ссылки не на все источники; 0 баллов – в тексте отсутствуют ссылки на источники.</p> <p>8. Структура изложения: 2 балла – материал изложен логично, есть оглавление; 1 балл – материал изложен логично, оглавления нет; 0 баллов – логика изложения материала отсутствует.</p> <p>9. Доклад: 2 балла – доклад подготовлен и рассказан без подглядываний; 1 балл – доклад подготовлен и прочитан; 0 баллов – доклад не подготовлен .</p> <p>10. Презентация: 2 балла – презентация подготовлена и включает не только текстовый, но и графический/ табличный/ иллюстративный материал; 1 балл – презентация подготовлена и включает только текстовый материал; 0 баллов – презентация не подготовлена.</p>	
5	9	Промежуточная аттестация	Зачет	-	40	<p>Билет содержит 20 вопросов. Форма билета - тест. Максимально ответ на каждый вопрос оценивается в 2 балла.</p> <p>2 балла - дан полный и верный ответ.</p> <p>1 балл - дан частично верный ответ (наряду с верным указан неверный ответ).</p> <p>0 баллов - ответа нет.</p>	зачет

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ОПК-9	Знает: базовые понятия и определения киберфизической системы, базовые принципы теории управления системами, формирования целей, методов и критериев качества управления, формализованных стратегий управления; основы, понятия и определения информационно-управляющих систем; основы теории сетевой организации информационно-вычислительных распределенных систем и компьютерных сетей, архитектуры и иерархии сетевой организации; основы модели знаний, базовые понятия теории формирования баз данных и баз знаний; подходы к построению платформы киберфизической системы как гибридной сетевой среды с интегрированными вычислительными и физическими возможностями	+	+	+	+	+
ОПК-9	Умеет: анализировать подходы к построению гибридной информационно-управляющей среды, ориентированной на решение широкого класса прикладных задач, в том числе связанных с обеспечением информационной безопасности; ставить задачи формирования архитектуры, принципов построения и функционирования киберфизической системы; ставить задачи проведение аналитики киберугроз и оценки уязвимостей и рисков киберфизической системы	+	+	+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) *основная литература:*

Не предусмотрена

б) *дополнительная литература:*

Не предусмотрена

в) *отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:*

Не предусмотрены

г) *методические указания для студентов по освоению дисциплины:*

1. Г.И. Радченко. Распределенные вычислительные системы

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Г.И. Радченко. Распределенные вычислительные системы

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Ли, П. Архитектура интернета вещей / П. Ли ; перевод с английского М. А. Райтман. — Москва : ДМК Пресс, 2019. — 454 с. — ISBN 978-5-97060-672-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112923 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.

2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Грингард, С. Интернет вещей: Будущее уже здесь / С. Грингард ; перевод М. Трощенко. — Москва : Альпина Паблишер, 2016. — 188 с. — ISBN 978-5-9614-5853-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/87981 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	eLIBRARY.RU	Cyber-Physical Systems and Control, 10–11 июня 2019 года, 2020. – 124 p. – ISBN 978-5-7422-7048-5. https://www.elibrary.ru/item.asp?id=44147114
4	Основная литература	Электронно-библиотечная система издательства Лань	Кабалдин, Ю. Г. Управление киберфизическими и механообрабатывающими системами в цифровом производстве на основе искусственного интеллекта и облачных технологий : учебное пособие / Ю. Г. Кабалдин, Д. А. Шатагин, П. В. Колчин. — Москва : Машиностроение, 2019. — 293 с. — ISBN 978-5-907104-17-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151072 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
5	Основная литература	Электронно-библиотечная система издательства Лань	Гаврилова, Т. А. Инженерия знаний. Модели и методы : учебник для вузов / Т. А. Гаврилова, Д. В. Кудрявцев, Д. И. Муромцев. — 4-е изд., стер. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-8793-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180874 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
6	Основная литература	Электронно-библиотечная система издательства Лань	Каширская, Е. Н. Защита информации в информационно - управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167621 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
7	Основная литература	Электронно-библиотечная система издательства Лань	Пачкин, С. Г. Распределенные информационно-управляющие системы : учебное пособие / С. Г. Пачкин, Р. В. Котляров. — Кемерово : КемГУ, 2020. — 98 с. — ISBN 978-5-8353-2798-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/186353 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
8	Основная литература	Электронно-библиотечная система издательства Лань	Певзнер, Л. Д. Теория автоматического управления. Задачи и решения : учебное пособие / Л. Д. Певзнер. — Санкт-Петербург : Лань, 2021. — 604 с. — ISBN 978-5-8114-2161-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168937 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
9	Основная литература	Электронно-библиотечная система издательства Лань	Коновалов, Б. И. Теория автоматического управления : учебное пособие / Б. И. Коновалов, Ю. М. Лебедев. — 5-е изд., стер. — Санкт-Петербург : Лань, 2020. — 220 с. — ISBN 978-5-8114-5816-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/145842 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
10	Дополнительная	Электронно-	Модели и способы взаимодействия пользователя с

	литература	библиотечная система издательства Лань	киберфизическим интеллектуальным пространством : монография / И. В. Ватаманюк, Д. К. Левоневский, Д. А. Малов [и др.]. — Санкт-Петербург : Лань, 2019. — 176 с. — ISBN 978-5-8114-3877-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/119635 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.
11	Дополнительная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222 (дата обращения: 04.02.2022). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Не предусмотрено