

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Иркутский национальный исследовательский технический университет»

Институт информационных технологий и анализа данных

Центр компетенций по кибербезопасности

УТВЕРЖДАЮ:

Директор института ИТ и АД
/ А.С. Говорков
28 марта 2022 г.

Фонд оценочных средств

Инженерия киберфизических систем

10.04.01 Информационная безопасность

Безопасность киберфизических систем

Форма обучения: Очная

Составитель программы:

Маринов А.А.



/ “ 28 ” марта 20 22 г.

Год набора – 2022

Иркутск 2022

1. Показатели и критерии оценивания компетенций на этапах их формирования

Индикатор достижения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания промежуточной аттестации
ПК-4.1 Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	Знать инструментарий для графического моделирования и архитектурного проектирования, реализующий рекомендации и принципы метода arcadia. Уметь провести моделирование архитектуры (arcadia/capella) будущей системы и на ранних этапах отследить возможность выполнения функциональных и нефункциональных требований. Владеть методом arcadia, на практике показать выполнение (последовательность действий) следующих шагов: – определение потребностей пользователя; – формализация требований к системе; – разработка логической архитектуры; – разработка физической архитектуры; – формализация требований к компонентам.	Способен описать необходимость и целесообразность внедрения результатов по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий
ПК-3.3 Способен предлагать в рамках проектно-конструкторской деятельности системные решения инженерных задач в различных	Знать маршруты проектирования и подходы к проектированию программного обеспечения систем произвольного назначения.	Способен продемонстрировать специализированные знания в рамках проектно-конструкторской деятельности: решение инженерных задач в информационных	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.

информационных технологий.	Уметь применять на практике структура «альф» и «суб-альф», которая позволяет essence соответствовать ISO 15288, в частности v-диаграмме. Владеть методами архитектурное описания рабочего продукта, в частности v-диаграмме (ISO 15288), в следующем порядке согласовать требования: – требования предметной области; – требования к системе; – требования к отдельным элементам; – запуска процесса разработки (в контексте киберфизических систем); – верификации элемента системы, а в конце самой системы и проверки на выполнение всех требований (требований заказчика).	технологиях.	
ПК-1.3 Собирает и систематизирует научно-техническую информацию по теме исследования, определяет методы и средства решения задачи, планирует практическое проведение научных исследований и технических разработок	Знать: как использовать и развивать передовые достижения в сфере обеспечения защиты информации в инфокоммуникационных системах. Уметь: эффективного применения результатов научно-исследовательских и опытно-конструкторских работ в области защиты информации. Владеть: информацией о современных	Способен продемонстрировать специализированные знания в области систематизации научно-технической информации по теме исследования: определение методов и средств решения задач, практическое проведение научных исследований и технических разработок.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.

	тенденциях в области разработки систем защиты на основе российских и международных стандартов.		
ПК-1.6 Способен работать с механическими и программными компонентами; изготовить и запрограммировать реальную киберфизических систему	Знать основные сегменты деятельности, которые непосредственно относятся к созданию вычислительной компоненты КФС: – проектирование систем на кристалле (включая технологии asic, asip, fpga); – проектирование специализированных контроллеров и всс на их основе; – проектирование систем автоматики на базе готовых программируемых логических контроллеров, scada-систем, технологий информационных систем. Уметь эффективно решать вопросы ограниченного числа типовых проектных ик-платформ для множества разнообразных задач, среди которых: – нехватка вычислительной мощности; – большое энергопотребление; – сложность программирования задач реального времени (рв); – сложность реализации и программирования гетерогенных многопроцессорных структур; – низкая информационная безопасность. Владеть навыками анализа документов	Способен продемонстрировать специализированные знания в области механических и программных компонентов: изготовить и запрограммировать киберфизических систему.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.

	для получения достоверной информации о работе системы или ее части («реверс-инжиниринг»), работать с полным стеком технологий определяющими основные задачи создания как специализированных ВС, так и вычислительных платформ широкого назначения.		
--	--	--	--

1. Оценочные средства для проведения текущего контроля

1.1. Оценочные средства для проведения текущего контроля в _3_ семестре

Перечень тестовых заданий

ПК-4.1

Множественный выбор

1. Какие последствия могут возникнуть при неправильном внедрении систем обеспечения информационной безопасности в киберфизические системы?

- А) Потеря конкурентоспособности**
- Б) Улучшение производительности системы
- В) Повышение уровня доверия пользователей

2. Какие факторы следует учитывать при оценке целесообразности внедрения систем обеспечения информационной безопасности?

- А) Финансовые затраты и потенциальные убытки от нарушений безопасности**
- Б) Только технические возможности системы
- В) Отношение сотрудников к новым технологиям

3. Какие методы анализа рисков используются при оценке целесообразности внедрения систем обеспечения информационной безопасности?

- А) Методика оценки вероятности возникновения угроз**
- Б) Анализ цветовых схем интерфейса пользователя
- В) Оценка погодных условий на месте установки системы

ПК-3.3

Короткий ответ

4. Что такое киберфизическая система (CPS)?...(CPS - это интегрированные системы, объединяющие вычислительные и физические компоненты для управления физическими процессами).

5. Какие технологии используются для связи между вычислительной и физической частями киберфизической системы?...(Интернет вещей (IoT), беспроводные сети, протоколы связи).

6. Какие методы анализа применяются для оптимизации работы киберфизических систем?...(

Метод конечных элементов (FEM), методы оптимизации, метод Монте-Карло).

7. Какие принципы проектирования учитываются при создании киберфизических систем?...(**Распределенность, время реакции, надежность**).

8. Какие технологии обеспечивают безопасность киберфизических систем?...(**Шифрование данных, аутентификация пользователей, защита от вредоносного программного обеспечения**).

ПК-1.3

Короткий ответ

9. Что такое систематизация научно-технической информации?...(**Это процесс организации и классификации информации для удобного доступа и использования**).

10. Какие методы систематизации информации используются в области безопасности киберфизических систем?...(**Классификация, тематический анализ, организация по источникам**).

11. Какие средства решения задач используются при систематизации научно-технической информации?...(**Информационные системы, базы данных, методы математического моделирования**).

12. Какие практические методы проведения научных исследований применяются в области безопасности киберфизических систем?...(**Эксперименты, наблюдение и измерение, анализ статистических данных**).

13. Какие технические разработки могут быть использованы для обеспечения безопасности киберфизических систем?...(**Разработка криптографических алгоритмов, создание систем мониторинга и детекции аномалий, разработка защищенных протоколов связи**).

ПК-1.6

Множественный выбор

14. Какой из следующих компонентов является механическим?

- А) Центральный процессор
- Б) Датчик движения**
- В) Оперативная память

15. Какое взаимодействие между механическими и программными компонентами является ключевым для киберфизических систем?

- А) Механические компоненты управляют программными компонентами
- Б) Программные компоненты управляют механическими компонентами
- В) Оба варианта верны**

16. Какой из нижеперечисленных примеров является интеграцией механических и программных компонентов в киберфизической системе?

- А) Робот-пылесос, который использует алгоритмы машинного обучения для определения оптимального маршрута
- Б) Система управления складом, которая использует электронные бирки для отслеживания инвентаря
- В) Все перечисленные варианты**

17. Какие технологические тренды в области механических компонентов киберфизических систем наиболее перспективны?

А) Использование наноматериалов для создания легких и прочных деталей

Б) Развитие 3D-печати для быстрого производства запасных частей

В) Все перечисленные варианты

18. Какое влияние выбора механических и программных компонентов имеет на безопасность киберфизических систем?

А) Непосредственного влияния нет

Б) Выбор компонентов может повлиять на уязвимости системы

В) Все перечисленные варианты

Перечень кейсовых заданий (задания с развернутым ответом)

№ задания	Содержание задания	Коды компетенций
1	Выгоды и преимущества компании от внедрения систем и средств обеспечения информационной безопасности киберфизических систем	ПК-4.1
2	Вызовы и риски внедрения новых систем и средств обеспечения информационной безопасности киберфизических систем, и их минимизация	ПК-4.1
3	Обеспечение внедрения и эксплуатации новых систем и средств обеспечения информационной безопасности киберфизических систем	ПК-4.1
4	Эффективность внедрения современных систем и средств обеспечения информационной безопасности киберфизических систем	ПК-4.1
5	Методы и средства убеждения заинтересованных сторон в целесообразности внедрения результатов по вводу в эксплуатацию систем и средств обеспечения информационной безопасности киберфизических систем	ПК-4.1
6	Методы и подходы анализа и решения сложных инженерных задач в процессе проектирования киберфизических систем	ПК-3.3
7	Взаимодействие между программными и аппаратными компонентами при разработке решений для киберфизических систем	ПК-3.3
8	Технологии и инструменты, используемые для моделирования и тестирования инженерных решений в рамках проектирования киберфизических систем	ПК-3.3
9	Выбор оптимального технического решения при проектировании киберфизических систем, учитывая их взаимодействие с физическим окружением	ПК-3.3
10	Управление сложностью и неопределенностью при решении инженерных задач в процессе проектирования киберфизических систем	ПК-3.3
11	Методы и средства для систематизации научно-технической информации в области безопасности киберфизических систем	ПК-1.3
12	Методы и средства решения задач в области безопасности киберфизических систем на основе систематизированной информации	ПК-1.3
13	Примеры практического проведения научных исследований в области безопасности киберфизических систем, основанных на систематизации научно-технической информации	ПК-1.3

14	Технические разработки , проведенные на основе систематизированной информации в области безопасности киберфизических систем и их результаты	ПК-1.3
15	Эффективность использования систематизированной научно-технической информации при решении задач в области безопасности киберфизических систем	ПК-1.3
16	Механические компоненты киберфизических систем. Влияние их выбора на общую производительность системы.	ПК-1.6
17	Взаимодействие программных компонентов с механическими компонентами в киберфизических системах, и их влияние на общую надежность системы.	ПК-1.6
18	Примеры интеграции механических и программных компонентов в киберфизических системах, которые привели к улучшению производительности или эффективности системы	ПК-1.6
19	Наиболее перспективные для будущего развития технологические тренды в области механических и программных компонентов киберфизических систем.	ПК-1.6
20	Влияние выбора механических и программных компонентов на безопасность киберфизических систем, и меры предосторожности при их выборе и интеграции.	ПК-1.6

2. Оценочные средства для проведения промежуточной аттестации

2.1 Оценочные средства для проведения зачета / экзамена / дифференцированного зачета / курсовой работы / курсового проектирования по дисциплине в _3_ семестре

Перечень тестовых заданий

ПК-4.1

Множественный выбор

1. Какие основные преимущества внедрения систем обеспечения информационной безопасности для киберфизических систем?

- А) **Защита от вредоносных атак**
- Б) Повышение производительности системы
- В) Улучшение качества физических процессов

2. Какие риски могут возникнуть при отсутствии систем обеспечения информационной безопасности в киберфизических системах?

- А) **Утечка конфиденциальной информации**
- Б) Недостаточная эффективность управления физическими процессами
- В) Повышенное энергопотребление

3. Какие методы защиты данных используются в системах обеспечения информационной безопасности киберфизических систем?

- А) **Шифрование данных**
- Б) Методика случайного удаления файлов
- В) Использование открытых сетей передачи данных

4. Какие технологии могут быть внедрены для обеспечения информационной безопасности киберфизических систем?

- А) Биометрическая аутентификация**
- Б) Применение устаревших операционных систем
- В) Открытый доступ к системам управления

5. Какие принципы следует учитывать при внедрении систем обеспечения информационной безопасности в киберфизические системы?

- А) Принцип минимальных привилегий**
- Б) Принцип открытости доступа ко всей информации
- В) Принцип игнорирования уязвимостей

Короткий ответ

6. Что такое киберфизические системы?...(Киберфизические системы - это интегрированные системы, объединяющие физические процессы и вычислительные средства).

7. В чем заключается целесообразность внедрения систем обеспечения информационной безопасности для киберфизических систем?...(Целесообразность заключается в защите от вредоносных атак, предотвращении утечки конфиденциальной информации и обеспечении надежности системы).

8. Какие преимущества могут быть получены от внедрения систем обеспечения информационной безопасности?...(Улучшение репутации компании, защита от потенциальных угроз, повышение уровня доверия пользователей).

9. Какие методы защиты данных используются в системах обеспечения информационной безопасности киберфизических систем?...(Шифрование данных, контроль доступа, мониторинг сетевой активности).

10. Какие риски могут возникнуть при отсутствии систем обеспечения информационной безопасности в киберфизических системах?...(Утечка конфиденциальной информации, нарушение работы системы, потеря конкурентоспособности).

11. Какие принципы следует учитывать при внедрении систем обеспечения информационной безопасности в киберфизические системы?...(Принцип минимальных привилегий, принцип защиты по периметру, принцип постоянного мониторинга).

12. Какие методы анализа рисков используются при оценке целесообразности внедрения систем обеспечения информационной безопасности?...(Методика оценки вероятности возникновения угроз, анализ последствий нарушений безопасности, оценка финансовых рисков).

13. Какие технологии могут быть внедрены для обеспечения информационной безопасности киберфизических систем?...(Биометрическая аутентификация, системы мониторинга и анализа сетевой активности, средства защиты от DDoS-атак).

14. Какие факторы следует учитывать при оценке целесообразности внедрения систем обеспечения информационной безопасности?...(Финансовые затраты и потенциальные убытки от нарушений безопасности, степень важности информации для компании, законодательные требования).

15. Какие методы обучения и поддержки персонала используются при внедрении систем обеспечения информационной безопасности?...(Обучающие курсы и тренинги по безопасности информации, проведение семинаров и вебинаров, распространение

ПК-3.3

Короткий ответ

1. Какие методы моделирования используются для анализа работы киберфизических систем?....(**Моделирование событий, моделирование нагрузок, моделирование времени отклика**).
2. Какие методы управления применяются в киберфизических системах?...(Пропорционально-интегрально-дифференциальное управление (PID), методы машинного обучения, адаптивное управление).
3. Какие аспекты учитываются при выборе аппаратных компонентов для киберфизических систем?...(Производительность, энергоэффективность, надежность).
4. Какие методы тестирования применяются для верификации киберфизических систем?...(Модульное тестирование, интеграционное тестирование, системное тестирование).
5. Какие принципы обеспечивают масштабируемость киберфизических систем?...(Распределенность, горизонтальное масштабирование, вертикальное масштабирование).
6. Какие методы сбора и обработки данных используются в киберфизических системах?...(Сенсоры и актуаторы, обработка потоков данных (stream processing), базы данных временных рядов (time series databases)).
7. Какие вызовы возникают при проектировании киберфизических систем?...(Интеграция различных технологий, обеспечение безопасности, оптимизация производительности).
8. Какие методы обеспечивают отказоустойчивость в киберфизических системах?...(Дублирование компонентов, резервирование ресурсов, автоматическое восстановление).
9. Какие требования предъявляются к сетевой инфраструктуре для поддержки киберфизических систем?...(Надежность передачи данных, низкая задержка (латентность), высокая пропускная способность).
10. Какие инструменты используются для разработки программного обеспечения киберфизических систем?...(Интегрированные среды разработки (IDE), языки программирования для встраиваемых систем, средства моделирования и анализа).

ПК-1.3

Короткий ответ:

1. Какие методы классификации информации используются при систематизации научно-технической информации?...(По уровню конфиденциальности, по типу угроз, по видам кибератак).
2. Какие виды информационных систем могут быть использованы для систематизации научно-технической информации?...(Системы управления базами данных (СУБД), системы управления контентом (CMS), системы управления знаниями (KM)).
3. Какие методы математического моделирования могут быть применены для решения задач в области безопасности киберфизических систем?...(Метод конечных элементов (МКЭ),

методы оптимизации, моделирование случайных процессов).

4. Какие технические средства мониторинга используются для обеспечения безопасности киберфизических систем?...(**Системы видеонаблюдения, датчики контроля доступа, системы обнаружения вторжений (IDS)**).

5. Какие методы анализа статистических данных применяются для оценки уровня угроз в области безопасности киберфизических систем?...(**Методы временных рядов, методы корреляционного анализа, методы машинного обучения**).

6. Какие методы экспериментов могут быть использованы для научных исследований в области безопасности киберфизических систем?...(**Лабораторные эксперименты, полевые эксперименты, симуляция моделей**).

7. Какие методы организации по источникам информации используются при систематизации научно-технической информации?...(**По авторам, по издательствам, по дате публикации**).

8. Какие методы машинного обучения могут быть применены для анализа статистических данных в области безопасности киберфизических систем?...(**Деревья решений, метод опорных векторов, нейронные сети**).

9. Какие средства визуализации данных используются для отображения результатов анализа статистической информации?...(**Графики, диаграммы, географические карты**).

10. Какие методы оптимизации могут быть применены для повышения эффективности систем безопасности киберфизических систем?...(**Методы генетических алгоритмов, методы линейного программирования, методы имитации отжига**).

ПК-1.6

Множественный выбор:

1. Какой из нижеперечисленных компонентов является программным?
А) Двигатель
Б) Алгоритм управления роботом
В) Датчик температуры
2. Какие механические компоненты обычно используются в киберфизических системах?
А) Электродвигатели
Б) Гидравлические цилиндры
В) Все перечисленные варианты
3. Какая из нижеперечисленных функций относится к программным компонентам киберфизических систем?
А) Преобразование электрического сигнала в механическое движение
Б) Управление траекторией движения робота
В) Все перечисленные варианты
4. Какой из нижеперечисленных примеров является интеграцией механических и программных компонентов в киберфизической системе?
А) Автомобиль с антиблокировочной тормозной системой (ABS)
Б) Кофейный автомат с автоматическим выбором напитка
В) Все перечисленные варианты
5. Какие технологические тренды в области программных компонентов киберфизических

систем наиболее перспективны?

- А) Использование искусственного интеллекта для оптимизации процессов управления**
- Б) Разработка специализированных операционных систем для киберфизических систем
- В) Все перечисленные варианты

Короткий ответ

6. Что такое механические компоненты в киберфизических системах?...(Это физические устройства, которые обеспечивают механическое движение или изменение состояния).

7. Какие компоненты управляют механическими устройствами в киберфизических системах?...(Программные компоненты, такие как алгоритмы управления и системы автоматизации).

8. Какие примеры механических компонентов можно найти в киберфизических системах?...(Двигатели, датчики, клапаны, гидравлические и пневматические системы).

9. Что представляют собой программные компоненты в киберфизических системах?...(Это программное обеспечение, которое управляет работой механических компонентов и обрабатывает данные).

10. Какие задачи выполняют программные компоненты в киберфизических системах?...(Управление движением, сбор и анализ данных, оптимизация процессов и принятие решений).

11. Какие технологии используются для создания механических компонентов в киберфизических системах?...(3D-печать, CNC-обработка, использование новых материалов (например, нанотехнологии)).

12. Какие языки программирования чаще всего применяются для разработки программных компонентов киберфизических систем?...(C/C++, Python, Java, MATLAB/Simulink).

13. Какие примеры киберфизических систем сочетают в себе механические и программные компоненты?...(Автоматизированные производственные линии, роботы-манипуляторы, автономные транспортные средства).

14. Какие преимущества применения киберфизических систем совместно с механическими и программными компонентами?...(Увеличение производительности, снижение затрат, повышение безопасности и надежности).

15. Какие вызовы и проблемы могут возникнуть при интеграции механических и программных компонентов в киберфизических системах?...(Сложность согласования работы различных компонентов, уязвимости кибербезопасности, необходимость постоянной оптимизации).

№ задания	Содержание задания	Коды компетенций
1	Перечислите основные структурные части КФС.	ПК-4.1
2	В чем отличия "узкой" и "широкой" трактовки понятия КФС?	ПК-4.1
3	Перечислите основные факторы появления появления КФС как нового класса систем.	ПК-4.1
4	Опишите связь понятий Интернета вещей и КФС.	ПК-4.1

5	Дайте характеристику актуальных проблем проектирования КФС.	ПК-4.1
6	Как принцип Копеца характеризует соотношение системы и ее моделей?	ПК-4.1
7	Почему важно закладывать высокую степень адаптивности в современные системы автоматики?	ПК-4.1
8	Перечислите направления компьютеринга в соответствии с Computing Curricula 2020.	ПК-4.1
9	В каких областях знаний должен иметь подготовку специалист по проектированию КФС?	ПК-4.1
10	Назначение стандарта Essence.	ПК-3.3
11	Общее описание метода ARCADIA.	ПК-3.3
12	Перечислите и охарактеризуйте составные части ядра Essence.	ПК-3.3
13	Что такое альфа ядра Essence? Перечислите стандартные альфы ядра.	ПК-3.3
14	Опишите графическую нотацию изображения «альф» и «суб-альф» ядра Essence.	ПК-3.3
15	Какие области деятельности определяет ядро Essence?	ПК-3.3
16	Какие компетенции определяет ядро Essence? Перечислите и охарактеризуйте уровни владения компетенциями.	ПК-1.3, ПК-1.6
17	Перечислите основные элементы языка Essence и связи между ними.	ПК-1.3, ПК-1.6
18	Опишите модификации Essence для системной инженерии.	ПК-1.3, ПК-1.6
19	Какую последовательность шагов определяет метод ARCADIA.	ПК-1.3, ПК-1.6
20	Какие компоненты входят в состав системное ПО для обеспечения безопасного и надежного функционирования прикладной программы.	ПК-1.3, ПК-1.6
21	Принцип актуализации вычислительного процесса в проектировании ВеС.	ПК-1.3, ПК-1.6
22	Объяснить модель актуализации вычислительного процесса.	ПК-1.3, ПК-1.6
23	Объяснить суть трансляторов в модели актуализации вычислительного процесса.	ПК-1.3, ПК-1.6
24	Что из себя представляют фазы актуализации вычислительного процесса ВСС.	ПК-1.3, ПК-1.6