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

Технологии обеспечения информационной безопасности объектов

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	Критерий оценивания	Средства (методы) оценивания промежуточной аттестации
ПК-5.1 Владеет научными методами сбора и обработки информации	1.Осуществляет системный анализ прикладной области с целью выявления угроз и оценки уязвимости информационных систем. 2.Умеет системно получать, анализировать и накапливать информацию с элементами прогнозирования по вопросам, относящимся к безопасности объекта. 3.Умеет выбирать способы решения прикладных проблем информационной безопасности 4.Может прогнозировать основные опасности и угрозы, возникающие в процессе информационного взаимодействия. 5.Анализирует в прикладной области с целью выявления угроз и оценки уязвимости информационных систем в условиях становления современного информационного общества.	Устное собеседование по теоретическим вопросам

2. Критерии оценивания в рамках промежуточной аттестации (Экзамен)

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	76 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Обучающийся в целом правильно интерпретирует полученный результат.	75-61 – ответ в основном правильный, логически выстроен, использована профессиональная терминология.	менее 60 – ответы на теоретическую часть неправильные или неполные.

КЕЙС-ЗАДАНИЯ ДЛЯ ТЕСТИРОВАНИЯ

Задания открытого типа (ПК-5)	
Что представляет собой системный анализ прикладной области с целью выявления угроз и оценки уязвимости информационных систем?	Системный анализ прикладной области включает в себя изучение структуры и функционирования информационных систем для выявления угроз безопасности и оценки уязвимостей.
Какие основные задачи решает системный анализ информации с элементами прогнозирования по вопросам безопасности объекта?	Системный анализ информации помогает выявить потенциальные угрозы безопасности объекта и разработать меры по их предотвращению.
Какие способы решения прикладных проблем информационной безопасности можно выбрать?	Способы решения прикладных проблем информационной безопасности могут включать в себя технические, организационные и правовые меры.
Что включает в себя прогноз основных опасностей и угроз, возникающих в процессе информационного взаимодействия?	Прогноз опасностей и угроз включает в себя анализ потенциальных рисков и разработку стратегий по их минимизации.
Какие методы можно использовать для анализа прикладной области с целью выявления угроз и оценки уязвимости информационных систем?	Методы SWOT-анализа, анализа уязвимостей, анализа рисков, экспертных оценок и т.д.
Что означает оценка уязвимости информационных систем в условиях становления современного информационного общества?	Оценка уязвимости информационных систем позволяет определить степень их подверженности угрозам в условиях быстрого развития информационных технологий.
Какие основные этапы включает в себя системный анализ прикладной области с целью обеспечения информационной безопасности?	Анализ текущего состояния, выявление уязвимостей, разработка мер по защите, контроль и мониторинг.
Какие факторы необходимо учитывать при выборе способов решения прикладных проблем информационной безопасности?	Технические возможности, бюджетные ограничения, особенности организации и другие факторы.
Какие методы прогнозирования опасностей и угроз используются при системном анализе информации?	Статистические данные, экспертные оценки, сценарный анализ, моделирование угроз.
Какие меры безопасности могут быть предприняты на основе результатов анализа прикладной области?	Внедрение шифрования данных, контроль доступа, обучение персонала, создание резервных копий и др.
Какие основные принципы следует соблюдать при проведении системного анализа информации с элементами прогнозирования по вопросам безопасности объекта?	Принцип комплексного подхода, принцип минимизации рисков, принцип непрерывного мониторинга.

Какие инструменты могут использоваться для проведения системного анализа прикладной области с целью выявления угроз и оценки уязвимости информационных систем?	Специализированные программы для анализа уязвимостей, методики SWOT-анализа, матрицы рисков и др.
Какие последствия могут возникнуть при недостаточной оценке уязвимости информационных систем?	Утечка конфиденциальной информации, нарушение работоспособности системы, финансовые потери.
Какие методы могут помочь предсказать возможные угрозы и опасности в процессе информационного взаимодействия?.	Методы анализа трендов, мониторинг новостей и событий, прогнозирование развития технологий
Какие факторы могут повлиять на выбор способов решения прикладных проблем информационной безопасности?	Сложность системы, наличие специалистов, бюджетные ограничения, законодательство.
Какие методы анализа рисков можно использовать для оценки уязвимости информационных систем?	Методика определения вероятности возникновения угроз, методика оценки потенциального ущерба, матрица рисков.
Какие практические рекомендации можно дать по проведению системного анализа прикладной области для обеспечения информационной безопасности?	Проводить регулярный мониторинг уязвимостей, обновлять программное обеспечение, обучать персонал по правилам безопасности.
Какие основные этапы включает в себя прогноз основных опасностей и угроз в процессе информационного взаимодействия?	Идентификация потенциальных угроз, анализ последствий возможных атак, разработка планов защиты.
Какие методы анализа прикладной области помогут выявить уязвимости информационных систем?	Аудит безопасности, сканирование уязвимостей, тестирование на проникновение
Какие основные требования следует учитывать при выборе способов решения прикладных проблем информационной безопасности?	Эффективность защиты, соответствие законодательству, соблюдение стандартов безопасности.
Что представляет собой системный анализ прикладной области с целью выявления угроз и оценки уязвимости информационных систем?	Системный анализ прикладной области включает в себя изучение структуры и функционирования информационных систем для выявления угроз безопасности и оценки уязвимостей.
Задания закрытого типа (ПК-5)	
1. Что такое системный анализ?	Б

А) Исследование информационных систем Б) Анализ функционирования системы в целом В) Оценка уязвимости компьютерной сети	
2. Какие цели преследует системный анализ прикладной области? А) Выявление угроз информационной безопасности Б) Оценка эффективности программного обеспечения В) Анализ рыночных тенденций	А
3. Какие методы используются для прогнозирования опасностей и угроз в информационном взаимодействии? А) SWOT-анализ Б) Метод дерева решений В) Анализ временных рядов	Б
4. Что такое уязвимость информационной системы? А) Возможность несанкционированного доступа к данным Б) Наличие низкоскоростного интернет-соединения, что в процессе приводит к перехвату «пакетов» и доступ в ИС В) Отсутствие антивирусного программного обеспечения	А
5. Какие основные опасности могут возникать в процессе информационного взаимодействия? А) Вирусы и вредоносное ПО Б) Сбои в работе оборудования В) Недостаточная производительность сотрудников	А
6. Какие методы оценки угроз информационной безопасности существуют? А) Метод анализа стоимости ущерба (TCO) Б) Метод маркетингового исследования В) Метод экспертных оценок	А
7. Что означает понятие "прогнозирование опасностей" в контексте информационной безопасности? А) Определение вероятности возникновения угрозы Б) Прогноз погоды В) Разработка новых методов шифрования данных	А
8. Какие инструменты системного анализа можно использовать для выявления уязвимостей информационных систем? А) Анализ, методы ISO 27000	В

Б) Методология TOGAF В) Метод дерева принятия решений	
9. Что такое SWOT-анализ в контексте системного анализа информационных систем? А) Комплексный анализ внутренних и внешних факторов Б) Метод прогнозирования кибератак В) Анализ производительности сети Г) Анализ, методы ISO 27001	А
10. Какие Меры, применяемые в управлении риска угроз могут возникать в процессе информационного взаимодействия? А) Кибератаки, утечка конфиденциальной информации, отказ в обслуживании (DDoS) Б) Низкая скорость интернет-соединения, отсутствие обновлений ПО, слабый пароль для доступа к системе В) Недостаточная производительность сотрудников, конфликты в коллективе, неправильная организация рабочего процесса	А

Короткий ответ

Информационно-коммуникационные технологии играют важную роль в решении ……., таких как защита данных, обеспечение конфиденциальности и целостности информации, контроль доступа, а также иных комплексных мероприятий ИБ (**фундаментальных проблем информационной безопасности**).

Зависимость требований от структуры объектов информатизации означает, что каждый объект может иметь свои ……в зависимости от его функциональности, данных, пользователей и других факторов (**уникальные требования к информационной безопасности**)

Проблемы информационной безопасности в условиях становления современного информационного общества включают в себя увеличение объема данных, рост киберугроз, сложность технологий, а также необходимость защиты…... (**ИСПДн и защита объектов КИИ**).

Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, ……. либо иные требования к порядку ее предоставления или распространения (**если федеральными законами не установлены ограничения доступа к информации**).

Информационные системы включают в себя:
государственные информационные системы - федеральные информационные системы и региональные информационные системы,……., законов субъектов Российской Федерации, на основании правовых актов государственных органов (**созданные на основании соответственно федеральных законов**).

В случае создания или модернизации информационной системы на основании концессионного соглашения, соглашения о государственно-частном партнерстве или соглашения о муниципально-частном партнерстве функции оператора информационной системы в пределах, в объемах и в сроки, которые предусмотрены……. (**соответствующим соглашением, осуществляются концессионером или частным партнером соответственно**).

Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны……. (**размещаться на территории Российской Федерации**).

Порядок создания и эксплуатации ИС, не являющихся государственными ИС или муниципальными ИС, определяется …….с требованиями, установленными настоящим ФЗ (**операторами таких информационных систем в соответствии**).

Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов, называется …… (**Государственная информационная система**)

Что определяют следующие условия: 1. Создание в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях; 2. Создаются, модернизируются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения гос. и мун. нужд либо законодательством РФ о ГЧП, о МЧП, законодательством о концессионных соглашениях, в соответствии с иными федеральными законами;3. Создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.
……. (**принципы создания ГИС**).

Вопросы для собеседования

№	Вопрос	Ответ
1.	Реализация системного анализа прикладной области для выявления угроз и оценки уязвимости информационных систем	Реализация системного анализа прикладной области для выявления угроз и оценки уязвимости информационных систем включает в себя изучение структуры и функционирования системы, выявление потенциальных угроз безопасности, оценку уязвимостей и разработку мер по их предотвращению.
2.	Методы и инструменты системного анализа для выявления угроз информационной безопасности	Методы и инструменты системного анализа для выявления угроз информационной безопасности могут включать в себя SWOT-анализ, анализ уязвимостей, анализ рисков, экспертные оценки, использование специализированных программ для анализа уязвимостей и другие методики.
3.	Опыт получения, анализа и накопления информации с элементами прогнозирования вопросов, связанных с безопасностью объекта	Опыт получения, анализа и накопления информации с элементами прогнозирования вопросов, связанных с безопасностью объекта помогает предсказать возможные угрозы, опасности и разработать стратегии защиты информационных систем.
4.	Требования информационной безопасности	Требования информационной безопасности включают в себя конфиденциальность, целостность, доступность данных, аутентификацию, авторизацию, аудит безопасности, защиту от вредоносных программ и другие аспекты.
5.	Зависимость требований от структуры объектов информатизации.	Зависимость требований от структуры объектов информатизации означает, что каждый объект может иметь свои уникальные требования к безопасности в зависимости от его функциональности, данных, пользователей и других факторов.
6.	Технологии формирования алгоритмов обработки информации.	Технологии формирования алгоритмов обработки информации включают в себя методы шифрования, хэширования, цифровой подписи, контроля целостности данных и другие методы для обеспечения безопасности информации.
7.	Информационно-коммуникационные технологии в фундаментальных проблемах информационной безопасности.	Информационно-коммуникационные технологии играют важную роль в решении фундаментальных проблем информационной безопасности, таких как защита данных, обеспечение конфиденциальности и целостности информации, контроль доступа и т.д.
8.	Информационно-коммуникационные технологии для выявления и анализа информационной безопасности.	Информационно-коммуникационные технологии для выявления и анализа информационной безопасности включают в себя системы мониторинга, детекции инцидентов, аналитику данных, системы предупреждения и реагирования на угрозы.
9.	Проблемы информационной безопасности в условиях становления современного информационного общества.	Проблемы информационной безопасности в условиях становления современного информационного общества включают в себя увеличение объема данных, рост киберугроз, сложность технологий, необходимость защиты персональных данных и другие вызовы.
10.	Специфика технологий обеспечения информационной безопасности объектов защиты.	Специфика технологий обеспечения информационной безопасности объектов защиты зависит от их функциональности, значимости данных, уровня доступа пользователей, возможных угроз и других факторов.

11.	Требования к технологиям обеспечения информационной безопасности объектов защиты.	Требования к технологиям обеспечения информационной безопасности объектов защиты включают в себя надежность, эффективность защиты, соответствие законодательству, минимизацию рисков и другие аспекты.
12.	Методы анализа информационной системы для выбора технологий обеспечения информационной безопасности.	Методы анализа информационной системы для выбора технологий обеспечения информационной безопасности могут включать в себя аудит безопасности, оценку уязвимостей, определение потенциальных угроз и разработку стратегии защиты на основе полученных результатов.