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

Комплексное обеспечение информационной безопасности

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-6.1. Разрабатывает системы, комплексы, средства и технологии обеспечения информационной безопасности, а также программы и методики испытаний средств и систем обеспечения информационной безопасности	Знает средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации. Демонстрирует навыки в вопросах методологии проектирования, реализации, оценки качества и анализа стандартов и методик, а также в области стандартизации и управлении качеством программного обеспечения.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий.

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-6)	
Что такое брандмауэр?	Это программно-аппаратный комплекс, предназначенный для защиты компьютерной сети от несанкционированного доступа.
Что такое система обнаружения вторжений (IDS)?	Это система, предназначенная для обнаружения попыток несанкционированного доступа к сети или компьютерным ресурсам.
Какие технические средства могут использоваться для предотвращения вторжений?	Брандмауэр, антивирусное ПО, система обнаружения вторжений (IDS)
Какие методы предотвращения утечки информации через USB-устройства могут быть использованы?	Блокирование USB-портов, установка политик контроля доступа к USB-устройствам, использование защищенных USB-накопителей.
Что такое система предотвращения утечки данных (DLP)?	Это система, предназначенная для контроля и предотвращения утечки конфиденциальной информации.

Какие виды угроз могут быть обнаружены с помощью систем обнаружения вторжений (IDS)?	Атаки на отказ в обслуживании (DoS), внедрение вредоносного ПО, несанкционированный доступ к сети.
Какие методы предотвращения утечки информации через сетевые каналы могут быть использованы?	Шифрование сетевого трафика, установка брандмауэра и контроль доступа, использование виртуальных частных сетей (VPN).
Какие методы обнаружения утечки информации могут использоваться для контроля сетевого трафика?	Deep packet inspection (DPI), анализ журналов событий, мониторинг аномального поведения сети
Какие технические каналы утечки информации могут быть использованы злоумышленниками?	Сетевые каналы, USB-устройства, принтеры и сканеры.
Какие методы предотвращения утечки информации через принтеры и сканеры могут быть использованы?	Установка политик печати и сканирования, шифрование печатаемых документов, мониторинг действий пользователей с принтерами и сканерами.
Что такое жизненный цикл разработки программного обеспечения?	Это последовательность этапов, через которые проходит разрабатываемое программное обеспечение: сбор требований, проектирование, реализация, тестирование, внедрение и поддержка.
Что такое методология Agile?	Это подход к разработке программного обеспечения, основанный на итеративной разработке, где требования и решения эволюционируют через совместную работу самоорганизующихся и многофункциональных команд.
Что такое тестирование программного обеспечения?	Это процесс проверки программы на соответствие требованиям и выявление ошибок и дефектов.
Какие основные принципы лежат в основе управления качеством программного обеспечения?	Непрерывное улучшение, участие персонала, фокус на клиенте, процессный подход, принятие решений на основе данных.
Что такое ISO 9000 в контексте программного обеспечения?	Это серия международных стандартов, устанавливающих требования к системам управления качеством и обеспечению качества продукции и услуг.
Что такое процесс стандартизации в области программного обеспечения?	Это процесс разработки и утверждения стандартов, руководящих документов и методик в области разработки, управления и оценки качества программного обеспечения.

Какие основные виды тестирования программного обеспечения существуют?	Модульное тестирование, интеграционное тестирование, системное тестирование, приемочное тестирование.
Что такое процесс оценки качества программного обеспечения?	Это процесс определения соответствия программного обеспечения установленным требованиям и оценки его характеристик.
Какие основные принципы лежат в основе методологии DevOps?	Автоматизация, непрерывная поставка, частые изменения, сотрудничество между разработкой и операционной деятельностью.
Что такое принципы СПИ (Software Process Improvement)?	Это набор методов и инструментов для улучшения процессов разработки программного обеспечения с целью повышения их эффективности и качества.
Задания закрытого типа (ПК-6)	
Какой метод используется для обнаружения вторжений в реальном времени? А) Системы мониторинга сетевого трафика Б) Анализ уязвимостей В) Шифрование данных Г) Регулярное обновление ПО	А
Какой стандарт относится к области стандартизации информационной безопасности? А) ISO/IEC 27001 Б) ISO 9001 В) ISO/IEC 25010 Г) ISO 14001	А
Какие инструменты могут использоваться для анализа стандартов в области информационной безопасности? А) GRC (Governance, Risk, and Compliance) Б) SWOT-анализ В) PDCA (Plan-Do-Check-Act) Г) Все вышеперечисленное	А
Какие стандарты могут использоваться для управления качеством программного обеспечения? А) ISO/IEC 9126 Б) ISO 20000 В) ISO 27001 Г) Все вышеперечисленное	А
Какие инструменты могут использоваться для анализа стандартов в области информационной безопасности? А) SWOT-анализ Б) GAP-анализ В) Парето-анализ	Б

Г) Все вышеперечисленное	
Какой методологии следует придерживаться при проектировании безопасной системы? А) Secure by Design Б) Security through Obscurity В) Security by Patching Г) Все вышеперечисленное	А
Какое средство позволяет обнаружить вторжение в компьютерную сеть? А) IDS (система обнаружения вторжений) Б) Файерволы В) Антивирусные программы Г) VPN (виртуальная частная сеть)	А
Какие методики могут применяться для анализа рисков информационной безопасности? А) Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Б) Методика SWOT-анализа В) Методика PDCA (Plan-Do-Check-Act) Г) Все вышеперечисленное	А
Какие меры безопасности могут быть рекомендованы для защиты от социальной инженерии? А) Ограничение доступа к конфиденциальной информации Б) Обучение сотрудников распознаванию признаков социальной инженерии В) Регулярная проверка физической безопасности помещений Г) Все вышеперечисленное	Б
Какие методы могут использоваться для предотвращения утечек конфиденциальной информации через технические каналы? А) Мониторинг сетевого трафика и обнаружение подозрительных активностей Б) Установка систем защиты от утечек данных (DLP) В) Шифрование данных при передаче и хранении Г) Все вышеперечисленное	Г

Вопросы для собеседования

№	Вопрос	Ответ
1.	Охарактеризуйте классы безопасности компьютерных систем.	- Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. - Целостность: защита информации от несанкционированных изменений. - Доступность: гарантирование доступности информации для авторизованных пользователей в нужное время.
2.	Какие ресурсы системы должны быть защищаемы и в какой степени?	- Данные: должны быть защищены от несанкционированного доступа и изменений. - Системы: должны быть защищены от взлома и уязвимостей. - Сети: должны быть защищены от атак и утечек данных.
3.	Какие угрозы должны быть устранены и в какой мере?	- Вредоносные программы: должны быть обнаружены и удалены сразу же. - Фишинг и социальная инженерия: должны быть предотвращены для защиты конфиденциальных данных. - DDoS-атаки: должны быть отражены для обеспечения доступности сервисов.
4.	Взаимодействие структурных подразделений по вопросам ИБ АС.	Структурные подразделения, ответственные за ИБ, должны регулярно обмениваться информацией, координировать действия и реагировать на угрозы совместно.
5.	Фильтрация трафика; выполнение функций посредничества.	- Фильтрация трафика позволяет контролировать и ограничивать передачу данных через сеть. - Функции посредничества могут включать контроль доступа, аутентификацию и шифрование данных.
6.	Фильтрующий маршрутизатор; шлюз сеансового уровня модели 0SI/1S0	- Фильтрующий маршрутизатор контролирует трафик на основе заданных правил безопасности. - Шлюз сеансового уровня модели OSI/ISO обеспечивает безопасное взаимодействие между различными узлами сети.
7.	Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 3 34.10-2001.	- Алгоритм ЭП DSA (Digital Signature Algorithm) используется для создания и проверки цифровой подписи. - Алгоритм ЭП ГОСТ 34.10-2001 является российским стандартом для электронной подписи.
8.	Варианты создания защищенных виртуальных каналов.	- Использование VPN (виртуальной частной сети) - Шифрование трафика с помощью SSL/TLS - Использование прокси-серверов для анонимизации данных

9.	Средства создания VPN.	- Программное обеспечение для настройки VPN-соединений - Облачные VPN-сервисы - VPN-роутеры для защиты всей сети
10.	Организация антивирусной защиты.	- Установка антивирусного программного обеспечения на все устройства - Регулярное обновление баз вирусных сигнатур - Проведение сканирования системы на наличие вредоносных программ
11.	Задачи ИБ в программе « цифровая экономика»	- Защита цифровых активов и данных - Обеспечение конфиденциальности информации - Предотвращение кибератак и утечек данных
12.	Доктрина информационной безопасности России.	Документ, определяющий стратегические приоритеты и задачи в области информационной безопасности России. Включает в себя меры по защите критической информационной инфраструктуры, борьбе с киберугрозами и укреплению кибероборонь.