МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КОСТРОМСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ»

Утверждаю:
И.о. декана электроэнергетического факультета
Николай Александрович Климов
Подписано цифровой подписью: Николай Александрович Климов
Дата: 2024.09.11 16:13:20 +03'00'
_____ /Климов Н.А./
11 сентября 2024 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность 09.02.07 Информационные системы и программирование

Квалификация выпускника программист

Форма обучения очная

Срок освоения ППССЗ 3 года 10 месяцев

На базе основного общего образования

Караваево 2024

Фонд оценочных средств предназначен для оценивания сформированности компетенций по дисциплине «Обеспечение качества функционирования компьютерных систем».

Разработчик:
преподаватель А.В. Смирнов Александр Владимирович Смирнов Подписано цифровой подписью: Александр Владимирович Смирнов

Утвержден на заседании кафедры информационных технологий в электроэнергетике, протокол № 1 от 05.09.2024

Заведующий кафедрой Н.А. Климов Николай Александрович Климов Подписано цифровой подписью: Николай Александрович Климов Дата: 2024.09.05 14:48:54 +03'00'

Согласовано:
Председатель методической комиссии электроэнергетического факультета

А.С. Яблоков Алексей Сергеевич Яблоков Подписано цифровой подписью: Алексей Сергеевич Яблоков Дата: 2024.09.10 15:15:02 +03'00'
протокол № 7 от 10.09.2024

Результаты освоения дисциплины

«Обеспечение качества функционирования компьютерных систем»

ППССЗ (СПО) по специальности:

09.02.07 Информационные системы и программирование

Коды компетенций по ФГОС	Компетенции	Результат освоения
Общие компетенции		
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	**Знать** формат оформления результатов поиска информации, порядок применения современных средств и устройств информатизации, как применять программное обеспечение в профессиональной деятельности, в том числе с использованием цифровых средств. **Уметь** оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; планировать процесс поиска; структурировать получаемую информацию; оформлять результаты поиска информации, пользоваться современными средствами поиска информатизации. **Владеть** навыками оформления результатов поиска информации; навыками планирования процесса поиска и структурирования полученной информации.
Профессиональные компетенции		
ПК 4.3	Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика	**Знать** основные принципы контроля конфигурации и поддержки целостности конфигурации программного обеспечения **Уметь** производить настройку отдельных компонентов программного обеспечения компьютерных систем **Владеть** навыками модификации отдельных компонентов программного обеспечения в соответствии с потребностями заказчика
ПК 4.4	Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.	**Знать** средства защиты программного обеспечения в компьютерных системах **Уметь** использовать методы защиты программного обеспечения компьютерных систем **Владеть** навыками по обеспечению защиты программного обеспечения компьютерных систем программными средствами

Паспорт
фонда оценочных средств

Таблица 1

№ п/п	Контролируемые дидактические единицы	Контролируемые компетенции (или их части)	Наименование оценочных средств		
			Тесты, кол-во заданий	Другие оценочные средства	
				вид	кол-во заданий
1	Тема 1. Основные методы обеспечения качества функционирования	ОК 02 ПК 4.3	20	Опрос	5
2	Тема 2. Методы и средства защиты компьютерных систем	ОК 02 ПК 4.4	20	Опрос	5
8	Темы 1-2	ОК 02 ПК 4.3 ПК 4.4		Собеседование	20
Всего:			40		30

Методика проведения контроля по проверке базовых знаний по дисциплине «Обеспечение качества функционирования компьютерных систем»

Тема 1 Основные методы обеспечения качества функционирования

Контролируемые компетенции (знания, умения) ОК 02; ПК 4.3

Вопросы для устного опроса

1. Какова роль автоматизированного тестирования в обеспечении качества программного обеспечения, и какие основные методы и инструменты могут быть использованы для его реализации?
2. Как могут быть интегрированы практики DevOps и CI/CD в процесс обеспечения качества компьютерных систем, и какие инструменты могут быть наиболее эффективны для этих процессов?
3. Какие методы мониторинга и управления производительностью систем можно использовать для обеспечения высокого уровня доступности и надежности приложений в условиях растущей нагрузки?
4. Каким образом тестирование безопасности (security testing) может быть интегрировано в общий процесс обеспечения качества ПО, и какие инструменты и методы следует использовать для выявления уязвимостей?
5. Какова роль подхода Agile в обеспечении качества разработки программных систем, и какие места в Agile-методологиях предназначены для проведения обеспечения качества на каждом этапе цикла разработки?

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который прочно усвоил программный материал в полном объеме, исчерпывающе, грамотно и логически стройно его излагает, четко формулирует основные понятия, приводит соответствующие примеры, уверенно владеет материалом.

Оценка «хорошо» выставляется обучающемуся, который твердо усвоил программный материал, грамотно и по существу излагает его без существенных ошибок, правильно применяет теоретические положения при решении конкретных задач, с небольшими погрешностями приводит формулировки определений, по ходу изложения допускает небольшие пробелы, не искажающие содержания ответа.

Оценка «удовлетворительно» выставляется обучающемуся, который не совсем твердо владеет программным материалом, знает основные теоретические положения изучаемой темы, при ответах допускает малосущественные погрешности, искажения логической последовательности при изложении материала, неточную аргументацию теоретических положений, испытывает затруднения при ответе на дополнительные вопросы.

Оценка «неудовлетворительно» выставляется обучающемуся, имеющему серьезные пробелы в знании учебного материала, допускающему принципиальные ошибки при ответе на вопросы.

Тестовые задания

Выберите один правильный вариант ответа и нажмите кнопку «Далее»

К методам обеспечения качества программного обеспечения НЕ относится:

Тестирование
Обзор кода
+Проектирование.
Анализ требований

Для процесса тестирования справедливо утверждение:
Тестирование всегда проводится в конце разработки
Тестирование проводится только для выявления ошибок
+Тестирование помогает улучшить качество программного обеспечения.
Тестирование не является обязательным этапом разработки

Тест-кейс – это:
документ, описывающий функциональность программного обеспечения
+набор действий, выполняемых для проверки определенного аспекта системы.
инструмент для автоматизации тестирования
программа, используемая для создания тестовых данных

Для метрик качества справедливо утверждение:
Метрики качества не имеют практического значения
Метрики качества используются только для оценки производительности
+Метрики качества помогают объективно оценить качество системы.
Метрики качества не могут быть использованы для сравнения различных систем

Регрессионное тестирование – это:
+тестирование, проводимое после внесения изменений в программное обеспечение.
тестирование, проводимое для проверки совместимости системы с другими приложениями
тестирование, проводимое для проверки функциональности системы в различных условиях
тестирование, проводимое для проверки безопасности системы

К стандартам качества программного обеспечения НЕ относится:
ISO 9001
IEEE 829
ГОСТ Р 51904
+ГОСТ Р 51500.

"Дефект" – это:
+ошибка в программном обеспечении, приводящая к некорректному функционированию.
недостаток в документации системы
проблема с производительностью системы
ошибка в дизайне системы

Для автоматизации тестирования НЕ используется:
Selenium
JMeter
+Git.
TestComplete

"Бета-тестирование" – это тестирование, проводимое:
разработчиками программного обеспечения
+группой пользователей до официального выпуска.
в лабораторных условиях
на реальных данных

Для процесса обеспечения качества справедливо утверждение:
Обеспечение качества - это задача только разработчиков.
+Обеспечение качества - это непрерывный процесс, охватывающий весь жизненный цикл системы.
Обеспечение качества - это одноразовая процедура, проводимая перед выпуском системы.
Обеспечение качества - это задача только тестировщиков.

Целью обеспечения качества функционирования компьютерных систем НЕ является:
Увеличение производительности системы
Снижение количества ошибок
Улучшение безопасности системы
+Увеличение стоимости разработки системы.

Метод тестирования, используемый для проверки соответствия системы установленным требованиям, называется:
Белое тестирование
Черное тестирование
+Функциональное тестирование.
Нагрузочное тестирование

Регрессионное тестирование – это тестирование:
новой функциональности системы
+ системы после внесения изменений.
системы с целью выявления ошибок
системы с целью оптимизации производительности

Метрики качества – это:
+критерии оценки качества системы.
методы тестирования системы
инструменты для разработки системы
схемы документирования системы

Метод тестирования, НЕ являющийся автоматизированным, называется:
Модульное тестирование
Тестирование производительности
Функциональное тестирование
+Ручное тестирование.

CI/CD – это:
метод разработки программного обеспечения
система управления версиями
+процесс непрерывной интеграции и доставки.
инструмент для проведения тестирования

Для метода тестирования “черный ящик” справедливо утверждение:
Тестировщик знает внутреннее устройство системы
+Тестировщик не знает внутреннее устройство системы.
Тестировщик разрабатывает тест-кейсы на основе кода системы
Тестировщик проводит тестирование с использованием специального оборудования

Bug tracking – это:
метод устранения ошибок в системе
+система для отслеживания и управления ошибками.
процесс написания документации по ошибкам
инструмент для анализа кода системы

К качеству пользовательского интерфейса НЕ относится:
Время загрузки страницы
Простота использования
Соответствие стандартам
+Количество функций.

Code review – это:
+процесс проверки кода разработчиками.
процесс анализа качества кода
процесс исправления ошибок в коде
процесс оптимизации кода

Методика проведения контроля

Параметры методики	Значение параметра
Предел длительности всего контроля	10 минут
Последовательность выбора вопросов	Случайная
Предлагаемое количество вопросов	10

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно выполнил 9-10 тестовых заданий.

Оценка «хорошо» выставляется обучающемуся, который: правильно выполнил 7-8 тестовых заданий.

Оценка «удовлетворительно» выставляется обучающемуся, который правильно выполнил 5-6 тестовых заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, который правильно выполнил менее 4 тестовых заданий.

Тема 2. Методы и средства защиты компьютерных систем

Контролируемые компетенции (знания, умения) ОК 02 ПК 4.4

Вопросы для устного опроса

1. Каким образом можно использовать атаку “побочного канала” для получения конфиденциальной информации, защищенной алгоритмом шифрования AES-256, если известно, что время выполнения операций шифрования зависит от используемых ключей?
2. В чем заключается основное отличие между атакой “man-in-the-middle” и атакой “replay attack” на протокол TLS/SSL? Как можно защититься от обоих типов атак?
3. Опишите принцип работы системы обнаружения вторжений (IDS) на основе машинного обучения и приведите примеры сценариев, когда такая система может давать ложные срабатывания.
4. Каковы преимущества и недостатки использования односторонних функций хэширования в системах аутентификации? Как можно минимизировать риски, связанные с использованием хэширования в контексте атак “brute-force”?
5. Какие меры безопасности необходимо предпринять для защиты данных, хранящихся в облачном хранилище от утечки и несанкционированного доступа, если разработчик облачной платформы не предоставляет детальную информацию о применяемых механизмах защиты?

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который прочно усвоил программный материал в полном объеме, исчерпывающе, грамотно и логически стройно его излагает, четко формулирует основные понятия, приводит соответствующие примеры, уверенно владеет материалом.

Оценка «хорошо» выставляется обучающемуся, который твердо усвоил программный материал, грамотно и по существу излагает его без существенных ошибок, правильно применяет теоретические положения при решении конкретных задач, с небольшими погрешностями приводит формулировки определений, по ходу изложения допускает небольшие пробелы, не искажающие содержания ответа.

Оценка «удовлетворительно» выставляется обучающемуся, который не совсем твердо владеет программным материалом, знает основные теоретические положения изучаемой темы, при ответах допускает малосущественные погрешности, искажения логической последовательности при изложении материала, неточную аргументацию теоретических положений, испытывает затруднения при ответе на дополнительные вопросы.

Оценка «неудовлетворительно» выставляется обучающемуся, имеющему серьезные пробелы в знании учебного материала, допускающему принципиальные ошибки при ответе на вопросы.

Тестовые задания

Выберите один правильный вариант ответа и нажмите кнопку «Далее»

Методом аутентификации НЕ является:

+пароль
биометрическая аутентификация
многофакторная аутентификация
шифрование данных

Брандмауэр – это:

программа, которая защищает компьютер от вирусов
+программа, которая блокирует нежелательные сетевые соединения

устройство, которое шифрует данные
программа, которая защищает от атак “отказ в обслуживании” (dos)
Симметричным алгоритмом шифрования является:
RSA
+AES
ECC
DSA

Фишинговая атака – это атака, направленная на:
+ получение доступа к учетным данным пользователя
внедрение вредоносного кода в систему
перехват данных в сети
отказ в обслуживании

Методом защиты от атак “отказ в обслуживании” (DoS) НЕ является:
брандмауэр
система обнаружения вторжений (ids)
+антивирусная программа
противодействие ботнетам

Вирус – это программа, которая:
может самовоспроизводиться
крадет данные
повреждает файлы
+все вышеперечисленное

Методом защиты от несанкционированного доступа к данным НЕ является:
шифрование данных
парольная защита
многофакторная аутентификация
+защита от вирусов

Хэширование – это:
метод шифрования данных
+метод проверки целостности данных
метод аутентификации пользователей
метод защиты от атак “отказ в обслуживании”

Для безопасного соединения с веб-сайтом используется протокол:
FTP
HTTP
+HTTPS
SMTP
Криптография – это:
+наука о защите информации
метод шифрования данных
метод аутентификации пользователей
метод защиты от атак “отказ в обслуживании”

Атаки на уровне сети наиболее эффективно предотвращает:
антивирусное программное обеспечение
+межсетевой экран (фаервол)

шифрование данных
регулярные обновления по

Система обнаружения вторжений (IDS) – это:
программа для шифрования данных
устройство, которое физически блокирует доступ к сети
+средство, анализирующее трафик и выявляющее подозрительную активность
антивирусный инструмент для удаления вредоносного по

Для управления безопасностью информации в организациях используется стандарт:
ISO 9001
+ISO 27001
COBIT
ITIL

Метод шифрования, наиболее безопасным для передачи данных, считается:
RSA
DES
+AES
Blowfish

Примером социальной инженерии является:
взлом пароля через брутфорс
+фишинг через электронную почту
установка антивирусного по
использование vpn-сервиса

Методов аутентификации, обеспечивающий наивысший уровень безопасности, называется:
пароль
+биоаутентификация (например, отпечатки пальцев)
смарт-карта
ответ на контрольный вопрос

"Предотвращения утечек данных" (DLP) – это:
идентификация пользователей
например, технология контроля доступа к физическим кабинетам
+политики и технологии, обеспечивающие защиту конфиденциальной информации
процесс резервного копирования данных
Технология, предназначенная для обеспечения конфиденциальности и аутентификации в компьютерных сетях, называется:
NAT
+SSL/TLS
DHCP
HTTP

Тип атаки, направленный на избыточное использование ресурсов системы, называется:
SQL-инъекция
+DDoS-атака
XSS-уязвимость
Криптографическая атака

Метод управления уязвимостями, предназначенный для регулярного проведения тестирования безопасности, называется:
Политика доступа
Управление патчами
Процесс рисков
+Пентестинг

Методика проведения контроля

Параметры методики	Значение параметра
Предел длительности всего контроля	10 минут
Последовательность выбора вопросов	Случайная
Предлагаемое количество вопросов	10

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно выполнил 9-10 тестовых заданий.

Оценка «хорошо» выставляется обучающемуся, который: правильно выполнил 7-8 тестовых заданий.

Оценка «удовлетворительно» выставляется обучающемуся, который правильно выполнил 5-6 тестовых заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, который правильно выполнил менее 4 тестовых заданий.

Вопросы для собеседования

Контролируемые компетенции (знания, умения) ОК 02; ПК 4.3; ПК 4.4

1.Многоуровневая защита (Defense in Depth)
2.Технология предотвращения вторжений (Intrusion Prevention Systems, IPS)
3.Обнаружение аномалий (Anomaly Detection)
4.Криптографические протоколы
5.Управление уязвимостями
6.Модели оценки надежности
7.Анализ жизненного цикла программного обеспечения (SDLC)
8.Метрики качества ПО
9.Тестирование с помощью симуляции (Simulation-based Testing)
10.Обеспечение качества на этапе эксплуатации
11.Каковы основные принципы многоуровневой защиты в компьютерных системах, и как они помогают в снижении рисков безопасности?
12.Как IPS отличается от систем обнаружения вторжений (IDS), и какие ключевые технологии используются для их реализации?
13.В чем разница между обнаружением аномалий и обнаружением сигнатур, и какие методы машинного обучения применяются для реализации обнаружения аномалий?
14.Обсудите основные криптографические протоколы, используемые для защиты данных в транзите, такие как TLS, и их значение для безопасности компьютерных систем.
15.Как осуществляется процесс управления уязвимостями, и какая роль анализа угроз и рисков в этом процессе?
16.Объясните основные методы оценки надежности программного обеспечения, такие как модель МКП (Markov Chain Processes) и как они относятся к системам с высокой доступностью.
17.Как концепция SDLC влияет на обеспечение качества в программных системах, и какие методологии (например, Agile, Waterfall) предпочтительнее для обеспечения качества?

18.Какие основные метрики качества программного обеспечения (например, COQ, Defect Density) используются для оценки его качества, и как они могут помогать в процессе разработки?
19.Как симуляция может использоваться для испытания систем в условиях, приближенных к реальным, и какие преимущества она предоставляет по сравнению с традиционными методами тестирования?
20.Каковы основные принципы и методы обеспечения качества функционирования компьютерных систем на этапе эксплуатации, и какую роль играют метрики производительности в этом процессе?

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, который правильно ответил на 5 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 4 вопроса правильно, но рассчитывает получить оценку «отлично» ему задаётся дополнительный вопрос ответить.

Оценка «хорошо» выставляется обучающемуся, который: правильно ответил на 4 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 3 вопроса правильно, но рассчитывает получить оценку «хорошо» ему задаётся дополнительный вопрос.

Оценка «удовлетворительно» выставляется обучающемуся, который: правильно ответил на 3 случайно выбранных вопросов, показав достаточный уровень знаний. В случае если студент ответил на 2 вопроса правильно, но рассчитывает получить оценку «удовлетворительно» ему задаётся дополнительный вопрос.

Оценка «неудовлетворительно» выставляется обучающемуся, который не ответил ни на один вопрос или ответил на 1 или 2 вопроса верно, но не ответил на дополнительный вопрос

Форма промежуточной аттестации по дисциплине *зачет с оценкой*.

Окончательные результаты обучения (формирования компетенций) определяются посредством перевода баллов, набранных студентом в процессе освоения дисциплины, в оценки:

– базовый уровень сформированности компетенции считается достигнутым, если результат обучения соответствует оценке «удовлетворительно» (50-64 рейтинговых баллов);

– повышенный уровень сформированности компетенции считается достигнутым, если результат обучения соответствует оценкам «хорошо» (65-85 рейтинговых баллов) и «отлично» (86-100 рейтинговых баллов).

Дополнительные контрольные испытания

для студентов, набравших менее 50 баллов (в соответствии с Положением «О модульно-рейтинговой системе»), формируются из числа оценочных средств по темам, которые не освоены студентом.