Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

—УТВЕРЖДАЮ‖
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
—__‖_____г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Проектирование и разработка безопасных программных систем

Образовательная программа: 10.04.01 Информационная безопасность, профиль: Методы и средства обеспечения технической защиты информации

Новосибирск - 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

В 3 семестре обязательным этапом текущей аттестации является курсовая работа. Требования к выполнению курсовой работы, состав и правила оценки сформулированы в паспорте курсовой работы

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме экзамена, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций УК-1 и ПК-2 и соотнесенных с ними индикаторов.

Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 2, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций УК-1 и ПК-2, закрепленных за дисциплиной.

2. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт экзамена

по дисциплине «Проектирование и разработка безопасных программных систем», 3 семестр

1. Методика оценки Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).
Тестовые задания охватывают все содержание дисциплины «Проектирование и разработка безопасных программных систем». Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на 5/6 вопросов теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов и не допускает ошибок при решении задач. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 35 до 40 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления, не допускает существенных ошибок при решении задач. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 34 до 27 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от 1/2 до 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 26 до 20 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 20 баллов.*

3. Шкала оценки Экзамен считается сданным, если сумма баллов по всем заданиям билета составляет от 20 до 40 баллов включительно. Сумма менее 20 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста[1]) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	1. знает процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения 2. умеет принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий 3. владеет методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях

Вопросы теста для оценки сформированности компетенции УК-1

Вопрос 1. Требования DevOps – DevSecOps. Выберите пункты
- ○ наличие DevOps инструментов ✔
- ○ соблюдены требования ФСТЭК России
- ○ наличие специализированных сертификатов проведен аудит сотрудников безопасности

(один вариант)

Вопрос 2. Как называется система, записывающая изменения в файл или набор файлов в течение времени и позволяющая вернуться позже к определѐнной версии? *Ответ:* **Решение:** Контроль версий SCM – это способ управления и документирования изменений, вносимых разработчиками в код программного обеспечения . Система контроля версий – это программное обеспечение, позволяющее создавать версии элементов и работать с этими версиями, как с самостоятельными элементами. В англоязычных источниках используется термин version control systems, сокращенно VCS.

Вопрос 3. Назовите базу данных общеизвестных уязвимостей информационной безопасности *Ответ:* **Решение:** Такая единая база существует. Она называется CVE - база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием CVE.

Вопрос 4. Каковы рекомендации перехода DevOps – DevSecOps?
- ○ Коллективная ответственность, Сотрудничество и интеграция, Прагматичная реализация Измерение, мониторинг, протоколирование и действие
- ○ Обеспечение соответствия стандартам и разработки, Автоматизация

[1] Правильные ответы выделены галочкой

Коллективная ответственность, Сотрудничество и интеграция, Прагматичная реализация, Обеспечение соответствия стандартам и разработки, Автоматизация, Измерение, мониторинг, протоколирование и действие ✔

(один вариант)

Вопрос 5. Как называются программы и программные комплексы, позволяющие централизованно управлять конфигурацией множества разнообразных разрозненных операционных систем и прикладного программного обеспечения, работающего в них *Ответ:*

Решение: Система управления конфигурациями, управление конфигурациями. В англоязычной терминологии – CVS, Concurrent Versions System.

Вопрос 6. Какая система является ядром автоматизации? *Ответ:* **Решение:** В области автоматизации разработки ПО - CI/CD система. Аббревиатура CI/CD означает «Continuous Integration/Continuous Delivery» — то есть «непрерывная интеграция/непрерывная доставка». Это подход к разработке, при котором задачи сборки, публикации, тестирования продукта полностью или частично автоматизированы.

Вопрос 7. DevSecOps это методология? Да

Нет ✔

(один вариант)

Вопрос 8. Security Champions.

Ориентирован на риски

Осведомленность безопасности

Дать возможность обеспечению безопасности

Все пункты ✔

(один вариант)

Вопрос 9. Какой анализатор представляет собой проверку программы на наличие уязвимостей непосредственно во время ее выполнения? *Ответ:*

Решение: DAST, динамический анализатор. Dynamic Application Security Testing – это одна из практик безопасной разработки. В рамках DAST проводится автоматизированный анализ развѐрнутого и функционирующего приложения. Динамический сканер проверяет все точки доступа по HTTP, имитирует внешние атаки с применением распространѐнных уязвимостей, моделирует случайные действия пользователей. Инструмент определяет, какие API есть у сервиса, отправляет проверочные запросы, например подставляет, где это возможно, неправильные данные…

Вопрос 10. С какой целью вводится паттерн Security Champions? Выберите пункты.

☐ Консультирование команды по вопросам ИБ ✔

☐ Переход DevOps – DevSecOps

☐ Проведение код-ревью, тренингов ✔

☐ Работа с инструментальным стеком ИБ ✔

(возможно нескольких вариантов)

Вопрос 11. Какой анализатор представляет собой тип тестирования, при котором не происходит выполнения программы, а анализируется весь ее код? *Ответ:* **Решение:** SAST, статический анализатор приложения с доступом к исходному коду (методом «белого ящика»). Поиск уязвимостей во многих тысячах строках кода вручную требует огромных затрат времени.

SAST ускоряет этот процесс. Одной из ключевых сильных сторон SAST является широкий охват языков программирования и платформ разработки

Вопрос 12. Основные отличия культуры программирования.

- Сборка, Скорость, Компиляция
- Размер кодовой базы, Скорость, Тестирование ✔
- Документация, Тестирование, Алгоритмы
- Производительность, Интерфейс, Компиляция

(один вариант)

Вопрос 13. Какое средство анализирует код на наличие уязвимостей безопасности, пока приложение запускается автоматическим тестом, тестером-человеком или любым действием, «взаимодействующим» с функциональностью приложения?

Ответ:

Решение: IAST, интерактивный анализатор. Исторически существуют статический (SAST) и динамический (DAST) анализ. IAST реализует гибридный подход к анализу софта.

Вопрос 14. Безопасность в безопасном программировании

- Надежность
- Целостность, Доступность, Конфиденциальность
- Атрибут качества ✔
- Все пункты

(один вариант)

Вопрос 15. Какой анализатор позволяет обнаруживать уязвимые компоненты, дефекты безопасности или проблемы с условиями лицензирования? *Ответ:* **Решение:** SCA, анализ состава программного обеспечения. Открытый исходный код может содержать критические уязвимости. SCA – это процесс определения компонентов (в особенности – с открытым исходным кодом), из которых состоит программное обеспечение, и проверки их безопасности.

Вопрос 16. Назовите открытый проект обеспечения безопасности веб-приложений или сообщество. Работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе *Ответ:* **Решение:** OWASP. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. OWASP не аффилирован ни с одной компанией, занимающейся разработкой технологий, но он поддерживает грамотное использование технологий безопасности.

Вопрос 17. Какой анализатор позволяет приложению проводить непрерывные проверки безопасности и отвечать на атаки в реальном времени, завершая сеанс злоумышленника и предупреждая защитников об атаке?

Ответ:

Решение: RASP, защита приложений в реальном времени. Runtime Application Self-Protection – технология безопасности, которая обнаруживает и блокирует атаки на приложения в реальном времени с помощью

добавления функций защиты в среду исполнения, что дает приложению возможность «самозащиты» в автоматическом режиме.

Вопрос 18. Что позволяет защитить приложение, даже если защита периметра сети нарушена? *Ответ:*

Решение: RASP, защита приложений в реальном времени. RASP добавляет в приложение функцию «самозащиты» от внешних атак.

19. Какой анализатор рекомендуются внедрить в первую очередь?

Ответ:

Решение: При анализе приложения должен осуществляться системный подход. Логично в первую очередь использовать SAST, статический анализатор.

Вопрос 20. Какой анализатор зависит от языка программирования? *Ответ:*

Решение: SAST, статический анализатор. По той причине, что он исследует исходный код приложения, написанный на том или ином языке.

Вопрос 21. По какому стандарту происходит идентификация уязвимостей в DAST? *Ответ:* **Решение:** OWASP топ 10. Это отчет или информационный документ от OWASP, в котором перечислены основные проблемы, связанные с безопасностью веб-приложений. Он регулярно обновляется, чтобы постоянно отображать 10 наиболее серьезных рисков, с которыми сталкиваются организации.

Вопрос 22. Какой анализатор может мешать работе тестировщиков? *Ответ:*

Решение: DAST, динамический анализатор. Из-за отсутствия доступа к исходному коду DAST не позволяет проанализировать внутреннюю структуру приложения и его архитектуру. Это затрудняет выявление потенциальных уязвимостей, связанных с нарушениями принципов безопасного программирования или архитектурных решений.

Вопрос 23. Чем можно обнаружить транзитивные зависимости?

Ответ:

Решение: Сторонние компоненты софта очень часто зависят от других сторонних компонент, в то же время ваш продукт состоит и из них. Такие элементы называются транзитивными зависимостями. Их может обнаружить SCA – анализатор состава программного обеспечения.

Вопрос 24. Кем разработан ГОСТ по безопасному программированию? *Ответ:*

Решение: ФСТЭК России. Им разработан ГОСТ Р 56939-2016. «Защита информации. РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Общие требования»

Вопрос 25. Какой вид документации является обязательной для выполнения в безопасном программировании? *Ответ:*

Решение: ГОСТ относится к нормативной документации, обязательной для исполнения. Конечно, в том случае, если продукция или деятельность попадает под сферу применения данного стандарта.

Вопрос 26. Самая популярная уязвимость OWASP топ 10 на момент 2023 года *Ответ:* **Решение:** Впервые рейтинг OWASP был опубликован в 2003 году и впоследствии выпускался каждые три- четыре года. В 2023 году на первом месте рейтинга стоит «Инъекция». Это атака заключается в инъекции SQL-запросов через входной интерфейс приложения.

Вопрос 27. Числовая оценка, показывающая потенциальную серьѐзность уязвимости. Она основана на стандартизированном наборе характеристик *Ответ:*

Решение: CVSS, система оценки уязвимостей. В случае CVSS v3.0 оценка лежит в диапазоне от 0 до 10, и, по мере возрастания еѐ значения, уязвимость меняется от низкой и средней до высокой и критической.

28. Назовите стандарт разработки программного обеспечения, целью которого является улучшение безопасности, переносимости и надежности программ для встраиваемых систем. Существует набор руководящих принципов для языка C и C++. *Ответ:* **Решение:** MISRA & AUTOSAR. Первый - стандарт разработки программного обеспечения на языке Си, разработанный MISRA (Motor Industry Software Reliability Association). Цель стандарта – улучшить безопасность, переносимость и надѐжность программ для встраиваемых систем. Второй, AUTOSAR – это партнерство по развитию заинтересованных сторон в автомобильной отрасли, основанное в 2003 году. Оно преследует цель создать и внедрить открытую и стандартизированную архитектуру программного обеспечения для автомобильных электронных блоков управления (ЭБУ).

Вопрос 29. Меры по разработке безопасного ПО могут применяться для каких объектов?
Ответ:

Решение: Разработчику ПО следует определить область действия реализуемых мер по разработке безопасного ПО. Область действия реализуемых мер – для разрабатываемого ПО, для группы, для организации.

Вопрос 30. Как называется этический кодекс для специалистов по информационной безопасности, созданный форумом группы реагирования на инциденты и обеспечения безопасности? *Ответ:* **Решение:** ethicsfIRST, или Ethics for Incident Response and Security Teams. Вышеупомянутые команды специалистов имеют доступ ко многим цифровым системам и источникам информации. Их действия могут изменить мир. Будучи представителем этой профессии, член команды должен осознавать свою ответственность перед другими специалистами в области безопасности, а также перед обществом в целом.

Формируемая компетенции	Индикаторы компетенции
ПК-2.В/НИ Способен разрабатывать решения для программных и технических средств защиты информации	1. умеет формулировать требования по безопасности для разработки программного продукта 2. умеет применять принципы безопасного проектирования программных систем

Вопросы теста для оценки сформированности компетенции ПК-2В/ НИ

Вопрос 31. Разработчику ПО следует разработать и описать процедуры, которые будут использоваться для безопасного распространения ПО или его отдельных частей. Основной целью таких процедур является обеспечение возможности обнаружения каких воздействий на ПО? *Ответ:*

Решение: Модификация информации.

Вопрос 32. Варианты получения кода при анализе.

- ○ source, open source
- ○ source, internal code
- ○ external code, internal code
- ○ **open source, external code, internal code** ✔

(один вариант)

Вопрос 33. С чего стоит начать анализировать код в большом проекте? *Ответ:*

Решение: функция main.

Вопрос 34. IAST анализатор защищает приложение?

- **Нет** ✔
- Да

(один вариант)

35. Сколько практик в Synopsys BSIMM? *Ответ:*

Решение: 12

Вопрос 36. Дополните: ..... - официальный реестр или словарь общих дефектов безопасности, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к системе? *Ответ:*

Решение: CWE

Вопрос 37. Как влияет внедрение RASP-анализатора на производительность системы?

- **Ухудшает производительность, поскольку анализ происходит в реальном времени и требует дополнительных ресурсов.** ✔
- Не оказывает никакого влияния на производительность, так как анализ проводится в фоновом режиме.
- Улучшает производительность за счёт оптимизации запросов к базам данных.
- Существенно улучшает производительность, так как уменьшает количество ошибок в коде.

(один вариант)

Вопрос 38. Какова самая популярная уязвимость топ 25 CWE на момент 2023 года? *Ответ:*

Решение: CWE 787.

Вопрос 39. Что следует учесть в первую очередь, при внедрении нескольких анализаторов кода? *Ответ:*

Решение: растущее время сканирования.

Вопрос 40. Дополните: ..... - список требований или тестов для проверки безопасности приложений во фреймворке OWASP SAMM *Ответ:*

Решение: ASVS.

Вопрос 41. Руководство по тестированию безопасности web-приложений, входящее во фреймворк OWASP SAMM
Ответ:

Решение: Руководство по тестированию веб-безопасности

Вопрос 42. Время жизни уязвимости. Что входит?

- ☐ CWE
- ☐ Various error
- ☐ CVE
- ☐ **Все ответы верны** ✔

(один вариант)

Вопрос 43. Дополните: Модель обеспечения безопасности программного обеспечения ..... позволяет оценить уровень зрелости на каждой итерации развития ИБ в компании, а также предлагает набор методов по еѐ улучшению *Ответ:*

Решение: SAMM.

Вопрос 44. Классифицируйте в CWE уязвимость, связанную с неправильной или ненадежной аутентификацией пользователей. Эта уязвимость может привести к предоставлению злоумышленникам конфиденциальной информации или к выполнению произвольного кода

- ☐ **CWE 287. неправильная аутентификация** ✔
- ☐ CWE-89: SQL Injection
- ☐ CWE-79: (XSS)
- ☐ CWE-352: CSRF

(один вариант)

Вопрос 45. Какой инструмент может помочь в определении уязвимости на раннем этапе разработки? *Ответ:*

Решение: Компилятор среды разработки.

Вопрос 46. К какому топу уязвимостей относится небезопасный дизайн? *Ответ:*

Решение: OWASP топ 10.

Вопрос 47. В чем заключается основное отличие анализа в "сером ящике" от анализа в "черном ящике"?

- ☐ анализ в "сером ящике" включает частичный доступ к исходному коду, а анализ в "черном ящике" выполняется без доступа к коду.
- ☐ **анализ в "сером ящике" включает частичный доступ к исходному коду, тогда как анализ в "черном ящике" выполняется без всякого доступа к коду.** ✔
- ☐ анализ в "черном ящике" использует автоматизированные инструменты, а анализ в "сером ящике" выполняется вручную.
- ☐ анализ в "сером ящике" проводится с полным пониманием внутренней структуры системы, в отличие от анализа в "черном ящике"

(один вариант)

Вопрос 48. К какому домену относятся практики для сбора и консолидации знаний в области ИБ внутри организации? *Ответ:*

Решение: разведка.

Вопрос 49. Деятельность «Требовать подтверждения безопасности для рисков, связанных с соблюдением требований» фремворка Synopsys BSIMM необходима для какого уровня зрелости? *Ответ:*

Решение: Для второго

Вопрос 50. Какую методологию называют ―гибкой‖? *Ответ:*

Решение: Agile.

Вопрос 51. Связующее звено между инженерией, разработкой и тестированием

Ответ:

Решение: Безопасность

Вопрос 52. Как называется модель с общим «корнем» и двумя «ветвями»?
Ответ:

Решение: V-Model.

Вопрос 53. классическая модель жизненного цикла разработки ПО. Была придумана в 1950-х годах, и, пока не появился Agile, все продукты и проекты реализовывали с еѐ помощью
Ответ:

Решение: водопад.

Вопрос 54. Что характеризуют пункты: - Безопасное проектирование. - Моделирование угроз. - Безопасная разработка. - Тестирование ПО в части безопасности. - Обеспечение приватности. *Ответ:*
Решение: тренинг безопасности.

Вопрос 55. Как называется концепция разработки, заключающаяся в обеспечении безопасности разрабатываемого приложения, идентификации рисков и управления им?

- DevOps
- **Secure Software Development Lifecycle (SSDLC).** ✔
- Agile.
- Continuous Integration

(один вариант)

Вопрос 56. Интегрировать SCA нельзя на уровне.

- CVS
- IDE
- **Monitoring** ✔
- CI

(один вариант)

Вопрос 57. ____ ___ ___ представляет собой несколько этапов (или фаз), которые проходит любое ПО?
Ответ:

Решение: Жизненный цикл ПО.

Вопрос 58. Кол-во бизнес-функций в OWASP SAMM? *Ответ:*

Решение: 5.

Вопрос 59. На каком уровне разработки программного обеспечения обычно интегрируется инструмент статического анализа безопасности приложений (SAST)?

- после развертывания приложения.
- **во время компиляции исходного кода.** ✔
- в процессе тестирования.
- при планировании требований

(один вариант)

Вопрос 60. Сколько существует уровней зрелости компании? *Ответ:*

Решение: 3

Паспорт курсовой работы

по дисциплине «Проектирование и разработка безопасных программных систем», 3 семестр

1. Методика оценки.

Выполнение курсовой работы (далее – КР) является обязательным видом самостоятельной работы студента по дисциплине, предусмотренным учебным планом.

Основной целью выполнения КР является формирование компетенций и соотнесенных с ними индикаторов по дисциплине «Проектирование и разработка безопасных программных систем», 3 семестр, посредством закрепления, углубления и обобщения знаний, полученных студентами за время теоретического обучения и прохождения практик, а также выработка навыков самостоятельного применения знаний и навыков для творческого решения конкретных задач. Выполнение курсовой работы должно способствовать подготовке их к решению более сложной задачи - выполнению выпускной квалификационной работы.

Задачами выполнения курсовой работы является овладение студентами рациональными приѐмами сбора, обработки, систематизации информации, применения компьютерных технологий в области разработки безопасного программного обеспечения и применения нормативно-законодательной базы.

Тематика КР соответствует профилю (направленности) подготовки, формируются преподавателями в начале семестра и утверждаются на заседании кафедры ЗИ. Количество тем КР – достаточное для обеспечения каждого обучающегося.

Выполнение студентами КР начинается с ознакомления с примерной тематикой. Закрепление тем КР за студентами и назначение научных руководителей производится распоряжением заведующего кафедрой и/или утверждается решением кафедры. Курсовая работа выполняется индивидуально.

Структура курсовой работы:

1. Титульный лист
2. Введение (актуальность, цель, задачи).
3. Теоретическая часть, включающая в себя четкий развернутый ответ на вопрос, включающий в себя анализ темы исследования по разработке безопасной программной системы.
4. Практическая часть.
5. Заключение (выводы и рекомендации).
6. Список литературы и источников.

Во введении производится обзор заданной предметной области и возможные проблемы данной предметной области.

Теоретическая часть включает в себя концептуальное проектирование модели системы, в рамках которой происходит выбор системы моделирования, выбор первоначальных сущностей или объектов (зависит от выбранной студентом модели).

Практическая часть включает в себя логическое проектирование, выявление основных правил модели, проектирование построенной системы и еѐ тестирование на предмет выявления уязвимостей.

Заключение: изложение общего вывода по решаемым задачам и предлагаемых рекомендаций. Список литературы оформляется в соответствии с библиографическими требованиями в алфавитном порядке и включает от 5 до 25 источников (книг, статей разных авторов, интернет-источников, документов), которые были изучены при выполнении работы.

Требования к оформлению:

Объем КР до 50 страниц машинописного текста формата А4. Шрифт Times New Roman, 14. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. КР должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Законченная курсовая работа предоставляется для проверки в электронном виде в срок, установленный преподавателем. Преподаватель оценивает качество КР с учетом теоретического и практического содержания, достижения ее целей и задач.

Если при выполнении КР были допущены ошибки, то работа возвращается студенту для исправления выявленных недочетов и затем вновь предоставляется руководителю для проверки. При положительном результате оценивания студент распечатывает работу, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита КР проходит в формате беседы с преподавателем.

По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

2. Уровни сформированности компетенций и критерии оценки

В соответствии с балльно-рейтинговой системой НГТУ курсовая работа дисциплине «Проектирование и разработка безопасных программных систем», 3 семестр, имеет максимальную оценку 100 баллов.

Курсовая работа выполнена **на продвинутом** уровне, если:

- она выполнена в полном соответствии с заданием, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно (в частности, отмечает его инициативу, самостоятельность, систематичность работы на всех этапах выполнения работы);
- в докладе исчерпывающе, последовательно, четко и логически правильно изложена суть работы и ее основные результаты;
- студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач, сформулированных в задании;
- в докладе суть работы и ее основные результаты представлены исчерпывающе, последовательно, четко и логически правильно; на все вопросы студент дал обстоятельные и аргументированные ответы, убедительно защищал свою точку зрения; - компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которым выполняется курсовая работа сформированы в полном объеме.

Оценка за выполнение КР составляет *100-87 баллов.*

Курсовая работа выполнена на **базовом** уровне, если:

- соответствует заданию, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно, но с незначительными замечаниями;
- в докладе правильно изложена суть работы и ее основные результаты;
- студент достаточно твердо усвоил теоретический материал и может самостоятельно его применять;
- в докладе суть работы и ее основные результаты представлены полно; на все вопросы студент дал ответы, но их полнота и аргументированность недостаточны;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которым выполняется курсовая работа сформированы с небольшими пробелами и соответствуют базовому уровню.

Оценка за выполнение КР составляет *86-73 балла*.

Курсовая работа выполнена **на пороговом** уровне, если:
- выполнена в основном правильно, но без необходимой проработки некоторых разделов;
- в докладе упущены некоторые принципиальные моменты содержательной части работы;
- в докладе представлены суть работы и ее основные результаты; ответы на вопросы вызвали существенные затруднения;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которым выполняется курсовая работа сформированы с пробелами и соответствуют пороговому уровню.

Оценка за выполнение КР составляет *72-50 баллов.*

Курсовая работа считается **не выполненной,** если студентом не проработаны важные разделы исследования, допущены принципиальные ошибки, не исправленные после замечаний руководителя курсовой КР. Студент не допущен к защите курсовой работы. компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которым выполняется курсовая работа не сформированы. Оценка составляет *менее 50 баллов*.

3. Шкала оценки.

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

Курсовая работа по дисциплине считается успешно выполненной, если сумма полученных баллов составляет от 100 до 50 баллов включительно.

Оценка за выполнение КР является частью общей оценки по дисциплине «Проектирование и разработка безопасных программных систем», 3 семестр и учитывается с коэффициентом 20 баллов в соответствии с правилами аттестации по дисциплине.

4. Примерный перечень тем курсовой работы

1. Разработка программного обеспечения для управления доступом к защищенным объектам в регионе

2. Разработка приложения, для анализа тестов и опросов, проводимых в регион
3. Разработка чат-бота для ответов на типовые вопросы студентов преподавателям
4. Разработка чат-бота для управления записью клиентов в косметологическом салоне
5. Анализ пунктуальности и эффективного времени работы работников в организации 6. Разработка приложения для координации волонтѐрского движения в рамках региональной политик
7. Разработка системы обработки заявок сервисного центра
8. Разработка базы данных клиентов летнего пансионата
9. Разработка системы управления доставками грузов по городу
10. Разработка приложения по оценке тормозного пути автомобиля, при различных параметрах
11. Разработка приложения для знакомств по общим интересам
12. Разработка приложения, для предсказания успеваемости студентов на основе предыдущих результатов
13. Разработка приложения для определения времени в пути на пригородных поездах
14. Разработка программного обеспечения для обеспечения защищенного соединения
15. Загрузчик зашифрованного shell – кода
16. Разработка удаленного управляющего программного модуля для загрузки и выгрузки данных
17. Разработка приложения по подбору лекарств на основании информации из интернет-магазинов
18. Разработка голосового помощника по управлению элементами умного дома для лиц с ограниченными возможностями.
19. Разработка чат-бота для использования внутри организации
20. Моделирование работы склада с использованием многопоточности процессов 21. Разработка приложения для обеспечения контроля за запросами пользователей в локальной сети
22. Разработка приложения оценки загруженности общественного трафика
23. Разработка приложения по контролю питания
24. Разработка приложения для проведения голосования и последующего анализа результатов
25. Разработка приложения по анализу звуковых записей кашля для определения хрипов

5. Примерный перечень вопросов к защите курсовой работы

1. В чем выражена проблематика выбранной предметной области с точки зрения защиты информации?
2. Какие моменты необходимо учитывать в процессе проектирования и разработки?
3. Чем вы руководствовались при выборе модели проектирования?
4. Какие проблемы были на логическом этапе проектирования?
5. Как вы обеспечили безопасность программного обеспечения?
6. Какие инструменты использовали для тестирования вашей программы?
7. Вы использовали статическое, динамическое или интерактивное тестирование программы?
8. Какие нормативные документы по разработке безопасного ПО вы знаете?

9. Какие библиотеки уязвимостей вам известны?
10. Какой методологией вы руководствовались в ходе разработке своей программы?