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

Паспорт зачета

по дисциплине «Методология безопасной разработки и эксплуатации программного обеспечения», 8 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:

- первый вопрос выбирается из диапазона вопросов 1-12;
- второй вопрос из диапазона вопросов 13-25.

Таким образом, проверяются результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

На зачете преподаватель вправе задавать студенту уточняющие и дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Методология безопасной разработки и эксплуатации программного обеспечения»

---

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

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

Ответ на билет для зачета засчитывается на **продвинутом** уровне, если студент проводит сравнительный комплексный анализ материала, выявляет проблемы, предлагает механизмы их решения, представляет количественные характеристики определенных процессов, приводит конкретные примеры. 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* 18 *до* 20 *баллов.*

Ответ на билет для зачета засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, дает характеристику процессов, явлений, проводит анализ причин, условий, способен представить количественные и качественные характеристики процессов. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от* 1*4 до* 17 *баллов.*

Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений. 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* 1*0 до* 13 *баллов.*

Ответ на билет для зачета считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 1*0 баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

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

4. Вопросы к зачету по дисциплине «Методология безопасной разработки и эксплуатации программного обеспечения»

1. Аудит информационной безопасности и понятие тестирования на проникновение.
2. Основные методы и подходы при проведении аудита информационной системы и приложений.
3. Типовые примеры эксплуатации уязвимостей и слабостей системы.
4. Подходы к поиску уязвимостей в ПО.
5. Основные уязвимости и понятия, которые встречаются при реализации web-приложений.
6. Уязвимости в Web-приложениях.
7. Внедрение кода на клиенте. Обход аутентификации и CSRF-атаки.
8. Инструментарий для анализа Web-приложений. OWASP-Top10.
9. Внедрение кода на сервере.
10. SQL-инъекции.
11. XML-инъекции и другие типы инъекций.
12. Уязвимости, связанные с манипуляциями программной памяти.
13. Организация памяти в современном программном обеспечении. Переполнение буфера на стеке.
14. Уязвимости в динамической памяти. Уязвимости форматной строки. Инструментарий для поиска уязвимостей.

15. Ошибки, связанные с целочисленным переполнением.
16. Раскрытие информации. «Состояние гонки».
17. Некорректная обработка исключений.
18. Слабости в реализации криптографических модулей приложения.
19. Уязвимости вне программных средств.
20. Уязвимости, связанные с политикой безопасности и бизнес-процессами в организации.
21. Социальная инженерия.
22. Программные средства для анализа кода.
23. Средства для статического и динамического анализа исходного кода приложений.
24. Декомпиляция приложений.
25. Инъекции команд.