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

Паспорт экзамена

по дисциплине «Программные средства профессиональной деятельности», 7 семестр

1. Методика оценки

Экзамен проводится в устной (письменной) форме, по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:

- первый вопрос выбирается из диапазона вопросов 1-15;
- второй вопрос из диапазона вопросов 16-29.

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

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

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Программные средства профессиональной деятельности»

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 экзаменационный билет 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 (модулю) 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.*

Ответ на экзаменационный билет 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 (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.*

Ответ на экзаменационный билет 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 (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от* 26 *до* 20 *баллов.*

Ответ на экзаменационный билет 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 (модулю) 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 (модулю).

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

4. **Вопросы к** экзамену **по дисциплине «**Программные средства профессиональной деятельности**»**

1. Какие основные классы сетевых средств защиты информации вы знаете и каковы их функции?
2. Как сетевые средства защиты интегрируются в общую архитектуру безопасности организации?
3. Какие виды DDoS-атак существуют и как они работают?
4. Какие методы и средства защиты от DDoS-атак применяются?
5. Какие стратегии резервного копирования существуют?
6. Что такое правило 3-2-1 резервного копирования и как оно обеспечивает надёжность хранения данных?
7. Какие типы виртуализации существуют и каковы их особенности?
8. Какие угрозы безопасности характерны для виртуализированных сред?
9. Какие механизмы безопасности используются в контейнерах?
10. Что такое SIEM-система и какие основные функции она выполняет?
11. Что такое EDR (Endpoint Detection and Response) и чем он отличается от традиционного антивируса?
12. Что такое XDR (Extended Detection and Response) и какие преимущества он даёт по сравнению с EDR?
13. Что такое SOAR-платформа и какие задачи она решает в процессе реагирования на

инциденты?
14. Как автоматизация процессов безопасности ускоряет реагирование на инциденты?
15. Какие типы сканеров безопасности существуют и как они работают?
16. Как организуется процесс управления уязвимостями?
17. Какие каналы утечки информации контролируются DLP-системами?
18. Что такое MDM, EMM и UEM? Чем они отличаются друг от друга?
19. Что такое IAM (Identity and Access Management) и какие компоненты в него входят?
20. Какие методы многофакторной аутентификации применяются в современных системах?
21. Что такое Threat Intelligence и какие уровни зрелости разведданных существуют?
22. Как работает песочница для анализа вредоносного ПО и какие методы анализа применяются?
23. Какие этапы включает процесс цифровой криминалистики?
24. Что такое DevSecOps и как безопасность интегрируется в процесс разработки?
25. Какие инструменты используются для безопасной разработки?
26. Что такое технологии обмана (honeypots, honeynets, decoys) и как они используются для выявления атак?
27. Чем honeypot отличается от honeynet и какие типы ловушек существуют?
28. Как организуется управление политиками безопасности в организации и какие инструменты для этого используются?
29. Как автоматизируется контроль соответствия нормативным требованиям?