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

Паспорт экзамена

по дисциплине «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей», 9 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 16-30.

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 «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей»

---

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 «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей»

1. Что такое мониторинг информационной безопасности и какие цели он преследует в организации?
2. Чем мониторинг информационной безопасности отличается от аудита и тестирования на проникновение?
3. Какие нормативно-правовые акты регулируют мониторинг информационной безопасности в Российской Федерации?
4. Что такое событие безопасности и инцидент информационной безопасности? В чём разница?
5. Что такое журнал событий, источник событий и поток телеметрии?
6. Что такое агрегация и нормализация журналов событий и зачем они нужны?
7. Какие основные классы средств мониторинга ИБ существуют?
8. Как выбираются средства мониторинга под задачи организации?
9. Какие источники событий наиболее важны для мониторинга Windows-систем?
10. Какие источники событий и инструменты используются для мониторинга Linux-систем?
11. Какие методы сетевого анализа трафика применяются для обнаружения угроз?

12. Чем системы обнаружения вторжений нового поколения (NGIDS/NGFW) отличаются от традиционных IDS?
13. Что такое фреймворк MITRE ATT&CK и как он используется для проектирования правил мониторинга?
14. Как с помощью MITRE ATT&CK выявляются сложные многоэтапные угрозы (APT)?
15. Какие компоненты входят в архитектуру современной системы мониторинга ИБ?
16. Какие архитектурные подходы используются при построении систем мониторинга?
17. Какие особенности имеет мониторинг промышленных сетей ICS/SCADA по сравнению с IT-сетями?
18. Какие источники Threat Intelligence используются и как они интегрируются в системы мониторинга?
19. Как индикаторы компрометации (IoC) и тактики, техники и процедуры (TTP) используются для улучшения детектирования?
20. Какие процессы мониторинга и первичного реагирования можно автоматизировать?
21. Как SOAR-платформы интегрируются с системами мониторинга для автоматизации реагирования?
22. Какие особенности имеет мониторинг безопасности в облачных средах?
23. Как организуется мониторинг в гибридных инфраструктурах, сочетающих on-premise и облачные компоненты?
24. Что такое инсайдерская угроза и какие методы мониторинга используются для её выявления?
25. Как работает поведенческий анализ и какие модели поведения он строит?
26. Какие базовые метрики используются для оценки эффективности SOC?
27. Как метрики SOC помогают улучшать процессы мониторинга и реагирования?
28. Какие модели зрелости SOC существуют и какие уровни они выделяют?
29. Зачем нужны базы знаний в системах мониторинга и что они содержат?
30. Как организуется управление знаниями в SOC для повышения эффективности аналитиков?