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

Паспорт зачета

по дисциплине «Расследование инцидентов информационной безопасности», 9 семестр

1. Методика оценки

Зачет 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 16-31.

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 «Расследование инцидентов информационной безопасности»

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 (тест) 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 (модулю) 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 (тест) 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 (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от* 14 *до* 17 *баллов.*

Ответ на билет (тест) 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 (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от* 10 *до* 13 *баллов.*

Ответ на билет (тест) 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 (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 10 *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 «**Расследование инцидентов информационной безопасности**»**

1. Что такое компьютерная форензика? Дайте определение и опишите основные цели.
2. Какие основные этапы включает процесс расследования инцидентов информационной безопасности?
3. Что такое цепочка custody (chain of custody) и почему она важна при расследовании?
4. Какие принципы лежат в основе проведения расследования инцидентов?
5. Какие нормативно-правовые акты регулируют расследование инцидентов ИБ в Российской Федерации?
6. Какие организационные меры необходимо принять до начала расследования инцидента?
7. Что такое инцидент информационной безопасности и чем он отличается от события безопасности?
8. Какие действия необходимо предпринять сразу после обнаружения инцидента?
9. Как правильно изолировать систему, не уничтожив при этом доказательства?
10. Почему анализ оперативной памяти важен при расследовании инцидентов?
11. Какую информацию можно извлечь из дампа оперативной памяти?
12. Что такое артефакты и как они помогают в расследовании?
13. Какие методы создания копии дискового носителя вы знаете?
14. Что такое хеширование и зачем оно используется при работе с дисковыми образами?
15. Что такое slack space, unallocated space и как они используются при расследовании?

16. Какие типы системных журналов существуют в операционных системах Windows и Linux?
17. Что такое Event Log в Windows и какие категории событий там регистрируются?
18. Как анализировать журналы syslog и journald в Linux?
19. Какие события в системных журналах наиболее важны при расследовании инцидентов?
20. Какие артефакты оставляют приложения в операционной системе?
21. Как определить, какие приложения были запущены на системе и когда?
22. Что такое prefetch-файлы в Windows и как они помогают в расследовании?
23. Как анализировать активность браузеров при расследовании?
24. Какие артефакты указывают на действия пользователя в системе?
25. Как определить время последнего входа пользователя и его активность?
26. Что такое LNK-файлы и как они помогают восстановить действия пользователя?
27. Как анализировать историю командной строки?
28. Какие признаки указывают на наличие вредоносного ПО в системе?
29. Как определить, какие изменения внесло вредоносное ПО?
30. Что такое статический и динамический анализ вредоносного ПО?
31. Как использовать песочницу (sandbox) для анализа поведения вредоносного ПО?