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

Паспорт экзамена

по дисциплине «**Безопасность и защита информации в информационных системах**»,

3 семестр

1. Методика оценки

Экзамен проводится в устной (письменной) форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов от 1 до 15-го, второй вопрос из диапазона вопросов 16-27 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «**Безопасность и защита информации в информационных системах**»

---

1. Вопрос 1
2. Вопрос 2.

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

2. Критерии оценки

- Ответ на билет (тест) для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *0 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, при решении задачи допускает непринципиальные ошибки, например, вычислительные,

оценка составляет *35 баллов.*

- Ответ на билет (тест) для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *40 баллов.*
- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет 45 *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 35 баллов (из 45 возможных).

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

4. **Вопросы к** экзамену **по дисциплине «Безопасность и защита информации в информационных системах»**

1. Понятие информационной безопасности.
2. Национальная безопасность.
3. Доктрина информационной безопасности Российской Федерации.
4. Национальные интересы РФ в информационной сфере и их обеспечение.
5. Виды угроз информационной безопасности РФ.
6. Источники угроз информационной безопасности РФ.
7. Информационные системы, классификация информационных систем. Причины, виды, каналы утечки информации.
8. Угрозы информационному обеспечению государственной политики РФ.
9. Методы и модели оценки угроз информации в информационных системах.
10. Причины, виды, каналы утечки информации.
11. Средства обеспечения безопасности информационных систем.
12. Методы обеспечения безопасности информационных систем. Технические средства защиты.
13. Правовая защита информационных систем.
14. Направления и цели защиты информации и их взаимосвязь.
15. Угрозы информации. Виды угроз.
16. Классификация угроз информационной безопасности. Классификация источников угроз информационной безопасности.
17. Концептуальная модель безопасности продукции.
18. Концептуальная модель безопасности личности.
19. Концептуальная модель безопасности информации.
20. Организационная защита.

21. Технологии противодействие атакам на сетевые сервисы. Отказ а обслуживании (DOS)
22. Физические средства защиты информации.
23. Политика безопасности предприятия.
24. Способы и технологии противодействие атакам на WEB - прилижение.
25. Оценка эффективности средств защиты информации (СЗИ).
26. Принцип осуществления атак типа BRUTEFORCE. Подбор пароля через SMTP протокол.
27. Способы получения полного контроля над целевой машиной .