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

Паспорт зачета

по дисциплине «Гуманитарные аспекты информационной безопасности», 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 1–18;
- второй вопрос выбирается из диапазона вопросов 19–36.

Таким образом, проверяются результаты обучения по дисциплине, соотнесённые 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 «Гуманитарные аспекты 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 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, не допускает ошибок. 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, не допускает существенных ошибок. 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* 14 *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, допускает непринципиальные ошибки. 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* 10 *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, допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине 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 «**Гуманитарные аспекты информационной безопасности**»**

1. Какую роль играет человеческий фактор в обеспечении информационной безопасности организации?
2. Каковы основные мотивы нарушения требований информационной безопасности персоналом? Как различаются умышленные и неумышленные нарушения?
3. Какие личностные качества и особенности поведения работников могут способствовать нарушениям информационной безопасности?
4. По каким признакам можно выявить низкую мотивацию персонала к соблюдению требований информационной безопасности?
5. Как связаны организация труда, мотивация работников и выполнение требований информационной безопасности?
6. Как проанализировать ситуационную задачу по психологии персонала, определить причины нарушения и обосновать меры предупреждения повторного нарушения?
7. Как обосновать действия должностного лица при нарушении работником требований защиты информации и какие меры в пределах его полномочий могут потребоваться для восстановления нарушенных прав?
8. Что понимается под социальным инжинирингом и какие психологические механизмы используются при воздействии на человека?
9. Каковы основные виды социального инжиниринга и по каким признакам можно различать соответствующие воздействия?
10. Как используются доверие, авторитет, срочность и эмоциональное давление при социальном инжиниринге?

11. Какие признаки сообщений и обращений помогают распознать попытку получения информации с помощью социального инжиниринга?
12. Как организовать проверку личности и полномочий обращающегося перед передачей информации или выполнением его просьбы?
13. Как разобрать ситуацию социального инжиниринга, определить уязвимости поведения персонала и предложить организационные меры защиты?
14. В чём заключается принцип разделения обязанностей и какие угрозы информационной безопасности он позволяет снижать?
15. Как выявить несовместимые функции и конфликт полномочий при распределении обязанностей работников?
16. В чём заключается принцип минимизации привилегий и как обосновывается необходимый объём прав доступа?
17. Как совместно применяются принципы разделения обязанностей и минимизации привилегий при изменении должностных функций работника?
18. Какие нормативные, руководящие и методические документы уполномоченных федеральных органов необходимо учитывать при распределении обязанностей и предоставлении доступа к информации ограниченного доступа?
19. Как документировать распределение полномочий и организовать проверку соблюдения принципов разделения обязанностей и минимизации привилегий?
20. Что характеризует зрелость процессов обеспечения информационной безопасности и в чём назначение модели Information Security Maturity Model?
21. Какие уровни зрелости выделяются в изученной модели Information Security Maturity Model и по каким признакам они различаются?
22. Какие сведения и свидетельства необходимы для определения уровня зрелости процессов обеспечения информационной безопасности организации?
23. Как выявить недостатки процессов обеспечения информационной безопасности и определить условия перехода на следующий уровень зрелости?
24. Как результаты анализа и оценки угроз информационной безопасности объекта информатизации используются при выборе мероприятий по повышению зрелости процессов?
25. Как учитывать нормативные документы в области технической и криптографической защиты информации при оценке состояния процессов и планировании повышения их зрелости?
26. Каковы цель, задачи и основные элементы программы повышения осведомлённости персонала в области информационной безопасности?
27. Как определить целевые группы программы повышения осведомлённости и учесть их должностные обязанности и характер работы с информацией?
28. Как выбрать содержание и формы мероприятий по повышению осведомлённости персонала с учётом характерных угроз и нарушений?
29. Какие организационные условия необходимы для успешной реализации программы повышения осведомлённости персонала?
30. Как оценить результативность программы повышения осведомлённости и использовать результаты оценки для её улучшения?
31. Как согласовать программу повышения осведомлённости с политиками информационной безопасности и довести требования до работников?

32. Каковы назначение, структура и требования к стилю изложения политики информационной безопасности?
33. Чем отличаются документы типов «требования» и «процедура» и как обеспечить согласованность между ними?
34. Как разработать и документировать политику информационной безопасности типа «требования» по одному из направлений ГОСТ 27002?
35. Как при разработке политики информационной безопасности учесть законодательство Российской Федерации, нормативные правовые акты, нормативные и методические документы в области защиты информации?
36. Как разработать процедуру реализации требований политики по одному из направлений ГОСТ 27002, определить исполнителей, порядок действий и способы продвижения политики среди персонала?