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

Паспорт зачета

по дисциплине «Информационная безопасность в корпоративной сфере. Продвинутый уровень (для продолжающих)», 1 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 перечня вопросов 1–18, 20–21, 23, 27, 30, 33–36;
- второй вопрос выбирается из перечня вопросов 19, 22, 24–26, 28–29, 31–32.

Таким образом, проверяются результаты обучения по индикаторам ПК-3.В/ПР.3 и УК-4.3. Отвечая на первый вопрос, студент называет средства автоматизации проектирования защиты корпоративной инфраструктуры и обосновывает результат их применения. Отвечая на второй вопрос, студент указывает информационно-коммуникативные средства, участников и порядок обмена сведениями в рассматриваемом процессе профессионального взаимодействия.

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

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЭН

Билет № _____
к зачету по дисциплине «Информационная безопасность в корпоративной сфере. Продвинутый уровень (для продолжающих)»

1. Вопрос из перечня 1–18, 20–21, 23, 27, 30, 33–36.
2. Вопрос из перечня 19, 22, 24–26, 28–29, 31–32.

Утверждаю: зав. кафедрой ____ доцент, к.т.н. Иванов А. В.
(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, например, вычислительные. 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 за два вопроса билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине. Каждый вопрос оценивается в пределах 0–10 баллов; итоговая оценка равна сумме баллов за оба вопроса.

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 «Информационная безопасность в корпоративной сфере. Продвинутый уровень (для продолжающих)»

1. Понятие информационной системы и основания классификации информационных систем. Как назначение системы, состав обрабатываемой информации и условия эксплуатации влияют на задачи её защиты?

2. Государственные и муниципальные информационные системы, информационные системы персональных данных, автоматизированные системы управления производственными и технологическими процессами, объекты критической информационной инфраструктуры: особенности и основания отнесения к соответствующему виду. Почему эти признаки нельзя считать взаимоисключающими?

3. Правовые, нормативные и методические документы, национальные стандарты в области защиты информации: назначение и особенности применения. Как определить, какие документы относятся к конкретной корпоративной информационной системе?

4. Как сформировать перечень источников требований по защите информации для предприятия профильной отрасли своего региона? Сопоставьте официальный нормативный документ, методические рекомендации и публикацию поставщика: как проверить актуальность, область применения и обоснованность содержащихся в них требований?

5. Определение класса защищённости государственных и муниципальных информационных систем: назначение процедуры, необходимые исходные сведения и оформление результата. Как выбор применимого нормативного источника влияет на обоснованность классификации?

6. Определение класса защищённости автоматизированной системы управления производственными и технологическими процессами. Какие сведения о предприятии, технологическом процессе и возможных последствиях нарушения его работы необходимы для принятия решения?

7. Определение уровня защищённости персональных данных при их обработке в информационной системе. Какие характеристики системы и обработки данных необходимо установить и как обосновать принятое решение?

8. Определение категории значимости объекта критической информационной инфраструктуры: последовательность действий, исходные сведения и документирование решения. На примере предприятия профильной отрасли своего региона объясните, как выявить недостаток исходных данных и проверить обоснованность вывода о категории.

9. Цели моделирования угроз безопасности информации и место модели угроз в системе защиты организации. Какие исходные сведения об информационной системе, защищаемой информации и условиях эксплуатации необходимо собрать?

10. Основные процедуры моделирования угроз по Методике оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 года. Как связаны возможные негативные последствия, объекты воздействия, источники угроз и способы реализации угроз?

11. Определение актуальных угроз безопасности информации и описание сценариев их реализации. Какие сведения позволяют обосновать включение угрозы в модель или её исключение и в каких случаях модель необходимо пересматривать?

12. Разработка фрагмента модели угроз для корпоративной системы предприятия профильной отрасли своего региона. Сопоставьте сведения из методического документа, технической документации системы и описания инцидента; предложите и обоснуйте варианты противодействия выявленной угрозе.

13. Требования по защите информации, устанавливаемые регуляторами. Как связаны вид информационной системы, её класс или уровень защищённости, категория значимости и состав применимых требований?

14. Требования ФСТЭК России к защите информации: выбор применимых требований и формирование комплекса организационных и технических мер. Как учитывать результаты моделирования угроз при обосновании выбранных мер?

15. Требования ФСБ России в отношении применения средств криптографической защиты информации. Какие исходные условия необходимо установить для определения применимых требований и почему использование криптографии не заменяет остальные меры защиты?

16. Обоснование мер защиты для корпоративной информационной системы предприятия профильной отрасли своего региона. Как сопоставить нормативные требования, модель угроз и технические ограничения, разработать варианты реализации и проверить, что выбранный вариант не подменяет обязательные требования рекомендациями поставщика?

17. Средства защиты информации от несанкционированного доступа, межсетевые экраны, системы обнаружения и предотвращения вторжений: назначение, основные принципы действия и различия. Какие задачи защиты они решают и почему не являются взаимозаменяемыми?

18. Антивирусные средства защиты, решения классов EDR и XDR, сканеры уязвимостей: назначение, принципы работы и ограничения. Чем различаются обнаружение вредоносной активности, реагирование на неё и выявление уязвимостей?

19. Средства криптографической защиты информации и электронные подписи в корпоративном обмене данными. Какие задачи решают шифрование и электронная подпись? Обоснуйте их применение для защиты канала связи и проверки электронного документа, не смешивая конфиденциальность и подтверждение подлинности.

20. Выбор комплекса базовых средств защиты для предприятия профильной отрасли своего региона. Сравните два варианта сочетания средств защиты рабочих станций, серверов и сетевых соединений по покрытию угроз, совместимости и ресурсам сопровождения; укажите, какими источниками следует проверить заявленные возможности.

21. Песочницы (sandbox) и системы предотвращения утечек конфиденциальной информации (DLP): назначение, принципы функционирования и ограничения. В каких корпоративных сценариях они применяются и как различаются результаты их работы?

22. SIEM, UBA и UEBA: назначение, используемые данные и принципы выявления подозрительной активности. Как сопоставить их возможности и ограничения при выборе средств анализа событий корпоративной инфраструктуры?

23. Системы классов IRP и SOAR: задачи управления реагированием и автоматизации. Разработайте вариант их применения при обработке корпоративного инцидента и обоснуйте, какие действия можно автоматизировать, а какие требуют проверки специалистом.

24. Системы Threat Intelligence: назначение и применение сведений об угрозах в корпоративной защите. Как сравнить два источника по достоверности, актуальности и применимости к предприятию, проверить противоречивые сведения и выбрать вариант их использования?

25. Реактивная и проактивная информационная безопасность: различия целей и подходов. Как сочетать их при организации мониторинга безопасности предприятия и какими примерами можно показать ограничения каждого подхода?

26. Центр мониторинга информационной безопасности (SOC): назначение, основные задачи и организация взаимодействия специалистов. Как связать выявление события, его проверку, эскалацию и передачу на реагирование?

27. Построение и сопровождение процесса мониторинга информационной безопасности организации. Как определить источники событий, организовать сбор и анализ данных, проверять качество выявления угроз и корректировать настройки мониторинга?

28. Сравнение собственного, внешнего и смешанного вариантов организации мониторинга безопасности для предприятия профильной отрасли своего региона. Какие технические и организационные ограничения следует учесть и какие сведения необходимо проверить, прежде чем обосновывать выбранный вариант?

29. Threat Intelligence как процесс информационной безопасности: цели, задачи, основные действия и использование результатов. Как организовать получение, проверку и применение сведений об угрозах с учётом потребностей предприятия?

30. Threat Hunting: цели и отличие от обработки готовых срабатываний средств защиты. Сформулируйте гипотезу поиска скрытой угрозы в корпоративной инфраструктуре, определите необходимые данные и объясните, как оценить результаты проверки.

31. Управление уязвимостями: выявление, проверка, приоритизация, устранение и контроль результата. Как выбрать последовательность действий на предприятии профильной отрасли своего региона при ограниченных ресурсах и необходимости сохранять работоспособность систем?

32. Реагирование на инциденты информационной безопасности: цели, основные действия и взаимодействие участников. На примере подозрения на компрометацию корпоративной системы сопоставьте имеющиеся свидетельства, предложите варианты реагирования и обоснуйте выбор с учётом последствий для деятельности предприятия.

33. Защита периметра сети организации: типовые технические решения, решаемые задачи и ограничения. Как обосновать состав средств защиты внешних соединений с учётом структуры корпоративной инфраструктуры и актуальных угроз?

34. Защита внутри корпоративной сети: разделение сетевых сегментов, разграничение доступа и контроль взаимодействий. Как выбрать вариант защиты рабочих станций и серверов, чтобы ограничить распространение атаки внутри организации?

35. Согласование средств защиты периметра и внутренних сегментов корпоративной инфраструктуры. Как проверить полноту покрытия угроз, совместимость решений и возможность их совместного мониторинга, не сводя защиту к приобретению отдельных продуктов?

36. Разработка вариантов защиты типовой инфраструктуры предприятия профильной отрасли своего региона. Сравните два варианта по покрытию угроз, требованиям к ресурсам и влиянию на деятельность предприятия; укажите необходимые источники информации, проверьте исходные допущения и обоснуйте выбранное решение.