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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН
АВТФ к.т.н., доцент
И.Л. Рева
“___”_____г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Программно-аппаратное обеспечение информационной безопасности

Образовательная программа: 10.04.01 Информационная безопасность, профиль: Методы и средства обеспечения технической защиты информации

Новосибирск - 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

Промежуточная аттестация по **дисциплине** проводится во 2 семестре - в форме экзамена, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-2 и соотнесенных с ними индикаторов.

Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 2, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенции ОПК-2, закрепленных за дисциплиной.

2. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт экзамена

по дисциплине «Программно-аппаратное обеспечение информационной безопасности», 2 семестр

1. Методика оценки

Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание дисциплины «Аудит информационной безопасности».

Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на 5/6 вопросов теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов и не допускает ошибок при решении задач. 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 35 до 40 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления, не допускает существенных ошибок при решении задач. 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 27 до 34 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от 1/2 до 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач 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 20 до 26 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач 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 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.

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста[1]) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	1. владеет навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью 2. умеет разрабатывать тестовые планы и сценарии тестирования разработанного продукта 3. умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью

Вопросы теста для оценки сформированности компетенции ОПК-2

Вопрос 1. СДЗ платы расширения (АМДЗ) – это:

- **программно-аппаратное решение, встраивается в корпус компьютера, подключаясь к материнской**

плате через PCI-разъем ✓

- программное решение, которое встраивается в BIOS
- программное решение, которое заменяет загрузочную запись на жестком

(один вариант)

Вопрос 2. Опишите принцип фильтрации трафика «черный список»

Ответ:

Решение: разрешать все, что явно не запрещено

Вопрос 3. Из чего состоит архитектура EDR решений?

Ответ:

Решение: состоит из агентов и серверной части

Вопрос 4. Избирательный метод управления доступом предусматривает право владельца или администратора объекта определять и контролировать всех, кто имеет доступ к системе или ресурсам, основываясь на идентификационной информации о субъектах, допущенных к контролируемой системе – это определение:

- **Дискреционного контроля доступа ✓**

[1] Правильные ответы выделены галочкой

- мандатного контроля доступа
- контроля на основе правил

(один вариант)

Вопрос 5. Опишите принцип фильтрации трафика «белый список»

Ответ:

Решение: запрещать все, что явно не разрешено

Вопрос 6. Опишите вид сканирования сканера уязвимостей – белый ящик

Ответ:

Решение: известна вся информация о системе.

Вопрос 7. Система обнаружения вторжений – это:

- **программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет ✓**
- прибор, объединяющий несколько интеллектуальных устройств в локальную сеть для обмена данными
- система защиты информации от несанкционированного доступа в процессе её хранения и обработки

(один вариант)

Вопрос 8. Опишите особенности межсетевого экрана типа «B»

Ответ:

Решение: хостовые МСЭ

Вопрос 9. Опишите вид сканирования сканера уязвимостей – черный ящик

Ответ:

Решение: неизвестна информация о системе

Вопрос 10. Система предотвращения вторжений – это:

- **программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них ✓**
- специализированное устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации
- класс устройств для объединения компьютеров в сетях Ethernet с применением кабельной инфраструктуры типа витая пара

(один вариант)

Вопрос 11. Опишите особенности межсетевого экрана типа «A»

Ответ:

Решение: сетевые МСЭ

Вопрос 12. Опишите вид сканирования сканера уязвимостей – серый ящик

Ответ:

Решение: известна частичная информацию о системе

Вопрос 13. Средства шифрования – это:

- **аппаратные, программные и программно-аппаратные криптографические СЗИ (например, криптошлюзы и шлюзы безопасности), которые реализуют алгоритмы шифрования информации для ее безопасной передачи по каналам связи, хранения и обработки ✓**
- средства, в которых некоторые криптографические преобразования выполняются вручную или специальными автоматизированными решениями
- средства, защищающие информацию от внесения изменений в исходные данные

(один вариант)

Вопрос 14. Дополните определение Аутентификация — это основа безопасности любой системы, которая заключается в проверке ___ ___ о пользователе сервером.

Ответ:

Решение: подлинности данных

Вопрос 15. Состав DLP состоит из

- **сетевых компонент, хостовых компонент (агентов), модуля централизованного управления (консоль администратора) ✓**
- только из хостовых компонент (агентов)
- сетевых компонент, хостовых компонент (агентов)

(один вариант)

Вопрос 16. Выберите, что входит в архитектуру SIEM систем

- Ядро нормализации
- Ядро корреляции
- Хранилище
- Коллекторы
- Транспорт
- **Все варианты верны ✓**

(один вариант)

Вопрос 17. Система сбора и корреляции событий ИБ, обеспечивающая анализ событий ИБ в реальном времени – это:

- **SIEM – система ✓**
- IDS – система
- IPS – система

(один вариант)

Вопрос 18. За что отвечает действие accept в правилах фильтрации межсетевого экрана?

Ответ:

Решение: разрешение на прохождение трафика.

Вопрос 19. Дополните. Метод работы сигнатурных IDS/IPS позволяет детектировать ___ ____ атак

Ответ:

Решение: известные способы

Вопрос 20. Дополните. Метод работы IDS/IPS, работающих по аномалиям позволяет детектировать ____ ____атаки

Ответ:

Решение: ранее неизвестные

Вопрос 21. Приведите один из примеров идентификации.

Ответ:

Решение: логин, электронная почта, номер телефона

Вопрос 22. Что такое антивирусная программа?

- **специальное программное обеспечение для обнаружения вредоносного программного обеспечения и восстановления файлов, модифицированных вредоносным программным обеспечением, а также очистка СВТ от вредоносного программного обеспечения ✓**
- специальное программное обеспечение для обнаружения вредоносного программного обеспечения
- специальное программное обеспечение для обнаружения вредоносной сетевой активности

(один вариант)

Вопрос 23. За что отвечает действие reject в правилах фильтрации межсетевого экрана?

Ответ:

Решение: Запрет на прохождение трафика

Вопрос 24. Место установки СПВ (IDS)

Ответ:

Решение: на границе сети

Вопрос 25. За что отвечает действие drop в правилах фильтрации межсетевого экрана?

Ответ:

Решение: Запрет на прохождение трафика

Вопрос 26. Место установки СОВ (IDS)

Ответ:

Решение: на границе сети

Вопрос 27. Межсетевой экран (Брандмауэр, firewall) – это…

- Комплекс аппаратных средств
- Комплекс программных средств
- **Комплекс аппаратных или программных средств ✓**

(один вариант)

Вопрос 28. Дополните определение идентификации. Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его _____, однозначно определяющий этого субъекта в информационной системе.

Ответ:

Решение: идентификатор

Вопрос 29. Приведите один из примеров аутентификации.

Ответ:

Решение: пароль, пин-код, секретное слово

Вопрос 30. К видам системы обнаружения атак относятся:

- системы, обнаружения атаки на ОС
- системы, обнаружения атаки на конкретные приложения
- системы, обнаружения атаки на удаленных БД
- **все варианты верны✓**

(один вариант)