Контрольно-оценочные средства для проведения текущего контроля
по МДК.07.02 Сертификация информационных систем
(4 курс, 7 семестр 2023-2024 уч. г.)

Текущий контроль №1

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Письменный опрос
Задание №1

Назовите типы резервного копирования и дайте их краткое описание.

Оценка	Показатели оценки
3	Названы все типы резервного копирования. (например, 1.обычное; 2.копирующее; 3.добавочное; 4.разностное; 5. ежедневное).
4	Названы все типы резервного копирования. (например, 1.обычное; 2.копирующее; 3.добавочное; 4.разностное; 5. ежедневное). Дано описание 1,2,3 типа.

5	Названы все типы резервного копирования. (например, 1.обычное; 2.копирующее; 3.добавочное; 4.разностное; 5. ежедневное). Дано описание всем типам резервного копирования.

Задание №2

Дайте определения:

1. Политика безопасности

2. Резервное копирование

3. Восстановление

4. Журнал транзакций

Оценка	Показатели оценки
3	Даны определения 2 терминам.
4	Даны определения 3 терминам
5	Даны определения всем терминам.

Текущий контроль №2

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Письменный опрос
Задание №1

1. Дать определения "брандмауэр", "система контроля действий пользователя".

2. Перечислить основные опасности, существующие в сети.

Оценка	Показатели оценки
3	Выполнено 1 пункт задания.

4	Даны определения, но перечислены не все опасности, существующие в сети.
5	Выполнены и представлены в полном объеме 2 пункта задания.

Задание №2

1. Перечислить классификации брандмауэров.

2. Назвать и дать краткое пояснение всем уровням, на которых функционируют брандмауэры.

Оценка	Показатели оценки
3	Выполнен 1 пункт задания.
4	Перечислены все классификации. Названы уровни, на которых функционируют брандмауэры, но не дано пояснение.
5	2 пункта задания представлены в полном объеме.

Задание №3

Назвать функции персонального брандмауэра.

Оценка	Показатели оценки

3	Названы 3-4 функции из: • Блокировка внешних атак В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр. • Блокировка утечки информации Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть. • Контроль приложений Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Проверка аутентичности приложения. • Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. Необходим дифференцируемый подход к анализу опасности того или иного содержания. • Протоколирование и предупреждение Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются. • Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (wizards) по настройке и прочих буржуйских штучек, даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

4	Названы 5 функций из: • Блокировка внешних атак В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр. • Блокировка утечки информации Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть. • Контроль приложений Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Проверка аутентичности приложения. • Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. Необходим дифференцируемый подход к анализу опасности того или иного содержания. • Протоколирование и предупреждение Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются. • Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (wizards) по настройке и прочих буржуйских штучек, даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

5	Названы все функции: • Блокировка внешних атак В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр. • Блокировка утечки информации Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть. • Контроль приложений Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Проверка аутентичности приложения. • Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. Необходим дифференцируемый подход к анализу опасности того или иного содержания. • Протоколирование и предупреждение Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются. • Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (wizards) по настройке и прочих буржуйских штучек, даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

Текущий контроль №3

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Письменный опрос
Задание №1

Дать определения:

1. сертификат безопасности

2. качество программного продукта

3. сертификация

4. система сертификации

5. сертификат разработчика

Оценка	Показатели оценки
3	Даны определения 3 терминам
4	Даны определения 4 терминам
5	Даны определения всем терминам

Задание №2

Назвать:

1. виды

2. функции

3. срок дествия

(сертификата соответствия)

Оценка	Показатели оценки
3	Назван 1 пункт задания
4	Названы 2 пункта задания
5	названы все пункты задания

Задание №3

Назвать и дать краткое описание критериям качества программного продукта.

Оценка	Показатели оценки
3	Названы все критерии качества ПП (-функциональность; - надежность; - легкость применения; - эффективность; - сопровождаемость; - мобильность) Не представлено описание критериев.

4	Названы все критерии качества ПП (-функциональность; - надежность; - легкость применения; - эффективность; - сопровождаемость; - мобильность) Описание дано к 4 критериям.
5	Названы все критерии качества ПП (-функциональность; - надежность; - легкость применения; - эффективность; - сопровождаемость; - мобильность) Представлено описание всех критериев

Задание №4

Назовите этапы процесса сертификации программного обеспечения

Оценка	Показатели оценки

3	Названы 5 этапов (1 подачу заявки на сертификацию; 2 принятие решения по заявке на сертификацию, в том числе назначение экспертов на проведение основных работ по сертификации из числа экспертов органа по сертификации; 3 оформление договора на проведение работ по сертификации; 4 проведение сертификационной проверки ПО, в том числе при необходимости проведение испытаний/контроля ПО по согласованным с заказчиком методикам; 5 принятие решения о выдаче Сертификата соответствия и разрешения использования знака соответствия либо об отказе в выдаче Сертификата соответствия; 6 выдача Сертификата соответствия и разрешения использования знака соответствия; 7 занесение заявителя/изготовителя ПО и перечня сертифицированных ПО в Реестр СДС ПО; 8 проведение инспекционного контроля сертифицированных ПО.)
4	Названы 6-7 этапов (1 подачу заявки на сертификацию; 2 принятие решения по заявке на сертификацию, в том числе назначение экспертов на проведение основных работ по сертификации из числа экспертов органа по сертификации; 3 оформление договора на проведение работ по сертификации; 4 проведение сертификационной проверки ПО, в том числе при необходимости проведение испытаний/контроля ПО по согласованным с заказчиком методикам; 5 принятие решения о выдаче Сертификата соответствия и разрешения использования знака соответствия либо об отказе в выдаче Сертификата соответствия; 6 выдача Сертификата соответствия и разрешения использования знака соответствия; 7 занесение заявителя/изготовителя ПО и перечня сертифицированных ПО в Реестр СДС ПО; 8 проведение инспекционного контроля сертифицированных ПО.)

5	Названы все этапы (1 подачу заявки на сертификацию; 2 принятие решения по заявке на сертификацию, в том числе назначение экспертов на проведение основных работ по сертификации из числа экспертов органа по сертификации; 3 оформление договора на проведение работ по сертификации; 4 проведение сертификационной проверки ПО, в том числе при необходимости проведение испытаний/контроля ПО по согласованным с заказчиком методикам; 5 принятие решения о выдаче Сертификата соответствия и разрешения использования знака соответствия либо об отказе в выдаче Сертификата соответствия; 6 выдача Сертификата соответствия и разрешения использования знака соответствия; 7 занесение заявителя/изготовителя ПО и перечня сертифицированных ПО в Реестр СДС ПО; 8 проведение инспекционного контроля сертифицированных ПО.)

Задание №5

Назовите виды и категории стандартов.

Оценка	Показатели оценки

3	Названы только виды или категории стандартов (виды стандартов: - *основополагающие стандарты* (организационно-технические и общетехнические) (содержат общие и руководящие положения для определенной области) *- стандарты на продукцию (услуги),* *- стандарты на работы (процессы),* *- стандарты на методы контроля (испытаний, измерений).* категории стандартов: *- государственные стандарты (ГОСТ),* *- стандарты отраслей (ОСТ),* *- стандарты предприятий (СТП),* *- стандарты научно-технических, инженерных и других общественных организаций (СТО).)*
4	Названы не все виды и категории стандартов (виды стандартов: - *основополагающие стандарты* (организационно-технические и общетехнические) (содержат общие и руководящие положения для определенной области) *- стандарты на продукцию (услуги),* *- стандарты на работы (процессы),* *- стандарты на методы контроля (испытаний, измерений).* категории стандартов: *- государственные стандарты (ГОСТ),* *- стандарты отраслей (ОСТ),* *- стандарты предприятий (СТП),* *- стандарты научно-технических, инженерных и других общественных организаций (СТО).)*

5	Названы все виды и категории стандартов (виды стандартов: - *основополагающие стандарты* (организационно-технические и общетехнические) (содержат общие и руководящие положения для определенной области) - *стандарты на продукцию (услуги),* - *стандарты на работы (процессы),* - *стандарты на методы контроля (испытаний, измерений).* категории стандартов: - *государственные стандарты (ГОСТ),* - *стандарты отраслей (ОСТ),* - *стандарты предприятий (СТП),* - *стандарты научно-технических, инженерных и других общественных организаций (СТО).)*