Контрольно-оценочные средства для проведения текущего контроля
по ОП.19 Безопасность информационных систем
(3 курс, 5 семестр 2025-2026 уч. г.)

Текущий контроль №1 (45 минут)

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Проверочная работа
Задание №1 (19 минут)

Дать определение:

1. "Информационной безопасности",

2. "Защита информации",

3. "Доступность",

4. "Целостность информации",

5. "Конфиденциальность информации".

Оценка	Показатели оценки
5	Дано определение пяти понятиям.
4	Дано определение четырем понятиям.
3	Дано определение трем понятиям.

Задание №2 (26 минут)

1. Описать методы оценки уязвимости информации. Виды утечки информации.
2. Используя "Доктрину информационной безопасности РФ" описать уровни информационной безопасности РФ.
3. Дать определение : лицензия, лицензирующие органы (привести примеры), электронная цифровая подпись (открытая и закрытая).

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено 2 пункта задания.
3	Выполнен один пункт задания.

Текущий контроль №2 (45 минут)

Форма контроля: Письменный опрос (Опрос)

Описательная часть: Проверочная работа
Задание №1 (20 минут)

1. Дать определение "угроза", "окно опасности". Дать классификацию угроз.
2. Дать определение "вредоносное ПО", привести пример.
3. Дать определение "Основные угрозы целостности", привести пример.
4. Дать определение "Угроза конфиденциальности", привести пример.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Выполнено три пункта задания.
3	Выполнено два пункта задания.

Задание №2 (25 минут)

1. Понятие конфиденциальной информации, классификация, степени конфиденциальности.
2. Описать жизненные циклы конфиденциальной информации.
3. Понятие "государственная тайна". Описать способы защиты государственной информации.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Текущий контроль №3 (45 минут)
Форма контроля: Письменный опрос (Опрос)
Описательная часть: Проверочная работа
Задание №1 (19 минут)

1. Дать определение - вирус. Описать классификация вирусов и способы заражения.
2. Дать определение - антивирус. Описать основные классы антивирусных программ.
3. Написать средства анализа защищенности сетевых протоколов и ОС. Перечислить требования к антивирусам.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №2 (26 минут)

1. Описать методы и системы защиты информации.
2. Написать виды доступа,уровни доступа. Дать определение - контроль доступа.

3. Описать основные методы и приемы защиты от несанкционированного доступа.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.
5	Выполнено три пункта задания.

Текущий контроль №4 (45 минут)

Форма контроля: Лабораторная работа (Опрос)
Описательная часть:
Задание №1 (15 минут)

Расписать виды угроз и атак, характерные для сферы электронной коммерции. Меры предотвращения угроз и атак, такие как

использование антивирусного ПО, шифрование данных, контроль доступа. Меры реагирования на инциденты

информационной безопасности, такие как обнаружение и блокировка атак, восстановление системы после атак.

Оценка	Показатели оценки
5	Задание выполнено полностью.
4	Задание выполнено с незначительными ошибками.
3	Задание выполнено с грубыми ошибками.

Задание №2 (30 минут)

Разработайте систему контроля доступа для гипотетической компании, занимающейся разработкой программного обеспечения. Система должна включать в себя различные уровни доступа для сотрудников, клиентов и внешних подрядчиков, а также механизмы аутентификации и авторизации. Для каждого уровня доступа определите набор прав и возможностей, доступных пользователю. Например, сотрудники отдела разработки могут иметь право на чтение и изменение исходного кода проектов, а клиенты — только на просмотр демонстраций продуктов.

Разработайте механизмы контроля доступа, которые будут проверять соответствие прав пользователя его текущему

уровню доступа. Опишите, как система будет реагировать на попытки несанкционированного доступа.

Представьте свою систему в виде диаграммы или схемы, отражающей уровни доступа, механизмы аутентификации и авторизации, а также принципы контроля доступа.

Оценка	Показатели оценки

5	Определены пять уровней доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень и уровень аудита.Механизмы аутентификации и авторизации разработаны для каждого уровня доступа с учетом специфики выполняемых задач.Права и возможности для каждого уровня доступа четко определены, обоснованы и соответствуют должностным обязанностям.Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа, а также механизмы аудита действий пользователей.
4	Определены четыре уровня доступа для сотрудников, клиентов и внешних подрядчиков, включая административный уровень. Для каждого уровня доступа разработаны подробные механизмы аутентификации и авторизации. Права и возможности для каждого уровня доступа четко определены и обоснованы. Принципы контроля доступа описаны подробно и включают меры реагирования на попытки несанкционированного доступа.
3	Определены три уровня доступа для сотрудников, клиентов и внешних подрядчиков. Описаны механизмы аутентификации и авторизации для каждого уровня доступа. Указаны права и возможности для каждого уровня доступа. Описаны принципы контроля доступа.

Текущий контроль №5 (45 минут)

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Проверочная работа
Задание №1 (20 минут)

1. Описать проблемы безопасности IP-сетей.
2. Описать угрозы и уязвимости проводных корпоративных сетей.Описать угрозы и уязвимости беспроводных сетей.
3. Пояснить и описать технологии межсетевых экранов. Перечислить показатели защищенности межсетевых экранов.

Оценка	Показатели оценки
5	Выполнено три пункта задания.
4	Выполнено два пункта задания.
3	Выполнен один пункт задания.

Задание №2 (25 минут)

1. Дать определение - "политика безопасности ", "сетевая политика безопасности ".
2. Перечислить классификация систем обнаружения атак.
3. Описать компоненты и архитектура системы обнаружения атак.

Оценка	Показатели оценки
3	Выполнен один пункт задания.
4	Выполнено два пункта задания.

5	Выполнено три пункта задания.