МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Краснодонский факультет инженерии и менеджмента (филиал)
Кафедра информационных технологий и транспорта

УТВЕРЖДАЮ:
Директор
_____ Панайотов К.К.
(подпись)
«14» марта 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Управление информационной безопасностью
(наименование учебной дисциплины, практики)
09.04.01 Информатика и вычислительная техника
(код и наименование направления подготовки (специальности))
«Интеллектуальные системы
в производственно-транспортных комплексах»
наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик(разработчики):
доцент _____ Панайотов К. К.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры информационных технологий и транспорта от «26» февраля 2025 г., протокол № 7

Заведующий кафедрой
информационных
технологий и транспорта _____ Верительник Е. А.
(подпись)

Краснодон 2025

Комплект оценочных материалов по дисциплине
«Управление информационной безопасностью»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. *Выберите один правильный ответ.*

Как называется документ, в котором описываются процедуры и меры по управлению рисками информационной безопасности?

А) Стратегия развития компании.
Б) Техническое задание.
В) Политика конфиденциальности.
Г) Политика управления рисками.

Правильный ответ: Г

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

2. *Выберите один правильный ответ.*

Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

А) Комплексное обеспечение информационной безопасности.
Б) Комплексное обеспечение экономической безопасности.
В) Комплексное обеспечение национальной безопасности.
Г) Политика безопасности

Правильный ответ: А

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

3. *Выберите один правильный ответ.*

Уязвимость информации— это:

А) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

Б) Созможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

В) Сто действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

Правильный ответ: Б

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

4. *Выберите один правильный ответ.*

Полномочная политика безопасности подразумевает, что:

А) Каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Б) Все пользователи имеют одинаковый уровень доступа ко всем данным в системе.

В) Права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Правильный ответ: А

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Задания закрытого типа на установление соответствия

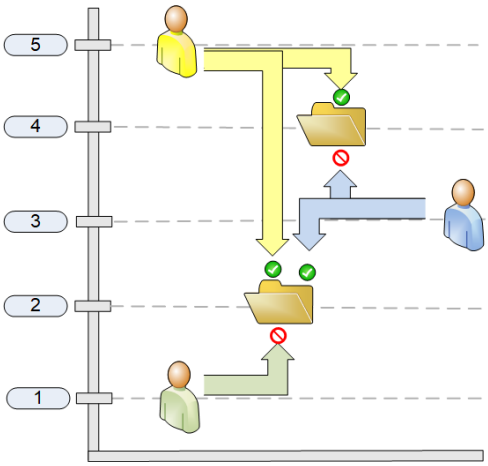
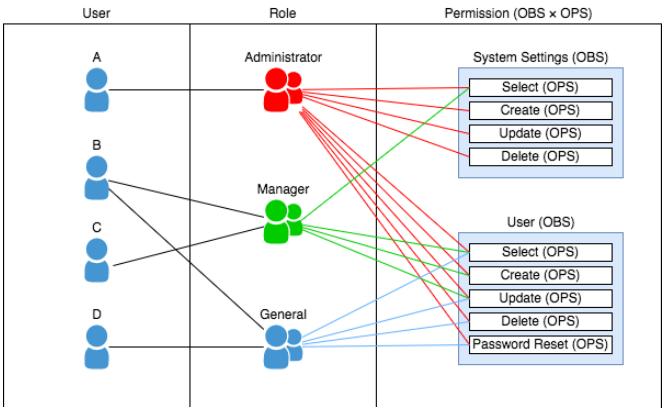
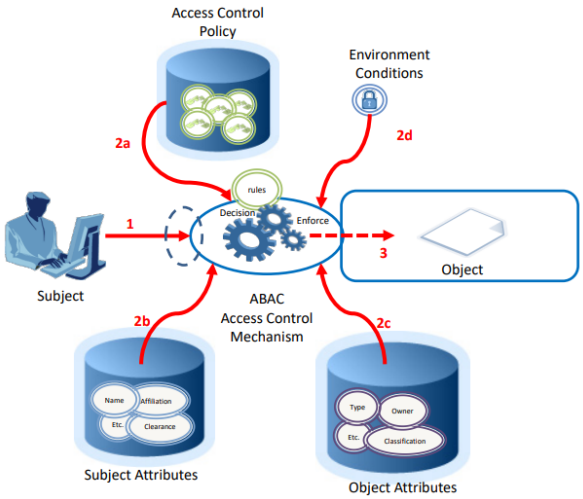
1. Прочитайте текст и установите соответствие между названием элемента в нотации CORAS и его визуальным отображением. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Название элемента в нотации CORAS		Визуальное отображение элемента в нотации CORAS
1) Пиктограмма "Уязвимость" в CORAS	А)	
2) Пиктограмма "Риск" в CORAS	Б)	
3) Пиктограмма "Противодействие угрозам" в CORAS	В)	
4) Пиктограмма "Инцидент" в CORAS	Г)	
5) Пиктограмма "Владелец информации" в CORAS	Д)	

Правильный ответ: 1-Б; 2-А; 3-В 4-Г 5-Д

Компетенции (индикаторы): ОПК-2 (ОПК-2.3)

2. Прочитайте текст и установите соответствие между визуальным представлением модели управления доступом и ее названием. Каждому элементу левого столбца соответствует только один элемент правого столбца.

	Визуальное представлением модели управления доступом	Название модели управления доступом
1)		А) мандатная модель управления
2)		Б) управление доступом на основе правил
3)		В) ролевая модель управления

Правильный ответ: 1-А; 2-В; 3-Б
Компетенции (индикаторы): ОПК-3 (ОПК-3.1))

3. Прочитайте текст и установите соответствие между названием информационной системы сферы информационной безопасности и ее назначением. Каждому элементу левого столбца соответствует только один элемент правого столбца.

	Название информационной системы сферы информационной безопасности		Назначение системы сферы информационной безопасности
1)	SIEM-системы	А)	программный продукт для предотвращения утечек конфиденциальных данных в корпоративной сети.
2)	DLS-система	Б)	решение, которое позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб бизнесу.
3)	IDS-система	В)	система, предназначенная для обнаружения и реагирования на несанкционированные действия и атаки в сети.

Правильный ответ: 1-А; 2-Б; 3-В.
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

4. Прочитайте текст и установите соответствие между содержанием средств и методов защиты информационной безопасности и их названием. Каждому элементу левого столбца соответствует только один элемент правого столбца.

	Содержание средств и методов защиты информационной безопасности		Название средств и методов защиты информационной безопасности
1)	средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.	А)	аппаратно-программные средства защиты
2)	электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы	Б)	аппаратные средства защиты

	или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками.		
3)	средства защиты с помощью преобразования информации (например, шифрования).	В)	криптографические средства защиты
4)	средства предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.	Г)	программные средства защиты
5)	предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.	Д)	физические средства защиты

Правильный ответ: 1-А; 2-Б; 3-В; 4-Г; 5-Д
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Задания закрытого типа на установление правильной последовательности

1. *Прочитайте текст и установите последовательность. Запишите правильную последовательность букв слева направо.*

Компания "CyberGuard" занимается предоставлением услуг по облачным вычислениям для различных клиентов, включая малый и средний бизнес. Недавно у одного из клиентов произошла утечка данных из облачного хранилища, что привело к потере доверия и репутации для компании "CyberGuard". Инцидент был связан с неправильной конфигурацией доступов и недостаточными мерами защиты данных. Идентифицированы основные риски информационной безопасности, с которыми столкнулась компания "CyberGuard". Расположите их в порядке приоритетности (от самой значимой к менее значимой).

А) Недостаточные меры шифрования данных.

Б) Отсутствие регулярного мониторинга и аудита безопасности.

В) Низкий уровень осведомленности клиентов о методах защиты данных.

Г) Неправильная конфигурация доступов к облачным хранилищам.

Правильный ответ: Г,А,Б,В

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

2. *Прочитайте текст и установите последовательность. Запишите правильную последовательность букв слева направо.*

Каковы правильные последовательные этапы управления информационной безопасностью? Укажите порядок следующих действий:

А) Оценка рисков.

Б) Идентификация активов.

В) Разработка политики безопасности.

Г) Контроль доступа.

Д) Мониторинг и аудит.

Е) Управление инцидентами.

Ж) Восстановление после инцидентов.

З) Технические меры защиты.

Правильный ответ: Б, А, В, Г, З, Д, Е, Ж

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

3. *Прочитайте текст и установите последовательность. Запишите правильную последовательность букв слева направо.*

Каковы правильные этапы процесса реагирования на инциденты информационной безопасности? Укажите порядок следующих действий:

А) Оценка инцидента.

Б) Документирование инцидента.

В) Реагирование на инцидент.

Г) Анализ причин инцидента.

Д) Восстановление после инцидента.

Е) Обновление политики и процедур.

Ж) Обнаружение инцидента.

Правильный ответ: Ж, А, В, Б, Г, Д, Е

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

4. *Прочитайте текст и установите последовательность. Запишите правильную последовательность букв слева направо.*

Каковы последовательные этапы управления рисками в области информационной безопасности? Укажите порядок следующих действий:

А) Оценка рисков.

Б) Идентификация рисков.

В) Внедрение мер по снижению рисков.

Г) Определение мер по снижению рисков.
Д) Мониторинг и пересмотр рисков.
Правильный ответ: Б ,А, Г, В, Д
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

5. *Прочитайте текст и установите последовательность. Запишите правильную последовательность букв слева направо*.
Каковы этапы создания и внедрения политики информационной безопасности? Укажите порядок следующих действий:
А) Разработка проекта политики.
Б) Анализ требований и стандартов.
В) Обсуждение и согласование политики.
Г) Обучение сотрудников.
Д) Регулярный пересмотр и обновление политики.
Е) Внедрение политики.
Правильный ответ: Б, А, В, Е, Г, Д
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Задания открытого типа

Задания открытого типа на дополнение

1. *Напишите пропущенное слово (с маленькой буквы).* Всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности — это _____информационной безопасности.
Правильный ответ: аудит.
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

2. *Напишите пропущенное слово (с маленькой буквы).* Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации — это _____информационной безопасности.
Правильный ответ: риск / риски.
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

3. *Напишите пропущенное слово (с маленькой буквы).* Процесс наблюдения, анализа и оценки систем и сетей на предмет возможных угроз, вредоносного кода, уязвимостей и нарушений политик безопасности — это _____информационной безопасности.
Правильный ответ: мониторинг.
Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Задания открытого типа с кратким свободным ответом

1. *Дайте ответ на вопрос (с маленькой буквы).* Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется _____.

Правильный ответ: политикой безопасности / политика безопасности.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

2. *Дайте ответ на вопрос (с маленькой буквы).* Система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности информации предприятия, называется _____.

Правильный ответ: служба безопасности / служба информационной безопасности / службой безопасности / службой информационной безопасности.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

3. *Дайте ответ на вопрос (с маленькой буквы).* Одиночная атаки, в котором мошенники нападают с целью вызвать перегрузку подсистемы сервиса, путём отправки максимального количества трафика жертве. _____. Правильный ответ: DoS-атака / Denial of Service / атака отказа в обслуживании.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

4. *Дайте ответ на вопрос (с маленькой буквы).* Какие права предоставлены к объекту (файлам или директориям) группе "все остальные" -rw-r--r-- в операционной системе Linux?

Правильный ответ: только чтение / чтение.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

5. *Дайте ответ на вопрос (с маленькой буквы).* Какие права предоставлены к объекту (файлам или директориям) группе "хозяина" -rw-r--r-- в операционной системе Linux?

Правильный ответ: чтение и запись / чтение, запись / чтение запись.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Задания открытого типа с развернутым ответом

1. Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.

Компания "ИнфоТек" занимается разработкой программного обеспечения и хранит конфиденциальные данные клиентов. В связи с увеличением числа кибератак и утечек данных, руководство компании решило провести оценку рисков в области информационной безопасности.

Данные:

Идентифицированные риски:

- Утечка данных из-за несанкционированного доступа:
  - Вероятность: 15%.
  - Потенциальные убытки: 2,000,000 рублей.
- Вирусная атака на серверы:
  - Вероятность: 10%.
  - Потенциальные убытки: 1,500,000 рублей.
- Потеря данных из-за сбоя оборудования:
  - Вероятность: 5%.
  - Потенциальные убытки: 1,000,000 рублей.

Формула для расчета ожидаемого убытка (E): $E=P \times L$

где:

- E — Ожидаемый убыток.
- P — Вероятность наступления риска.
- L — Потенциальные убытки.

Необходимо найти:

1. Рассчитайте ожидаемый убыток для каждого из идентифицированных рисков.
2. Определите общий ожидаемый убыток для компании "ИнфоТек" от всех рисков.

Привести расширенное решение. Время выполнения – 35 мин.

Ожидаемый результат:

1. Ожидаемый убыток от утечки данных:

$E1=0.15 \times 2,000,000=300,000$ рублей .

2. Ожидаемый убыток от вирусной атаки:

$E2=0.10 \times 1,500,000=150,000$ рублей.

3. Ожидаемый убыток от потери данных:

$E3=0.05 \times 1,000,000=50,000$ рублей.

4. Общий ожидаемый убыток:

$Eобщий=E1+E2+E3=300,000+150,000+50,000=500,000$ рублей.

Выводы: Общий ожидаемый убыток для компании "ИнфоТек" от всех идентифицированных рисков составляет 500,000 рублей.

Критерии оценивания: наличие в ответе правильного результата вычисления 500,000 рублей.

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

2. Прочитайте текст задания. Продумайте логику и полноту ответа. Запишите развернутый и обоснованный ответ.

Предположим, что ваша компания рассматривает возможность внедрения новой системы управления данными. Вам необходимо оценить риски, связанные с утечкой данных, и рассчитать потенциальные потери от этой утечки.

Данные для расчета:

Вероятность утечки данных (P): 5% (0,05)

Количество записей, которые могут быть утрачены в связи с утечками: 10 000 записей.

Средняя стоимость утечки одной записи: $150.

Оценка затрат на восстановление после утечки: $100 000.

Привести расширенное решение. Время выполнения – 35 мин.

Ожидаемый результат:

Потенциальные потери=Вероятность утечки×Количество записей×Стоимость одной записи.

Потенциальные потери=0,05×10 000×150=75 000 долларов.

Общие потери=Потенциальные потери+Затраты на восстановление.

Общие потери=75 000+100 000=175 000 долларов.

Выводы: 175 000 долларов.

Таким образом, общие потенциальные потери от утечки данных в вашей компании составляют $175,000. Это важная информация для принятия решения о внедрении системы управления данными и необходимости инвестиций в меры по повышению информационной безопасности.

Критерии оценивания: наличие в ответе правильного результата вычисления 175 000 долларов

Компетенции (индикаторы): ОПК-3 (ОПК-3.1)

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Управление информационной безопасностью» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 09.04.01 Информатика и вычислительная техника.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки обучающихся по указанному направлению 09.04.01 Информатика и вычислительная техника.

Председатель учебно-методической
комиссии Краснодонского факультета
инженерии и менеджмента (филиала) _____ Родионова О.Ю.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)