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

Институт управления и государственной службы
Кафедра производственного менеджмента

УТВЕРЖДАЮ:
Директор института управления и
государственной службы
_____Р.Г. Харьковский
(подпись)
«12» 02 2025 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
Информационная безопасность предприятия и технологии защиты информации
(наименование учебной дисциплины, практики)
38.04.02 «Менеджмент»
(код и наименование направления подготовки (специальности))
«**Управление организацией в цифровой экономике**»
(наименование профиля подготовки (специальности, магистерской программы); при отсутствии ставится прочерк)

Разработчик:
Доцент _____ Е.В. Щербакова
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры производственного менеджмента от «21» января 2025 г., протокол № 6

Заведующий кафедрой
производственного менеджмента _____ Родионов А.В.
(подпись)

Луганск 2025 г.

Комплект оценочных материалов по дисциплине
«Информационная безопасность предприятия и технологии защиты информации»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

Выберите один правильный ответ

1. Что является ключевым элементом системы формирования режима информационной безопасности?
А) Политика информационной безопасности
Б) Средства защиты информации
В) Управление доступом
Г) Резервное копирование данных
Д) Антивирусная защита
Правильный ответ: А
Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. Какая цель ставится перед системой формирования режима информационной безопасности?
А) Обеспечение конфиденциальности, целостности и доступности информации
Б) Повышение производительности информационных систем
В) Оптимизация затрат на защиту информации
Г) Увеличение количества пользователей
Д) Внедрение новых технологий
Правильный ответ: А
Компетенции (индикаторы): ПК-4 (ПК-4.1)

3. Какие угрозы являются основными для информационной безопасности?
А) Угрозы со стороны сотрудников компании
Б) Природные катастрофы
В) Утечка информации через социальные сети
Г) Атаки хакеров
Д. Все вышеперечисленные варианты
Правильный ответ: Д
Компетенции (индикаторы): ПК-4 (ПК-4.1)

4. Какой элемент не входит в систему формирования режима информационной безопасности?
А) Анализ рисков
Б) Разработка политики информационной безопасности
В) Обучение персонала

Г) Проведение аудита информационной безопасности
Д) Организация корпоративного отдыха
Правильный ответ: Д
Компетенции (индикаторы): ПК-4 (ПК-4.1)

5. Кто несет ответственность за соблюдение режима информационной безопасности в организации?
А) Руководитель службы информационной безопасности
Б) Сотрудники отдела кадров
В) ИТ-отдел
Г) Все сотрудники организации
Д) Аудиторы
Правильный ответ: Г
Компетенции (индикаторы): ПК-4 (ПК-4.1)

Выберите все правильные варианты ответов

6. Какие угрозы могут привести к утечке конфиденциальной информации предприятия? Выберите все подходящие ответы:
А) Внутренний злоумышленник
Б) Внешняя кибератака
В) Ошибка в программном обеспечении
Г) Неправильная настройка оборудования
Д) Несанкционированный доступ к данным
Е) Физическое проникновение в офис
И) Потеря устройства с данными
К) Использование нелицензионного ПО
Л) Социальная инженерия
М) Недостаточная подготовка сотрудников
Правильные ответы: А, Б, Д, И, Л, М
Компетенции (индикаторы): ПК-4 (ПК-4.1)

7. Какие меры могут предотвратить угрозу несанкционированного доступа к информационным ресурсам предприятия? Выберите все подходящие ответы:
А) Установка антивирусов
Б) Использование межсетевых экранов
В) Контроль физического доступа
Г) Регулярное обновление программного обеспечения
Д) Шифрование данных
Е) Ограничение прав доступа
И) Мониторинг сетевого трафика
К) Двухфакторная аутентификация
Л) Запрет использования личных устройств
М. Удаленное управление устройствами
Правильные ответы: Б, В, Е, К, Л

Компетенции (индикаторы): ПК-4 (ПК-4.1)

8. Какие типы угроз могут возникнуть при использовании облачных сервисов предприятием? Выберите все подходящие ответы:

А) Нарушение конфиденциальности данных
Б) Потеря контроля над данными
В) Риск отказа поставщика услуг
Г) Проблемы совместимости с локальными системами
Д) Недоступность сервиса
Е) Несоответствие требованиям законодательства
И) Низкая производительность
К) Отсутствие резервирования данных
Л) Кража учетных записей
М) Дефицит квалифицированных специалистов
Правильные ответы: А, Б, В, Д, Е, Л
Компетенции (индикаторы): ПК-4 (ПК-4.1)

9. Какие факторы могут способствовать возникновению внутренних угроз информационной безопасности предприятия? Выберите все подходящие ответы:

А) Ненадежные сотрудники
Б) Недостаточное обучение персонала
В) Низкий уровень мотивации сотрудников
Г) Несоблюдение правил информационной безопасности
Д) Отсутствие контроля за действиями сотрудников
Е) Использование устаревшего оборудования
И) Доступ к конфиденциальным данным без необходимости
К) Некорректная настройка политик безопасности
Л) Несвоевременное обновление программного обеспечения
М) Незащищенность от внешних атак
Правильные ответы: А, Б, Г, Д, И, К
Компетенции (индикаторы): ПК-4 (ПК-4.1)

10. Какие методы социальной инженерии могут использоваться для получения доступа к информации предприятия? Выберите все подходящие ответы:

А) Фишинг
Б) Телефонное мошенничество
В) Поддельные письма
Г) Взлом паролей
Д) Создание фальшивых сайтов
Е) Инсайдерская угроза
И) Перехват сообщений
К) Вредоносное ПО
Л) Сбор открытых данных
М) Шантаж

Правильные ответы: А, Б, В, Д, Л
Компетенции (индикаторы): ПК-4 (ПК-4.1)

Задания закрытого типа на установление соответствия

Установите правильное соответствие.
Каждому элементу левого столбца соответствует только один элемент правого столбца

1. Соотнесите название процессов механизма обеспечения информационной безопасности с их описанием.

Описание	Название процессов
1) Метод подтверждения личности пользователя с использованием двух или более факторов	А) Резервное копирование
2) Процесс записи всех действий, происходящих в системе, для последующего анализа	Б) Парольная политика
3) Механизм ограничения доступа к ресурсам системы на основе полномочий пользователя	В) Многофакторная аутентификация
4) Процесс создания копий важных данных для восстановления после сбоев или атак	Г) Логирование событий
5) Набор правил, определяющих требования к созданию и использованию паролей	Д) Контроль доступа

Правильный ответ: 1-В, 2-Г, 3-Д, 4-А, 5-Б
Компетенции (индикаторы): ПК-4 (ПК-4.1)

Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. Соотнесите название компонентов механизма обеспечения информационной безопасности с их описанием.

Описание	Название компонентов
1) Список разрешений, определяющий права доступа к файлам или другим ресурсам	А) ARP-сервер
2) Ложный сервер или система, используемая для привлечения и изучения атакующих	Б) WAF (Web Application Firewall)
3) Автоматизированный процесс поиска уязвимостей в системах и приложениях	В) Sandbox

4) Межсетевой экран для веб-приложений, фильтрующий HTTP-трафик	Г) Vulnerability scanner
5) Изоляция подозрительных файлов или приложений для безопасного тестирования	Д) Access Control List (ACL)

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

Компетенции (индикаторы): ПК-4 (ПК-4.1)

Задания закрытого типа на установление правильной последовательности

Установите правильную последовательность.

Запишите правильную последовательность букв слева направо.

1. Установите правильную последовательность этапов процесса внедрения системы информационной безопасности:

А) Оценка эффективности внедренных мер

Б) Идентификация активов и оценка рисков

В) Выбор и внедрение средств защиты

Г) Разработка политики информационной безопасности

Д) Обучение персонала

Правильный ответ: Б, Г, В, Д, А

Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. Установите правильную последовательность шагов при проведении аудита информационной безопасности:

А) Определение целей и задач аудита

Б) Анализ результатов и формирование отчета

В) Планирование аудита

Г) Сбор и анализ данных

Д) Представление отчета руководству

Правильный ответ: А, В, Г, Б, Д

Компетенции (индикаторы): ПК-4 (ПК-4.1)

3. Установите правильную последовательность действий при реагировании на инцидент информационной безопасности:

А) Устранение последствий инцидента

Б) Локализация инцидента

В) Выявление и идентификация инцидента

Г) Восстановление нормальной работы

Д) Анализ причин инцидента

Правильный ответ: В, Б, А, Д, Г

Компетенции (индикаторы): ПК-4 (ПК-4.1)

4. Установите правильную последовательность шагов при разработке политики информационной безопасности:

А) Реализация и внедрение политики

Б) Определение требований и стандартов

В) Утверждение политики руководством

Г) Разработка проекта политики

Д) Мониторинг и пересмотр политики

Правильный ответ: Б, Г, В, А, Д

Компетенции (индикаторы): ПК-4 (ПК-4.1)

5. Установите правильную последовательность стадий жизненного цикла управления рисками информационной безопасности:

А) Оценка остаточных рисков

Б) Идентификация рисков

В) Анализ рисков

Г) Выбор методов обработки рисков

Д) Мониторинг и пересмотр рисков

Правильный ответ: Б, В, Г, А, Д

Компетенции (индикаторы): ПК-4 (ПК-4.1)

Задания открытого типа

Задания открытого типа на дополнение

Напишите пропущенное слово (словосочетание).

1. _____ – это свойство информации, которое заключается в том, что она доступна только тем субъектам, которым разрешено её использовать.

Правильный ответ: Конфиденциальность

Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. _____ – это состояние информации, при котором она остается неизменной и точной, кроме случаев санкционированного изменения.

Правильный ответ: Целостность

Компетенции (индикаторы): ПК-4 (ПК-4.1)

3. _____ – это возможность субъектов получить доступ к необходимой им информации в нужное время.

Правильный ответ: Доступность

Компетенции (индикаторы): ПК-4 (ПК-4.1)

4. _____ – это документ, устанавливающий правила и процедуры для защиты информации в организации.

Правильный ответ: Политика информационной безопасности

Компетенции (индикаторы): ПК-4 (ПК-4.1)

5. _____ – это технические, программные и организационные меры, направленные на предотвращение несанкционированного доступа, уничтожения, модификации или раскрытия информации.

Правильный ответ: Средства защиты информации

Компетенции (индикаторы): ПК-4 (ПК-4.1)

6. _____ – это метод преобразования информации в такой вид, который может быть прочитан только теми, кто обладает соответствующим ключом.

Правильный ответ: Шифрование

Компетенции (индикаторы): ПК-4 (ПК-4.1)

7. _____ – это механизм, позволяющий контролировать доступ субъектов к объектам (информации, ресурсам).

Правильный ответ: Управление доступом

Компетенции (индикаторы): ПК-4 (ПК-4.1)

8. _____ – это программы, предназначенные для обнаружения, удаления и предотвращения распространения вирусов и другого вредоносного ПО.

Правильный ответ: Антивирусное ПО

Компетенции (индикаторы): ПК-4 (ПК-4.1)

9. _____ – это создание копий данных для их восстановления в случае потери или повреждения оригиналов.

Правильный ответ: Резервное копирование

Компетенции (индикаторы): ПК-4 (ПК-4.1)

10. _____ – это потенциальная возможность нанесения ущерба предприятию путем нарушения конфиденциальности, целостности или доступности информации.

Правильный ответ: Угроза информационной безопасности

Компетенции (индикаторы): ПК-4 (ПК-4.1)

11. _____ – это программное обеспечение, созданное для выполнения несанкционированных действий на компьютере или в сети, таких как кража данных, повреждение системы или нарушение ее работоспособности.

Правильный ответ: Вредоносное ПО

Компетенции (индикаторы): ПК-4 (ПК-4.1)

12. _____ – это методы манипуляции людьми с целью получения у них конфиденциальной информации или доступа к системам.

Правильный ответ: Социальная инженерия

Компетенции (индикаторы): ПК-4 (ПК-4.1)

13. _____ – это вид социальной инженерии, заключающийся в

отправке поддельных электронных писем или сообщений с целью заставить получателя раскрыть свои личные данные или установить вредоносное ПО.

Правильный ответ: Фишинг

Компетенции (индикаторы): ПК-4 (ПК-4.1)

14. _____ – это метод подтверждения личности пользователя, требующий предоставления двух или более различных типов доказательств, таких как пароль, биометрические данные или одноразовый код.

Правильный ответ: Многофакторная аутентификация (MEA)

Компетенции (индикаторы): ПК-4 (ПК-4.1)

15. _____ – это технология, создающая зашифрованное соединение между пользователем и сетью, обеспечивая безопасную передачу данных через Интернет.

Правильный ответ: VPN

Компетенции (индикаторы): ПК-4 (ПК-4.1)

Задания открытого типа с кратким свободным ответом

Дайте ответ на вопрос.

1. Каковы три основные цели, которые ставятся перед системой информационной безопасности предприятия?

Правильный ответ: Конфиденциальность, целостность, доступность.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. Приведите пример внутреннего злоумышленника в контексте информационной безопасности предприятия.

Правильный ответ: Сотрудник компании, имеющий легитимный доступ к информационным системам, но использующий этот доступ для совершения неправомерных действий.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

3. Опишите, что такое фишинг и как он может угрожать информационной безопасности предприятия.

Правильный ответ: Фишинг — это вид социальной инженерии, когда злоумышленники пытаются обманом получить у пользователей конфиденциальную информацию (логины, пароли, банковские данные). Это угрожает безопасности предприятия, так как может привести к краже данных, несанкционированному доступу к системам и финансовым потерям.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

4. Что означает термин "вредоносное ПО" и какие виды вредоносного ПО вы знаете?

Правильный ответ: Вредоносное ПО (malwarд) — это программное

обеспечение, разработанное для выполнения несанкционированных действий на компьютере или в сети. Примеры видов вредоносного ПО включают вирусы, черви, трояны, шпионское ПО, рекламное ПО и руткиты.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

5. Объясните, почему регулярное обновление программного обеспечения важно для обеспечения информационной безопасности предприятия.

Правильный ответ: Регулярные обновления программного обеспечения закрывают известные уязвимости, которые могут быть использованы злоумышленниками для атаки на информационные системы предприятия. Таким образом, своевременное обновление снижает риски взлома и утечек данных.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

6. Что такое многофакторная аутентификация и для чего она используется?

Правильный ответ: Многофакторная аутентификация — это метод подтверждения личности пользователя, требующий предоставления двух или более различных типов доказательств (например, пароль + SMS-код). Она используется для повышения уровня безопасности, усложняя задачу злоумышленникам для получения доступа к аккаунтам.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

7. Опишите, что такое межсетевой экран и какую роль он играет в защите информации.

Правильный ответ: Межсетевой экран — это устройство или программа, контролирующее входящий и исходящий трафик между сетями, позволяя пропускать только разрешенные соединения. Он защищает внутренние сети от несанкционированного доступа извне и помогает предотвратить утечку данных.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

8. Что такое шифрование данных и зачем оно применяется?

Правильный ответ: Шифрование данных — это процесс преобразования информации в такой вид, который может быть прочитан только теми, кто обладает соответствующим ключом. Оно применяется для защиты конфиденциальности данных, чтобы предотвратить их прочтение посторонними лицами даже в случае перехвата.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

9. Определите понятие «резервное копирование» и объясните его важность для обеспечения информационной безопасности.

Правильный ответ: Резервное копирование — это процесс создания копий важных данных для их восстановления после сбоев или атак. Оно критически важно для обеспечения сохранности информации и возможности быстрого восстановления в случае потери данных.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

10. Что такое аудит информационной безопасности и каковы его цели?

Правильный ответ: Аудит информационной безопасности — это систематический процесс оценки текущего состояния защиты информации в организации. Его цели включают выявление слабых мест в системе безопасности, проверку соблюдения установленных политик и процедур, а также разработку рекомендаций по улучшению защиты.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

Задания открытого типа с развернутым ответом

Дайте развернутый ответ на вопрос.

1. Опишите принципы и механизмы обеспечения конфиденциальности информации в информационных системах.

Время выполнения – 20 мин.

Ожидаемый результат:

Принципы обеспечения конфиденциальности информации включают:

1. Ограниченный доступ: Только уполномоченным пользователям предоставляется доступ к конфиденциальной информации.

2. Шифрование: Данные шифруются таким образом, чтобы они могли быть расшифрованы только теми, кому предоставлено право доступа.

3. Контроль доступа: Используются различные методы аутентификации и авторизации для ограничения доступа к информации.

4. Мониторинг и аудит: Осуществляется постоянный мониторинг и ведение журналов доступа к конфиденциальной информации для выявления нарушений.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

2. Объясните, каким образом обеспечивается целостность информации в информационных системах.

Время выполнения – 20 мин.

Ожидаемый результат:

Целостность информации подразумевает сохранение точности и полноты данных, а также отсутствие несанкционированных изменений. Для обеспечения целостности используются следующие подходы:

1. Контроль версий: Хранение истории изменений данных позволяет отслеживать и восстанавливать предыдущие версии.

2. Цифровые подписи: Использование криптографических методов для верификации источника и неизменности данных.

3. Хэш-функции: Применение хэширования для вычисления контрольных сумм, которые позволяют обнаружить любые изменения в данных.

4. Резервное копирование: Регулярное создание резервных копий данных для восстановления в случае повреждений или утрат.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

3. Раскройте понятие доступности информации в контексте информационной безопасности. Какие меры принимаются для обеспечения доступности информации в информационных системах?

Время выполнения – 20 мин.

Ожидаемый результат:

Доступность информации означает, что информация должна быть доступной для авторизованных пользователей в любое время, когда это необходимо. Для обеспечения доступности применяются следующие меры:

1. Резервирование ресурсов: Создание избыточных мощностей и компонентов системы, чтобы избежать простоев в случае выхода из строя отдельных элементов.

2. Балансировка нагрузки: Распределение запросов между несколькими серверами для равномерной загрузки и улучшения производительности.

3. Облачные решения: Использование облачных платформ для хранения и обработки данных, что обеспечивает высокую доступность благодаря распределенной инфраструктуре.

4. Отказоустойчивость: Проектирование систем с учетом возможных отказов и автоматическим восстановлением после сбоев.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

4. Опишите структуру и функции системы формирования режима информационной безопасности.

Время выполнения – 20 мин.

Ожидаемый результат:

Система формирования режима информационной безопасности представляет собой совокупность технических, программных и организационных мер, направленных на защиту информации от несанкционированного доступа, разрушения, изменения или разглашения.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

5. Какие элементы входят в состав системы формирования режима информационной безопасности?

Время выполнения – 20 мин.

Ожидаемый результат:

Структура системы формирования режима информационной безопасности обычно включает следующие элементы:

1. Политика информационной безопасности: Основной документ,

определяющий цели, задачи и принципы защиты информации в организации. Включает в себя правила и процедуры, регламентирующие работу с информацией.

2. Средства защиты информации: Технические и программные средства, используемые для обеспечения безопасности информации. Сюда относятся межсетевые экраны, антивирусные программы, системы шифрования и др.

3. Управление доступом: Механизмы, позволяющие контролировать доступ к информации на основе прав и привилегий пользователей. Включает в себя аутентификацию, авторизацию и учет действий пользователей.

4. Мониторинг и аудит: Процессы наблюдения за состоянием информационной безопасности и анализа событий, связанных с защитой информации. Включает в себя ведение журналов событий, анализ логов и регулярные проверки на соответствие политике безопасности.

5. Обучение и повышение квалификации персонала: Важнейший аспект, связанный с повышением осведомленности сотрудников об угрозах информационной безопасности и способах их предотвращения.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

6. Объясните, как разрабатывается и утверждается политика информационной безопасности в рамках системы формирования режима информационной безопасности.

Время выполнения – 20 мин.

Ожидаемый результат:

Разработка и утверждение политики информационной безопасности проходит несколько этапов:

1. Определение целей и задач: На этом этапе устанавливаются основные цели и задачи политики, исходя из специфики деятельности организации и существующих угроз информационной безопасности.

2. Анализ существующей инфраструктуры и процессов: Проводится анализ текущей информационной инфраструктуры и бизнес-процессов, чтобы определить, какие области требуют особого внимания и защиты.

3. Разработка содержания политики: Создается проект политики, включающий в себя описание правил и процедур, касающихся защиты информации. Важно учитывать законодательные требования, отраслевые стандарты и лучшие практики в области информационной безопасности.

4. Утверждение политики: Проект политики передается на рассмотрение и утверждение руководству организации. После утверждения политика становится обязательным документом для всех сотрудников.

5. Реализация и внедрение: Политика внедряется в повседневную практику организации, включая обучение персонала и внедрение соответствующих технических и программных средств защиты.

6. Мониторинг и пересмотр: Периодически проводится проверка исполнения политики и ее актуальности. При необходимости вносятся

коррективы и дополнения.

Критерии оценивания: полное содержательное соответствие приведенному выше пояснению.

Компетенции (индикаторы): ПК-4 (ПК-4.1)

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Информационная безопасность предприятия и технологии защиты информации» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 38.04.02 «Менеджмент».

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 подготовки 38.04.02 «Менеджмент».

Председатель учебно-методической комиссии
института управления и государственной службы _____ Студеникина В.П.

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)