ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для промежуточной аттестации

по дисциплине (модулю)

«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки
44.03.05 Педагогическое образование (2 профиля)

Направленности (профиль)

«Экономика и информатика»

Присваиваемая квалификация (степень)

БАКАЛАВР

Форма обучения
Очная

Челябинск 2025 г.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: **44.03.05 Педагогическое образование (с двумя профилями подготовки)**
Направленность (профиль) «**Экономика и информатика**»
Дисциплина: **Методы и средства защиты информации**
Семестр изучения: 5
Форма промежуточной аттестации: экзамен

Цель дисциплины – формирование профессиональных компетенций обучающихся при работе с современными системами информационной безопасности, технологическими способами защиты информации, организационными мерами по информационной защите, экономическими и правовыми принципами их функционирования, а также возможностями использования защиты в работе с информационными ресурсами в различных областях экономики и бизнеса.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «**Современные технологии поиска и обработки информации**» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-4	Способен использовать современные информационно-коммуникационные технологии для проектирования содержания образовательных программ и их элементов, создания и администрирования электронных образовательных ресурсов	ПК-4.1. Знает виды современных информационных технологий и электронных образовательных ресурсов ПК-4.2. Умеет проектировать содержание образовательных программ и их элементов, создавать и администрировать электронные образовательные ресурсы ПК-4.3. Владеет современные информационно-коммуникационными технологиям для проектирования содержания образовательных программ и их элементов, создания и администрирования электронных	**Знать:** современные информационные технологии и программные средства для решения профессиональных задач и электронные образовательные ресурсы **Уметь:** использовать современные информационные технологии и программные средства при решении профессиональных задач, создании и администрировании электронных образовательных ресурсов **Владеть:** Навыками использования современных информационных технологий и программных средств при решении профессиональных задач, создания и администрирования

		образовательных ресурсов	электронных образовательных ресурсов
ОПК-9	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК.9.1. Умеет использовать навыки работы с информацией из различных источников для решения профессиональных задач ОПК.9.2. Владеет базовыми компьютерными технологиями и программными средствами, технологиями обработки информации, навыками использования программных средств и работы в компьютерных сетях ОПК.9.3. Знает теоретические основы использования современных компьютерных технологий для решения задач профессиональной деятельности	**Знать**: принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности **Уметь:** понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности **Владеть** навыками понимания принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности

2.2. Сведения об иных дисциплинах, участвующих в формировании данных компетенций

2.2.1. **ПК-4** формируется в процессе изучения дисциплин (прохождения практик): Компьютерные сети и телекоммуникации; Информационные системы и базы данных; Web-технологии и web-дизайн; Аппаратное обеспечение информационных систем; Компьютерная графика и визуализация; ИКТ в образовании; Системы искусственного интеллекта; Теория алгоритмов; Производственная практика; Преддипломная практика; Государственная итоговая аттестация; Подготовка к процедуре защиты и защита выпускной квалификационной работы.

ОПК-9 формируется в процессе изучения дисциплин (прохождения практик): Технологии цифрового образования; Ознакомительная практика; Методы математической обработки данных; Программирование; Методика преподавания информатики; Компьютерные сети и телекоммуникации; Цифровая трансформация экономики; Информационные системы и базы данных; Аппаратное обеспечение информационных систем; ИКТ в образовании; Производственная практика; Преддипломная практика; Государственная итоговая аттестация; Подготовка к процедуре защиты и защита выпускной квалификационной работы.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1	**ПК-4** **Знать:** современные информационные технологии и программные средства для решения профессиональных задач и электронные образовательные ресурсы **Уметь:** использовать современные информационные технологии и программные средства при решении профессиональных задач, создании и администрировании электронных образовательных ресурсов **Владеть:** Навыками использования современных информационных технологий и программных средств при решении профессиональных задач, создания и администрирования электронных образовательных ресурсов	**Тема 1**. Информационная безопасность в системе национальной безопасности Российской Федерации	Вопросы на понимание материала 1-7	Тест 1– 18 Собеседование 1-9
		Тема 2. Основные понятия теории защиты информации. Анализ угроз информационной безопасности	Вопросы на понимание материала 8-16	Тест 19 – 34 Собеседование 10-19
		Тема 3. Методы и средства защиты информации. Защита информации криптографическими методами	Вопросы на понимание материала 17-23	Тест 35–48 Собеседование 20-26
		Тема 4. Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности	Вопросы на понимание материала 24-30	Тест 49–70 Собеседование 27-32
		Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	Вопросы на понимание материала 31-37	Тест 71–82 Собеседование 33-42

		Тема 6. Методология построения и анализа систем защиты информации	Вопросы на понимание материала 38-42	Тест 83–103 Собеседование 43-49
2	**ОПК-9** **Знать**: принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности **Уметь:** понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности **Владеть** навыками понимания принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности	**Тема 1**. Информационная безопасность в системе национальной безопасности Российской Федерации	Вопросы на понимание материа-ла 1-7	Тест 1–18 Собеседование 1-9
		Тема 2. Основные понятия теории защиты информации. Анализ угроз информационной безопасности	Вопросы на понимание материала 8-16	Тест 19–34 Собеседование 10-19
		Тема 3. Методы и средства защиты информации. Защита информации криптографическими методами	Вопросы на понимание материала 17-23	Тест 35–48 Собеседование 20-26
		Тема 4. Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности	Вопросы на понимание материала 24-30	Тест 49–70 Собеседование 27-32
		Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	Вопросы на понимание материала 31-37	Тест 71–82 Собеседование 33-42
		Тема 6. Методология построения и анализа систем защиты информации	Вопросы на понимание материала 38-42	Тест 83–103 Собеседование 43-49

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2 Содержание оценочных средств

3.2.1 Тестовые задания

Обозначения: * - для проверки ПК-4
**** - для проверки ОПК-9**

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации

1. **Невозможность получения сервиса законным пользователем называется
Атакой «man-in-the-middle»
Replay-атакой
DoS-атакой
Пассивной атакой

2. **Под безопасностью информационной системы понимается
Защита от неавторизованного доступа или модификации информации во время хранения, обработки или пересылки
Отсутствие выхода в интернет
Меры, необходимые для определения, документирования и учета угроз
Защита от отказа в обслуживании законных пользователей

3. **Риск — это
Вероятность того, что в системе остались неизвестные уязвимости
Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости
Невозможность ликвидировать все уязвимости в информационной системе
Невозможность исправить все ошибки в программном обеспечении

4. *Целостность – это

Невозможность несанкционированного доступа к информации
Невозможность несанкционированного выполнения программ
Невозможность несанкционированного изменения информации
Невозможность несанкционированного просмотра информации

5. *Анализ состояния в пакетном фильтре означает
Отслеживание состояния соединения и оповещение администратора о наличии пакета, который не соответствует ожидаемому
Отслеживание состояния соединения и отбрасывание пакетов, которые не соответствуют ожидаемому
Отслеживание состояния соединения и запрещение всего трафика, если обнаружен пакет, который не соответствует ожидаемому
Отслеживание состояния соединения и вставка собственных пакетов, если обнаружен пакет, который не соответствует ожидаемому

6. Сокетом называется
Пара (MAC-адрес, IP-адрес)
Пара (IP-адрес, порт)
Пара (DNS-имя, IP-адрес)
Пара (DNS-имя, порт)

7. *Инициализация TCP-соединения выполняется
Сервером
Клиентом
Третьей доверенной стороной
Администратором

8.** Межсетевые экраны для веб-приложений располагают
Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу)
Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен
После защищаемого веб-сервера (трафик вначале передается веб-серверу,

затем межсетевому экрану)
Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен

9. **Недостатки межсетевых экранов прикладного уровня
Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра
Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней
Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр
Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение

10. **Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются
Исключительно программными
Аппаратно-программными средствами защиты
Не могут быть встроенными в ОС, которую они защищают; всегда реализованы внешними производителями
Всегда встроены в ОС, которую они защищают; не могут быть реализованы внешними производителями

11.* Выделенные прокси-серверы предназначены для того, чтобы обрабатывать трафик
Конкретного пользователя
Конкретного уровня модели OSI
Конкретного адреса отправителя
Конкретного прикладного протокола

12.* Примеры IP-адресов, которые не должны появляться в пакетах
192.168.254.0
0.0.0.0

с 127.0.0.0 по 127.255.255.255
192.168.0.254

13. **Определение и реагирование на инциденты безопасности
При среднем уровне шкалы строгости инцидентом безопасности можно считать ту или иную форму активных попыток получения неавторизованного доступа к компьютерной системе
При низком уровне шкалы инцидентом может считаться любая успешная попытка получения неавторизованного доступа к системе или ресурсам
Верны все ответы
При высоком уровне шкалы строгости инцидентом безопасности может считаться зондирование сети или системы, которое может использоваться для изучения топологии сети

14. **При определении злоупотреблений
Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак»
Анализируется частота возникновения некоторого события
Анализируются события для обнаружения неожиданного поведения
Анализируются подписи в сертификатах открытого ключа

15. **Инструментальные средства проверки целостности файлов позволяют определить
Наличие Троянских программ
Нарушение авторизации пользователей
Нарушение аутентификации пользователей
Подмененные системные файлы

16. **Шейпингом трафика (traffic shaping) называется
Возможность указывать приоритеты для определенных сервисов
Возможность запрещать определенные сервисы
Возможность обеспечивать гарантии полосы пропускания
Возможность отбрасывать пакет, основываясь на IP-адресах отправителя и

получателя

17. *Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных:
Выделение персональных данных
Обеспечение безопасности персональных данных
Деавторизация
Деперсонификация

18. ** Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
Авторизация
Деперсонализация
Аутентификáция
Идентификация

Тема 2. Основные понятия теории защиты информации. Анализ угроз информационной безопасности

19. **Наиболее опасным источником угроз информационной безопасности предприятия являются:
Другие предприятия (конкуренты)
Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
Рядовые сотрудники предприятия
Хакеры

20. *Закон Российской Федерации «о государственной тайне» был принят в следующем году:
1991
1992
1993
2005

21. *Документированной информацией, доступ к которой ограничен в соответствии с законодательством РФ, называется
Конфиденциальная
Персональная
Документированная
Информация, составляющая государственную тайну

22. *Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в:
1 главе Уголовного кодекса
5 главе Уголовного кодекса
28 главе Уголовного кодекса
100 главе Уголовного кодекса

23. *В статье 272 уголовного кодекса говорится…
О неправомерном доступе к компьютерной информации
О создании, исполнении и распространении вредоносных программ для ЭВМ
О преступлениях в сфере компьютерной информации
Об ответственности за преступления в сфере компьютерной информации

24. *Федеральный закон «об информации, информатизации и защите информации» направлен на:
Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
Регулирование требований к работникам служб, работающих с информаций
Формирование необходимых норм и правил работы с информацией
Формирование необходимых норм и правил, связанных с защитой детей от информации

25. *Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер,

не подсоединяемые к компьютеру и имеющие собственный источник питания:
Автономный токен
USB-токен
Устройство iButton
Смарт-карта

26. *Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
наиболее важные субъекты
наиболее важные объекты
все субъекты
все объекты

27. *Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
уязвимость информации
надежность информации
защищенность информации
безопасность информации

28.* Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне
E5
E7
E4
E6

29.* Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев
D
A

В
С

30. *Соответствие средств безопасности решаемым задачам характеризует
эффективность
корректность
адекватность
унификация

31. *С помощью закрытого ключа информация
копируется
транслируется
расшифровывается
зашифровывается

32. *По документам ГТК количество классов защищенности АС от НСД
8
7
9
6

33.* Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется
избирательным
мандатным
привилегированным
идентифицируемым

34.* На многопользовательские системы с информацией одного уровня конфиденциальности согласно «Оранжевой книге» рассчитан класс
С1
В2

C2
B1

Тема 3. Методы и средства защиты информации. Защита информации криптографическими методами

35. *При избирательной политике безопасности в матрице доступа субъекту системы соответствует
ячейка
строка
прямоугольная область
столбец

36. *Недостаток систем шифрования с открытым ключом
при использовании простой замены легко произвести подмену одного шифрованного текста другим
относительно низкая производительность
необходимость распространения секретных ключей
на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

37. *По документам ГТК самый высокий класс защищенности СВТ от НСД к информации
1
6
9
7

38. *Конечное множество используемых для кодирования информации знаков называется
шифром
кодом
алфавитом
ключом

39. *Первым этапом разработки системы защиты ИС является
анализ потенциально возможных угроз информации
изучение информационных потоков
стандартизация программного обеспечения
оценка возможных потерь

40. *По документам ГТК количество классов защищенности СВТ от НСД к информации
9
6
8
7

41. *При избирательной политике безопасности в матрице доступа объекту системы соответствует
ячейка
столбец
прямоугольная область
строка

42. *Надежность СЗИ определяется
усредненным показателем
самым слабым звеном
количеством отраженных атак
самым сильным звеном

43. *Обеспечением скрытности информации в информационных массивах занимается
криптография
криптоанализ
криптология
стеганография

44. *Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
системой защиты
стандартом безопасности
профилем безопасности
профилем защиты

45. *Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности — согласно «Оранжевой книге» требованиями в области аудита являются
1, 2
3, 4
2, 4
1, 3

46.* Из перечисленных программных закладок: 1) вирусные; 2) троянские; 3) программно-аппаратные; 4) загрузочные; 5) драйверные; 6) прикладные — по методу внедрения в компьютерную систему различают
2, 3, 4, 5
3, 4, 5, 6
1, 2, 4, 6
1, 2, 3, 6

47.* Из перечисленных классов: 1) обнаруживаемые операционной системой при загрузке; 2) качественные и визуальные; 3) аппаратные; 4) обнаруживаемые средствами тестирования и диагностики — признаки присутствия программной закладки в компьютере можно разделить на
1, 4
1, 3
2, 3
2, 4

48. *Оконечное устройство канала связи, через которое процесс может

передавать или получать данные, называется
терминалом
портом
сокетом
хостом

Тема 4. Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности

49. **Из перечисленного тиражирование данных происходит в режимах: 1) синхронном; 2) асинхронном; 3) импульсном; 4) тоновом
2, 4
3, 4
1, 3
1, 2

50. **Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом
1, 2, 5
1, 3, 5
1, 2, 3
4, 5, 6

51. **Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем
сетевом
транспортном
физическом
канальном

52. **Недостатком матричных моделей безопасности является
отсутствие полного аудита
отсутствие контроля за потоками информации

сложность представления широкого спектра правил обеспечения безопасности
невозможность учета индивидуальных особенностей субъекта

53.* Из перечисленного цифровая подпись используется для обеспечения услуг: 1) аутентификации; 2) целостности; 3) контроля доступа; 4) контроля трафика
1, 2
1, 3
2, 4
3, 4

54. *Из перечисленного система защиты электронной почты должна: 1) обеспечивать все услуги безопасности; 2) обеспечивать аудит; 3) поддерживать работу только с лицензионным ПО; 4) поддерживать работу с почтовыми клиентами; 5) быть кросс-платформенной
2, 3, 4
1, 3, 5
1, 4, 5
1, 2, 3

55.* Иерархическая система классификации информации отличается от фасетной системы …
Возможностью группировки объектов
Более жесткой структурой
Использованием независимых классификационных признаков
Возможностью создания классификации большей емкости

56. **Перечислите основные топологии локальной вычислительной сети.
Звезда, кольцо, шина
Звезда, круг, шина
Квадрат, кольцо, шина
Звезда, кольцо, круг

57.* Какую функциональную задачу выполняет прикладной уровень сетевого
протокола взаимодействия открытых систем?
Управление логическими каналами
Обеспечение сеансов связи
Параметрическое отображение данных
Выполнение процессов

58. *Какую функциональную задачу выполняет представительный уровень сетевого протокола взаимодействия открытых систем?
Управление логическими каналами
Обеспечение сеансов связи
Параметрическое отображение данных
Выполнение процессов

59. *Какую функциональную задачу выполняет сеансовый уровень сетевого протокола взаимодействия открытых систем?
Управление логическими каналами
Обеспечение сеансов связи
Параметрическое отображение данных
Выполнение процессов

60 *Какую функциональную задачу выполняет транспортный уровень сетевого
протокола взаимодействия открытых систем?
Управление логическими каналами
Обеспечение сеансов связи
Параметрическое отображение данных
Выполнение процессов

61 *Какую функциональную задачу выполняет сетевой уровень сетевого протокола взаимодействия открытых систем?

Управление логическими каналами
Маршрутизация пакетов
Параметрическое отображение данных
Выполнение процессов

62 *Какую функциональную задачу выполняет канальный уровень сетевого протокола взаимодействия открытых систем?
Управление логическими каналами
Маршрутизация пакетов
Управление передачей по информационному каналу
Выполнение процессов

63 *Какую функциональную задачу выполняет физический уровень сетевого
протокола взаимодействия открытых систем?
Управление логическими каналами
Маршрутизация пакетов
Управление передачей по информационному каналу
Сопряжение физического канала

64. *С точки зрения ГТК основной задачей средств безопасности является обеспечение
сохранности информации
защиты от НСД
простоты реализации
надежности функционирования

65. *При качественном подходе риск измеряется в терминах
денежных потерь
заданных с помощью шкалы или ранжирования
оценок экспертов
объема информации

66. *Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
криптология
стеганография
криптоанализ
криптография

67. **Недостатком модели политики безопасности на основе анализа угроз системе является
изначальное допущение вскрываемости системы
статичность
необходимость дополнительного обучения персонала
сложный механизм реализации

68. **Политика информационной безопасности — это
профиль защиты
итоговый документ анализа рисков
стандарт безопасности
совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

69. **Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема регистрации и учета системы защиты информации должна обеспечивать
1, 4
2, 3
3, 4
1, 2

70.** Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема регистрации и учета

системы защиты информации должна обеспечивать
1, 4
2, 3
3, 4
1, 2

Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей

71.* Из перечисленного: 1) перехват; 2) искажение; 3) внедрение; 4) захват ресурсов; 5) уборка мусора; 6) наблюдение и компрометация — различают модели воздействия программных закладок на компьютеры
1, 2, 3, 6
1, 2, 3
4, 5, 6
1, 2, 5, 6

72 *Из перечисленного: 1) эффективность; 2) корректность; 3) унификация; 4) конфиденциальность — аспектами адекватности средств защиты являются
1, 3
1, 2
3, 4
2, 4

73. *Из перечисленных свойств: 1) конфиденциальность; 2) восстанавливаемость; 3) доступность; 4) целостность; 5) детерминированность — безопасная система обладает
1, 3, 4
1, 2, 3
1, 3, 5
2, 4, 5

74. *Количество уровней адекватности, которое определяют «Европейские критерии»
3
5
7
10

75. *Из перечисленных классов: 1) обнаруживаемые операционной системой при загрузке; 2) качественные и визуальные; 3) аппаратные; 4) обнаруживаемые средствами тестирования и диагностики — признаки присутствия программной закладки в компьютере можно разделить на
1, 4
1, 3
2, 3
2, 4

76. *Из перечисленных требований: 1) резервное копирование; 2) аутентификация; 3) необходимость записи всех движений защищаемых данных; 4) накопление статистики — при разработке протоколирования в системе защиты учитываются
2, 3
3, 4
1, 2
1, 4

77.* Из перечисленного: 1) случайная; 2) преднамеренная; 3) стихийная; 4) детерминированная; 5) объективная; 6) субъективная — угрозы безопасности по природе происхождения классифицируются как
1, 2, 3, 4
5, 6
3, 4
1, 2

78. *Из перечисленных категорий требований безопасности: 1) политика безопасности; 2) аудит; 3) идентификация; 4) корректность; 5) аутентификация — в «Оранжевой книге» предложены
1, 2, 4
3, 4, 5
1, 2, 5
1, 2, 3

79. *Из перечисленного: 1) оповещение о попытках нарушения защиты; 2) идентификация; 3) аутентификация; 4) учет носителей информации; 5) управление потоками информации — подсистема управления доступом системы защиты информации должна обеспечивать
2, 3, 5
3, 4, 5
1, 2, 5
1, 2, 3

80. **Достоинством дискретных моделей политики безопасности является
высокая степень надежности
числовая вероятностная оценка надежности
простой механизм реализации
динамичность

81. **Два ключа используются в криптосистемах
с открытым ключом
с закрытым ключом
двойного шифрования
симметричных

82.** Достоинствами аппаратной реализации криптографического закрытия данных являются
высокая производительность и простота
доступность и конфиденциальность

практичность и гибкость
целостность и безопасность

Тема 6. . Методология построения и анализа систем защиты информации

83. **Защита с применением меток безопасности, согласно «Оранжевой книге», используется в системах класса
C2
B1
C1
B2

84. **Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это
принцип многоуровневой защиты
принцип минимизации привилегий
принцип простоты и управляемости ИС
принцип максимизации привилегий

85.* Главным параметром криптосистемы является показатель
безошибочности шифрования
скорости шифрования
криптостойкости
надежности функционирования

86. *Длина исходного ключа в ГОСТ 28147–89 (бит)
256
64
128
56

87.** Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ

потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает
3, 4
1, 2
1, 3
2, 4

88. **При количественном подходе риск измеряется в терминах
объема информации
заданных с помощью шкалы
денежных потерь
заданных с помощью ранжирования

89. *Согласно «Оранжевой книге» мандатную защиту имеет группа критериев
D
C
A
B

90. *Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это
аутентификация
идентификация
аудит
авторизация

91. *Согласно «Оранжевой книге» с объектами должны быть ассоциированы
метки безопасности
типы операций
электронные подписи
уровни доступа

92. **Программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти в модели воздействия
компрометация
перехват
наблюдение
уборка мусора

93. **Содержанием параметра угрозы безопасности информации «конфиденциальность» является
несанкционированная модификация
искажение
несанкционированное получение
уничтожение

94. **Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется
мониторингом средств защиты
минимизацией риска
управлением риском
оптимизацией средств защиты

95. **Согласно «Оранжевой книге» верифицированную защиту имеет группа критериев
C
A
D
B

96.* С помощью открытого ключа информация
транслируется

расшифровывается
копируется
зашифровывается

97.** Требования к техническому обеспечению системы защиты
аппаратурные и физические
управленческие и документарные
процедурные и раздельные
административные и аппаратур

98. **У всех программных закладок имеется общая черта
обязательно выполняют операцию записи в память
перехватывают прерывания
обязательно выполняют опера-цию чтения из памяти
постоянно находятся в оперативной памяти

99. **Являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от кла-виатуры, клавиатурные шпионы типа
перехватчики
фильтры
заместители
имитаторы

100. *Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
восстанавливаемость
детермированность
целостность
доступность

101. **Брандмауэры первого поколения представляли собой «неприступные серверы»

маршрутизаторы с фильтрацией пакетов
«уполномоченные серверы»
хосты с фильтрацией пакетов

102. *Дескриптор защиты в Windows 2000 содержит список
привилегий, назначенных пользователю
объектов, не доступных пользователям
объектов, доступных пользователю и группе
пользователей и групп, имеющих доступ к объекту

103. **ACL-список ассоциируется с каждым
типом доступа
процессом
объектом
доменом

3.2.2 Вопросы для оценки среднего уровня

Вопросы для собеседования

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности

Тема 2. Основные понятия теории защиты информации. Анализ угроз информационной безопасности

10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации

Тема 3. Методы и средства защиты информации. Защита информации криптографическими методами

20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности

Тема 4. Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности

27. Защита от несанкционированного доступа
28. Антивирусная защита

29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации
32. В каком случае информационная безопасность обеспечивается комплексом программных средств?

Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей

33. Основные понятия, используемые при описании моделей разграничения доступа: объект, субъект, метод, право, привилегия, владелец, суперпользователь.
34. Избирательное разграничения доступа.
35. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки.
36. Изолированная программная среда. Полномочное разграничение доступа.
37. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.
38. Особенности разграничения доступа в системах управления базами данных.
39. Разграничение доступа в Unix- системах.
40. Формат, атрибутов защиты файла.
41. Разграничения доступа в Windows. Права, привилегии.
42. Формат атрибутов защиты объекта. Концепция олицетворения.

Тема 6. Методология построения и анализа систем защиты информации

43. Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы.
44. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок.
45. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг.

46. Факторы, ограничивающие эффективность антивирусных средств.
47. Задача защиты от несанкционированного копирования.
48. Методы привязки к программно-аппаратной среде.
49. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации.

3.2.3 База контрольных заданий для оценки высокого уровня

Вопросы на понимание материала

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.

2. Распространение объектно-ориентированного подхода на информационную безопасность.

3. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.

4. Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы.

5. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.

6. Международные стандарты информационного обмена. Стандарт ISO/IEC15408.

7. Российские стандарты защищенности автоматизированных систем.

Тема 2. Основные понятия теории защиты информации. Анализ

угроз информационной безопасности

8. Основные положения теории информационной безопасности. Модели безопасности и их применение.

9. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

10. Информационная безопасность в условиях функционирования в России глобальных сетей.

11. Виды противников или "нарушителей". Понятия о видах вирусов Виды возможных нарушений информационной системы. Виды защиты.

12. Файловые вирусы.

13. Загрузочные вирусы.

14. Вирусы и операционные системы.

15. Методы и средства борьбы с вирусами.

16. Профилактика заражения вирусами компьютерных систем.

Тема 3. Методы и средства защиты информации. Защита информации криптографическими методами

17. Защита информации от случайных угроз.

18. Дублирование информации.

19. Повышение надежности компьютерных систем.

20. Обеспечение отказоустойчивости компьютерных систем.

21. Блокировка ошибочных операций.

22. Защита информации от традиционного шпионажа и диверсий.

23. Система охраны объектов компьютерных систем.

Тема 4. Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности

24. Организация работы с конфиденциальными информационными ресурсами.

25. Противодействие подслушиванию и наблюдению в оптическом диапазоне.

26. Средства борьбы с закладными подслушивающими устройствами.

27. Защита от злоумышленных действий обслуживающего персонала и пользователей.

28. Средства защиты компьютеров. Программно аппаратные методы и средства ограничения доступа к компонентам компьютера. Типы несанкционированного доступа и условия работы средств защиты.

29. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

30. Защита от несанкционированного копирования программного обеспечения.

Тема 5. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей

31. Методы криптографии.

32. Основные понятия шифрования.

33. Методы шифрования с симметричным ключом.

34. Системы шифрования с открытым ключом.

35. Стандарты шифрования.

36. Промышленные программные средства Kerberos, PGP.

37. Методы и средства хранения ключевой информации. Анализ программных реализаций.

Тема 6. Методология построения и анализа систем защиты информации

38. Защита от разрушающих программных воздействий.

39. Основные технологии построения защищенных ЭИС.

40. Системные вопросы защиты программ и данных.

41. Основные категории требований к средствам обеспечения информационной безопасности

42. Место информационной безопасности экономических систем в национальной безопасности страны

3.3 Порядок проведения экзамена и критерии оценивания

Итоговое занятие по проверке сформированности компетенций проводится в форме выполнения письменного комплексного задания, включающего:

1) вопросы в форме закрытого теста:

№ п/п	Контролируемые разделы	Количество вопросов
1	Информационная безопасность в системе национальной безопасности Российской Федерации	1
2	Основные понятия теории защиты информации. Анализ угроз информационной безопасности	1
3	Методы и средства защиты информации. Защита информации криптографическими методами	1
4	Основы комплексной защиты информации. Модели, стратегии (политики) и системы обеспечения информационной безопасности	1

5	Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	1
6	Методология построения и анализа систем защиты информации	1

Критерии оценивания теста:

Вопрос теста предполагает 1 правильный вариант ответа	
Указан 1 вариант, который является правильным	2 балла
Указаны 2 варианта ответа, 1 из которых правильный	1 балл
Указаны 1 или 2 неправильных варианта	0 баллов
Указаны 3 и более варианта ответа	0 баллов

2) теоретический вопрос, предполагающий развернутый ответ на поставленный вопрос – по одному из разделов дисциплины.

Критерии оценивания ответа на теоретический вопрос:

Количество баллов	Критерии оценки
6	Задание выполнено полностью, студент демонстрирует сформированность как знаниевой, так и деятельностной составляющих компетенций, сформированы предметные и межпредметные знания и умения, демонстрируются умения применять знания в разных ситуациях. Ответ на вопрос является максимально полным и точным.
5	Студент четко определяет проблему, пути ее решения, у него частично сформированы предметные и межпредметные знания и умения, демонстрируются умения применять знания в разных ситуациях, однако отсутствуют умения аргументировать сделанный выбор, продемонстрировать предлагаемые способы решения проблемы. Ответ дан достаточно полно, но может быть дополнен с учетом материалов самостоятельной работы.
4	Студент четко определяет проблему, пути ее решения, у него частично сформированы предметные и межпредметные знания и умения, частично демонстрируются умения применять знания в разных ситуациях, отсутствуют умения аргументировать сделанный выбор, продемонстрировать предлагаемые способы решения проблемы. Ответ дан достаточно полно, но может быть дополнен с учетом материалов самостоятельной работы.
3	Студент формулирует проблему, содержащую в задании, определяет пути ее решения, однако сформированы изолированные знания и умения, отсутствуют умения устанавливать внутри- и межпредметные связи в содержании, нет опыта решения подобных заданий, в результате предложенные варианты решения неверны. Ответ дан недостаточно полно, может быть существенно дополнен с учетом материалов практических занятий и самостоятельной работы.
2	Студент не может сформулировать проблему, представленную в задании,

	не знает способов ее решения, в силу недостаточной теоретической подготовки. Дан неполный ответ, может быть существенно дополнен с учетом материалов лекционных и практических занятий, самостоятельной работы.
1	Студент не может сформулировать проблему, представленную в задании, не знает способов ее решения, в силу недостаточной теоретической подготовки. Дан неправильный ответ, который свидетельствует об отсутствии знаний, умений, навыков, свидетельствующих об овладении компетенциями по дисциплине, но содержатся признаки владения компетенциями, закрепленными за другими дисциплинами.
0	Нет ответа.

3) вопросы на понимание материала дисциплины (вопрос на сравнение понятия, процессов, явлений. объяснение причин и последствий определенных фактов, процессов, явлений и т. п.), которые предполагают лаконичный ответ путем формулировки и аргументации собственной точки зрения – по трем другим раздела дисциплины.

Критерии оценивания ответа

Количество баллов	Критерии оценки
4	Задание выполнено полностью, студент демонстрирует сформированность как знаниевой, так и деятельностной составляющих компетенций, сформированы предметные и межпредметные знания и умения, демонстрируются умения применять знания в разных ситуациях. Ответ на вопрос является максимально полным и точным.
3	Студент четко определяет проблему, пути ее решения, у него частично сформированы предметные и межпредметные знания и умения, частично демонстрируются умения применять знания в разных ситуациях, однако отсутствуют умения аргументировать сделанный выбор, продемонстрировать предлагаемые способы решения проблемы. Ответ дан достаточно полно, но может быть дополнен с учетом материалов самостоятельной работы.
2	Студент формулирует проблему, содержащую в задании, определяет пути ее решения, однако сформированы изолированные знания и умения, отсутствуют умения устанавливать внутри- и межпредметные связи в содержании, нет опыта решения подобных заданий, в результате предложенные варианты решения неверны. Ответ дан недостаточно полно, может быть существенно дополнен с учетом материалов практических занятий и самостоятельной работы.
1	Студент не может сформулировать проблему, представленную в задании, не знает способов ее решения, в силу недостаточной теоретической подготовки. Дан неполный ответ, может быть существенно дополнен с учетом материалов лекционных и практических занятий, самостоятельной работы.
0	Нет ответа.

Задание должно быть выполнено в течение 60 минут.

Критерии оценивания

Количество баллов	Итоговая оценка
20-22	Отлично
17-19	Хорошо
14-16	Удовлетворительно
0-13	Неудовлетворительно

Компетенции по дисциплине считаются сформированными, если по итогам промежуточной аттестации студент получил оценку удовлетворительно, хорошо, отлично.

44.03.05, Экономика и информатика, Педагогическое образование (с двумя профилями подготовки), Методы и средства защиты информации, 2025 год, очная

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено

Ученым советом факультета

Протокол заседания №

Председатель Ученого совета
экономического факультета согласовано А. А. Егорова

Заседанием кафедры

Протокол заседания №

Заведующий кафедрой согласовано

Автор (составитель) В. Н. Артамонов

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1