Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»
Колледж СКФУ в г. Ставрополе

УТВЕРЖДАЮ
и.о. директора института перспективной инженерии, канд. тех. наук,
доцент Порохня А.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по (учебной) дисциплине ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Форма обучения очная
очная, заочная, очно-заочная

Ставрополь

1. Паспорт фонда оценочных средств

1.1. Область применения

Фонд оценочных средств (далее - ФОС) предназначен для оценивания знаний, умений, уровня сформированности компетенций студентов, обучающихся по специальности 09.02.11 Разработка и управление программным по дисциплине ОП.05 Основы информационной безопасности.

ФОС составлен на основе ФГОС и рабочей программы дисциплины.

Промежуточная аттестация по *(учебной)* дисциплине предусмотрена в форме *экзамена* с выставлением отметки по системе «отлично, хорошо, удовлетворительно, неудовлетворительно».

1.2. Планируемые результаты освоения (учебной) дисциплины

ФОС позволяет оценить знания, умения, сформированность общих и профессиональных компетенций в соответствии с требованиями ФГОС и рабочей программой *(учебной)* дисциплины.

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-
ОК.02	определять задачи для поиска информации; определять необходимые источники	номенклатура информационных источников, применяемых в	-

	информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	
ОК.03	планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ОК.04	эффективно взаимодействовать и работать в коллективе и команде		
ПК 1.5	шифровать данные и обеспечивать их конфиденциальность	принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование паролей,	-

		сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	
ПК 2.4	выполнять тестирование и отладку программного обеспечения	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности	-
ПК 3.8	производить оценку информационной системы для выявления возможности ее модернизации	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных. стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA основные принципы безопасности информации и методов ее защиты. стандартные криптографические алгоритмы для шифрования данных принципы обеспечения безопасности передачи данных по сети основы безопасности приложений и инфраструктуры методы анализа на уязвимости и мониторинга безопасности знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа. обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных

		понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы	

1.3. Формы контроля и оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по *(учебной)* дисциплине, направленные на формирование общих и профессиональных компетенций

Таблица 1 Контроль и оценка освоения (учебной) дисциплины по темам (разделам)

Элемент учебной дисциплины	**Формы и методы контроля**			
	Текущий контроль		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые ОК, ПК**	**Форма контроля**	**Проверяемые ОК, ПК**
Раздел: Основы информационной безопасности		*ОК 01, ОК 03, ОК 04* ПК 1.5, ПК 2.4, ПК 3.8	Экзамен	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.5, ПК 2.4, ПК 3.8
Тема 1.1. Введение в информационную безопасность	Устный опрос Самостоятельная работа			
Тема 1.2. Управление безопасностью информации	Устный опрос Самостоятельная работа Практическая работа №1 Практическая работа №2 Практическая работа №3	*ОК 01, ОК 02, ОК 03* ПК 1.5, ПК 2.4		

Тема 1.3. Криптография	Устный опрос Самостоятельная работа Практическая работа №4 Практическая работа №5	*ОК 02, ОК 03, ОК 04* ПК 2.4, ПК 3.8		
Тема 1.4. Защита сетевой инфраструктуры	Устный опрос Самостоятельная работа Практическая работа № 6 Практическая работа № 7	*ОК 01, ОК 03, ОК 04* ПК 1.5, ПК 2.4, ПК 3.8		
Тема 1.5. Безопасность приложений	Устный опрос Самостоятельная работа Практическая работа № 8 Практическая работа № 9	*ОК 01, ОК 02, ОК 03* ПК 1.5, ПК 2.4		
Тема 1.6. Защита данных	Устный опрос Самостоятельная работа Практическая работа № 10 Практическая работа № 11	*ОК 02, ОК 03, ОК 04* ПК 2.4, ПК 3.8		
Тема 1.7. Безопасность облачных технологий	Устный опрос Самостоятельная работа Практическая работа № 12 Практическая работа № 13	*ОК 01, ОК 03, ОК 04* ПК 1.5, ПК 2.4, ПК 3.8		
Тема 1.8. Инциденты безопасности	Устный опрос Самостоятельная работа Практическая работа № 13 Практическая работа № 14	*ОК 01, ОК 02, ОК 03* ПК 1.5, ПК 2.4		

Тема 1.9. Социальная инженерия и человеческий фактор	Устный опрос Самостоятельная работа Практическая работа № 15 Практическая работа № 16	*ОК 02, ОК 03, ОК 04* ПК 2.4, ПК 3.8		
Тема 1.10. Будущее информационной безопасности	Устный опрос Самостоятельная работа Практическая работа № 17 Практическая работа № 18	*ОК 01, ОК 02, ОК 03* ПК 1.5, ПК 2.4		

2. Оценочные средства текущего контроля успеваемости и критерии оценки

Вариант 1

1. Что такое информационная безопасность? (1 правильный ответ)

a) Процесс разработки программного обеспечения

b) Защита информации от несанкционированного доступа, использования, раскрытия, искажения, уничтожения c) Управление базами данных

d) Создание резервных копий данных

2. Какие основные составляющие информационной безопасности? (1 правильный ответ)

a) Скорость, объем, качество

b) Надежность, совместимость, производительность

c) Конфиденциальность, целостность, доступность

d) Доступность, масштабируемость, безопасность

3. Какое место занимает информационная безопасность в системе национальной безопасности? (1 правильный ответ) a) Регулирует экономическую политику

b) Контролирует транспортную систему

c) Обеспечивает защиту государственных интересов в информационной сфере

d) Управляет образовательными процессами

4. Какие виды защищаемой информации существуют? (Несколько правильных ответов)

a) Персональные данные

b) Публичные отчеты

c) Коммерческая тайна

d) Рекламные материалы

5. Какие основные источники угроз информационной безопасности? (Несколько правильных ответов) a) Хакеры
b) Вирусы
c) Законодательные акты
d) Внутренние сотрудники

6. Что такое риск информационной безопасности? (1 правильный ответ)
a) Скорость обработки данных
b) Объем хранимой информации
c) Уровень защиты информации
d) Вероятность реализации угрозы с негативными последствиями

7. Какие этапы входят в жизненный цикл информации? (1 правильный ответ)
a) Разработка, тестирование, внедрение
b) Создание, обработка, передача, хранение, уничтожение
c) Планирование, исполнение, контроль
d) Анализ, проектирование, реализация

8. В чем различие между конфиденциальностью и целостностью информации? (1 правильный ответ)
a) Конфиденциальность регулирует хранение, целостность — доступность
b) Конфиденциальность защищает от вирусов, целостность — от хакеров
c) Конфиденциальность предотвращает несанкционированный доступ, целостность обеспечивает неизменность данных
d) Конфиденциальность обеспечивает скорость передачи, целостность — объем данных

9. Что подразумевается под доступностью информации? (1 правильный ответ)
a) Шифрование данных
b) Хранение данных на сервере
c) Возможность своевременного доступа для авторизованных пользователей
d) Уничтожение устаревшей информации

10. Как классифицируется информация по видам тайны? (Несколько правильных ответов) a) Государственная
b) Техническая
c) Коммерческая
d) Персональная

11. Какие степени конфиденциальности существуют для защищаемой информации? (1 правильный ответ) a) Высокая, средняя, низкая
b) Совершенно секретно, секретно, для служебного пользования
c) Публичная, ограниченная, закрытая

d) Основная, дополнительная, вспомогательная

12. Какое из перечисленных является примером преступления в сфере информационных технологий? (1 правильный ответ) a) Нарушение трудового законодательства

b) Несанкционированный доступ к компьютерной информации

c) Нарушение правил дорожного движения

d) Несоблюдение налогового законодательства

13. Какова цель политики информационной безопасности? (1 правильный ответ)

a) Разработка программного обеспечения

b) Управление финансовыми потоками

c) Обучение сотрудников программированию

d) Определение правил и процедур защиты информации

14. Какова роль менеджмента информационной безопасности в организации? (1 правильный ответ)

a) Разработка маркетинговых стратегий

b) Координация процессов защиты информации

c) Управление производственными процессами

d) Контроль качества продукции

15. Что такое уязвимость в контексте информационной безопасности? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Законодательный акт

c) Слабое место в системе, которое может быть использовано для атаки

d) Сертификат безопасности

16. Какие методы используются для оценки уязвимостей? (Несколько правильных ответов)

a) Сканирование уязвимостей

b) Тестирование на проникновение

c) Разработка программ

d) Финансовый аудит

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов) a) Сетевые атаки

b) Физический доступ

c) Обучение сотрудников

d) Социальная инженерия

18. Как классифицировать угрозы информационной безопасности по их источникам? (1 правильный ответ)

a) Технические, программные, аппаратные

b) Внешние, внутренние, случайные

c) Финансовые, юридические, административные

d) Плановые, внеплановые, периодические

19. Какие меры противодействия угрозам информационной безопасности существуют? (Несколько правильных ответов) a) Антивирусное программное обеспечение
b) Межсетевые экраны
c) Маркетинговая стратегия
d) Шифрование данных

20. Какова цель нормативно-правового регулирования в области информационной безопасности? (1 правильный ответ) a) Регулирование трудовых отношений
b) Установление правил защиты информации
c) Контроль качества продукции
d) Управление образовательными процессами

21. Какой российский законодательный акт регулирует защиту информации? (1 правильный ответ) a) Трудовой кодекс РФ
b) Федеральный закон «Об информации, информационных технологиях и о защите информации»
c) Гражданский кодекс РФ
d) Налоговый кодекс РФ

22. Какие международные стандарты определяют требования к защите информации? (Несколько правильных ответов) a) ISO/IEC 27001
b) ISO 9001
c) ISO/IEC 27002
d) IEEE 802.11

23. Что такое система сертификации в области защиты информации в РФ? (1 правильный ответ)
a) Процесс разработки программного обеспечения
b) Процесс подтверждения соответствия средств защиты стандартам
c) Процедура финансового аудита
d) Система обучения персонала

24. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов) a) Аутентификация
b) Шифрование
c) Разработка кода
d) Контроль доступа

25. Какие программно-аппаратные средства защиты информации существуют? (Несколько правильных ответов) a) Межсетевые экраны
b) Антивирусы
c) Текстовые редакторы

d) Системы обнаружения вторжений

26. Что такое организационно-распорядительная защита информации? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Совокупность документов и процедур для защиты информации

c) Физическая охрана объектов

d) Резервное копирование данных

27. Какие принципы лежат в основе организационно-распорядительной системы защиты? (Несколько правильных ответов) a) Законность

b) Системность

c) Скорость

d) Комплексность

28. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов) a) Угрозы

b) Уязвимости

c) Финансовые ограничения

d) Сбои оборудования

29. Что такое государственная тайна? (1 правильный ответ)

a) Публичные данные правительства

b) Информация, защищаемая государством от разглашения

c) Финансовые отчеты государства

d) Образовательные материалы

30. Какие методы анализа рисков информационной безопасности существуют? (Несколько правильных ответов) a) Анализ рисков

b) Моделирование угроз

c) Финансовый аудит

d) Тестирование на проникновение

Вариант 2

1. Что такое информация в контексте информационной безопасности? (1 правильный ответ)

a) Финансовые отчеты организации

b) Рекламные материалы

c) Данные, подлежащие защите от несанкционированного доступа

d) Программное обеспечение для управления базами данных

2. Какие объекты входят в состав защищаемых систем? (Несколько правильных ответов)

a) Информационные системы

b) Транспортные средства

c) Базы данных

d) Серверы

3. Как информационная безопасность связана с национальной безопасностью? (1 правильный ответ)

a) Регулирует экономические процессы

b) Контролирует транспортную инфраструктуру

c) Управляет образовательной системой

d) Защищает государственные интересы в информационной сфере

4. Какие носители защищаемой информации существуют? (Несколько правильных ответов) a) Жесткие диски

b) Бумажные документы

c) Рекламные буклеты

d) Флеш-накопители

5. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов) a) Финансовые ограничения

b) Угрозы

c) Уязвимости

d) Сбои оборудования

6. Что такое угроза информации? (1 правильный ответ)

a) Законодательный акт

b) Потенциальное событие, способное нанести ущерб информации

c) Программное обеспечение для защиты данных

d) Сертификат безопасности

7. Какие этапы включает жизненный цикл конфиденциальной информации? (1 правильный ответ)

a) Планирование, тестирование, внедрение

b) Анализ, проектирование, реализация

c) Создание, обработка, передача, хранение, уничтожение

d) Разработка, контроль, аудит

8. В чем заключается сущность целостности информации? (1 правильный ответ)

a) Сохранение данных на сервере

b) Обеспечение неизменности и достоверности данных

c) Уничтожение устаревших данных

d) Шифрование информации

9. Как обеспечивается конфиденциальность информации? (1 правильный ответ)

a) Увеличением скорости передачи данных

b) Резервным копированием

c) Ограничением доступа для неавторизованных лиц

d) Анализом уязвимостей

10. Какие степени секретности существуют для информации? (1 правильный ответ)

a) Высокая, средняя, низкая

b) Публичная, ограниченная, закрытая

c) Совершенно секретно, секретно, для служебного пользования

d) Техническая, финансовая, юридическая

11. Что такое государственная тайна? (1 правильный ответ)

a) Публичные данные правительства

b) Финансовые отчеты государства

c) Образовательные материалы

d) Информация, защищаемая государством от разглашения

12. Какое из перечисленных является примером информационного преступления? (1 правильный ответ)

a) Нарушение трудового законодательства

b) Нарушение экологических норм

c) Хакерская атака на сервер

d) Несоблюдение налоговых правил

13. Какова роль политики информационной безопасности в организации? (1 правильный ответ) a) Управление персоналом

b) Контроль финансов

c) Определение процедур защиты информации

d) Разработка маркетинговых стратегий

14. Какова модель интеграции информационной безопасности в деятельность организации? (1 правильный ответ) a) Разработка программного обеспечения

b) Проведение финансового аудита

c) Включение процессов защиты в основные бизнес-процессы

d) Обучение сотрудников продажам

15. Что такое уязвимость информации? (1 правильный ответ)

a) Законодательный акт

b) Сертификат безопасности

c) Программное обеспечение для защиты

d) Слабое место, которое может быть использовано для атаки

16. Какие методы оценки уязвимостей существуют? (Несколько правильных ответов)

a) Финансовый аудит

b) Анализ рисков

c) Тестирование на проникновение

d) Разработка кода

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов) a) Резервное копирование
b) Сетевые атаки

c) Социальная инженерия

d) Физический доступ

18. Как классифицировать угрозы по их системным характеристикам? (1 правильный ответ)
a) Финансовые, юридические, административные

b) Внешние, внутренние, случайные

c) Технические, программные, аппаратные

d) Плановые, внеплановые, периодические

19. Какие меры предотвращения угроз информационной безопасности существуют? (Несколько правильных ответов) a) Разработка маркетинговых стратегий
b) Антивирусное ПО

c) Межсетевые экраны

d) Шифрование

20. Что регулируют нормативные акты в области защиты информации? (1 правильный ответ)
a) Трудовые отношения

b) Правила и процедуры защиты информации

c) Производственные процессы

d) Образовательные программы

21. Какой международный стандарт применяется в области информационной безопасности? (1 правильный ответ) a) ISO 9001
b) IEEE 802.11

c) ISO/IEC 27001

d) ISO 14001

22. Какие документы входят в систему сертификации РФ по защите информации? (Несколько правильных ответов) a) Нормативные акты
b) Финансовые отчеты

c) Стандарты

d) Сертификаты соответствия

23. Какие программные средства используются для защиты информации? (Несколько правильных ответов) a) Текстовые редакторы

b) Антивирусы

c) Системы обнаружения вторжений

d) Браузеры

24. Какие меры защиты реализуются в автоматизированных системах? (Несколько правильных ответов) a) Аутентификация

b) Шифрование

c) Планирование

d) Контроль доступа

25. Что такое инженерно-техническая защита объектов информатизации? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Резервное копирование

c) Физическая защита объектов и оборудования

d) Обучение персонала

26. Какие принципы работы с кадрами применяются для обеспечения информационной безопасности? (Несколько правильных ответов) a) Обучение

b) Контроль

c) Разработка программ

d) Проверка персонала

27. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов) a) Планирование

b) Реализация

c) Финансовый аудит

d) Корректировка

28. Какие российские стандарты регулируют защиту информации? (1 правильный ответ)

a) ГОСТ Р ИСО 9001

b) ГОСТ Р ИСО/МЭК 27001

c) ГОСТ Р 52001

d) ГОСТ Р 14001

29. Что такое конфиденциальная информация? (1 правильный ответ)

a) Публичные данные

b) Информация, доступ к которой ограничен

c) Финансовые отчеты

d) Учебные материалы

30. Какие методы анализа угроз информационной безопасности существуют? (Несколько правильных ответов) a) Моделирование угроз

b) Финансовый аудит

c) Анализ рисков

d) Тестирование на проникновение

Вариант 3

1. Что такое информационные процессы в контексте информационной безопасности? (1 правильный ответ)

a) Процессы разработки программного обеспечения

b) Процессы создания, обработки, передачи и хранения информации

c) Процессы финансового учета

d) Процессы маркетингового анализа

2. Какие основные задачи информационной безопасности? (Несколько правильных ответов)

a) Обеспечение конфиденциальности

b) Увеличение скорости обработки данных

c) Обеспечение целостности

d) Обеспечение доступности

3. Как информационная безопасность влияет на национальную безопасность? (1 правильный ответ)

a) Регулирует экономические процессы

b) Контролирует транспортную систему

c) Защищает государственные интересы в информационной сфере

d) Управляет образовательной системой

4. Какие виды защищаемой информации существуют? (Несколько правильных ответов)

a) Персональные данные

b) Публичные новости

c) Государственная тайна

d) Коммерческая тайна

5. Какие источники угроз информационной безопасности существуют? (Несколько правильных ответов) a) Хакеры

b) Вирусы

c) Законодательные акты

d) Внутренние сотрудники

6. Что такое риск информационной безопасности? (1 правильный ответ)

a) Уровень защиты информации

b) Скорость обработки данных

c) Вероятность реализации угрозы с негативными последствиями

d) Объем хранимой информации

7. Какие этапы включает жизненный цикл информации ограниченного доступа? (1 правильный ответ)

a) Планирование, тестирование, внедрение

b) Анализ, проектирование, реализация

c) Разработка, контроль, аудит

d) Создание, обработка, передача, хранение, уничтожение

8. В чем заключается принцип доступности информации? (1 правильный ответ)

a) Хранение данных на сервере

b) Уничтожение устаревших данных

c) Обеспечение своевременного доступа для авторизованных пользователей

d) Шифрование информации

9. Что такое конфиденциальная информация? (1 правильный ответ)

a) Публичные данные

b) Финансовые отчеты

c) Информация, доступ к которой ограничен

d) Учебные материалы

10. Как классифицировать информацию по видам тайны? (Несколько правильных ответов) a) Государственная

b) Техническая

c) Служебная

d) Персональная

11. Какие степени секретности существуют для информации? (1 правильный ответ)

a) Высокая, средняя, низкая

b) Публичная, ограниченная, закрытая

c) Совершенно секретно, секретно, для служебного пользования

d) Техническая, финансовая, юридическая

12. Какое из перечисленных является примером преступления в сфере информации? (1 правильный ответ)

a) Нарушение трудового законодательства

b) Нарушение экологических норм

c) Фишинговая атака

d) Несоблюдение налоговых правил

13. Что такое политика информационной безопасности организации? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Финансовый отчет

c) Документ, определяющий правила защиты информации

d) Учебная программа

14. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов) a) Планирование

b) Финансовый аудит

c) Реализация

d) Корректировка

15. Что подразумевается под уязвимостью информации? (1 правильный ответ)

a) Программное обеспечение для защиты

b) Законодательный акт

c) Слабое место, которое может быть использовано для атаки

d) Сертификат безопасности

16. Какие методы используются для анализа угроз информационной безопасности? (Несколько правильных ответов) a) Анализ рисков

b) Моделирование угроз

c) Разработка кода

d) Тестирование на проникновение

17. Какие методы несанкционированного доступа к информации существуют? (Несколько правильных ответов) a) Социальная инженерия

b) Сетевые атаки

c) Резервное копирование

d) Физический доступ

18. Как классифицировать угрозы по их воздействию на информацию? (1 правильный ответ)

a) Технические, программные, аппаратные

b) Угрозы конфиденциальности, целостности, доступности

c) Финансовые, юридические, административные

d) Плановые, внеплановые, периодические

19. Какие меры защиты информации существуют? (Несколько правильных ответов) a) Антивирусное ПО

b) Межсетевые экраны

c) Разработка маркетинговых стратегий

d) Шифрование

20. Какова роль законодательных актов в обеспечении информационной безопасности? (1 правильный ответ) a) Регулирование трудовых отношений

b) Контроль качества продукции

c) Установление правил защиты информации

d) Управление образовательными процессами

21. Какой российский стандарт регулирует защиту информации? (1 правильный ответ)

a) ГОСТ Р ИСО 9001

b) ГОСТ Р 52001

c) ГОСТ Р ИСО/МЭК 27001

d) ГОСТ Р 14001

22. Что такое сертификация в области информационной безопасности в РФ? (1 правильный ответ)

a) Разработка программного обеспечения

b) Финансовый аудит

c) Подтверждение соответствия средств защиты стандартам

d) Обучение персонала

23. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов) a) Аутентификация

b) Шифрование

c) Планирование

d) Контроль доступа

24. Какие программно-аппаратные средства используются для защиты информации? (Несколько правильных ответов) a) Межсетевые экраны

b) Антивирусы

c) Текстовые редакторы

d) Системы обнаружения вторжений

25. Что такое внутриобъектовый режим в контексте информационной безопасности? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Меры контроля доступа на объекте

c) Резервное копирование

d) Обучение персонала

26. Какие принципы лежат в основе организационно-распорядительной защиты? (Несколько правильных ответов) a) Законность

b) Системность

c) Скорость

d) Комплексность

27. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов) a) Угрозы

b) Уязвимости

c) Финансовые ограничения

d) Сбои оборудования

28. Какие носители защищаемой информации существуют? (Несколько правильных ответов) a) Жесткие диски

b) Бумажные документы

c) Рекламные буклеты

d) Флеш-накопители

29. Что такое государственная тайна? (1 правильный ответ)

a) Публичные данные правительства

b) Финансовые отчеты государства

c) Информация, защищаемая государством от разглашения

d) Образовательные материалы

30. Какие методы анализа рисков информационной безопасности существуют? (Несколько правильных ответов) a) Анализ рисков

b) Моделирование угроз

c) Финансовый аудит

d) Тестирование на проникновение

Вариант 4

1. Дайте определение информационной безопасности как дисциплины. (1 правильный ответ)

a) Наука о разработке программного обеспечения

b) Наука о финансовом учете

c) Наука о защите информации от несанкционированного доступа и угроз

d) Наука о маркетинговом анализе

2. Какие объекты входят в сферу информационной безопасности? (Несколько правильных ответов) a) Информационные системы

b) Транспортные средства

c) Базы данных

d) Серверы

3. Как информационная безопасность связана с государственной безопасностью? (1 правильный ответ)

a) Регулирует экономические процессы

b) Контролирует транспортную инфраструктуру

c) Управляет образовательной системой

d) Защищает государственные интересы в информационной сфере

4. Какие источники защищаемой информации существуют? (Несколько правильных ответов) a) Базы данных

b) Рекламные буклеты

c) Серверы

d) Публичные новости

5. Какие факторы влияют на информацию в автоматизированных системах? (Несколько правильных ответов) a) Угрозы

b) Уязвимости

c) Финансовые ограничения

d) Сбои оборудования

6. Что такое угроза безопасности информации? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Законодательный акт

c) Потенциальное событие, способное нанести ущерб информации

d) Сертификат безопасности

7. Какие этапы включает жизненный цикл конфиденциальной информации? (1 правильный ответ)

a) Планирование, тестирование, внедрение

b) Создание, обработка, передача, хранение, уничтожение

c) Анализ, проектирование, реализация

d) Разработка, контроль, аудит

8. В чем заключается принцип целостности информации? (1 правильный ответ)

a) Сохранение данных на сервере

b) Уничтожение устаревших данных

c) Обеспечение неизменности и достоверности данных

d) Шифрование информации

9. Как обеспечивается доступность информации в системах? (1 правильный ответ)

a) Увеличение скорости передачи данных

b) Своевременный доступ для авторизованных пользователей

c) Резервное копирование

d) Анализ уязвимостей

10. Как классифицировать информацию по степеням конфиденциальности? (1 правильный ответ) a) Высокая, средняя, низкая

b) Публичная, ограниченная, закрытая

c) Совершенно секретно, секретно, для служебного пользования

d) Техническая, финансовая, юридическая

11. Что такое конфиденциальная информация? (1 правильный ответ)

a) Публичные данные

b) Финансовые отчеты

c) Учебные материалы

d) Информация, доступ к которой ограничен

12. Какое из перечисленных является примером информационного преступления? (1 правильный ответ)

a) Нарушение трудового законодательства

b) Вредоносное ПО

c) Нарушение экологических норм

d) Несоблюдение налоговых правил

13. Какова цель разработки политики информационной безопасности?

(1 правильный ответ)
a) Управление персоналом
b) Контроль финансов
c) Определение правил и процедур защиты информации
d) Разработка маркетинговых стратегий

14. Каков процесс интеграции информационной безопасности в организацию? (1 правильный ответ)
a) Разработка программного обеспечения
b) Проведение финансового аудита
c) Включение процессов защиты в основные бизнес-процессы
d) Обучение сотрудников продажам

15. Что такое уязвимость в информационной безопасности? (1 правильный ответ)
a) Программное обеспечение для защиты
b) Законодательный акт
c) Слабое место, которое может быть использовано для атаки
d) Сертификат безопасности

16. Какие методики анализа рисков информационной безопасности существуют? (Несколько правильных ответов) a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов) a) Сетевые атаки
b) Социальная инженерия
c) Резервное копирование
d) Физический доступ

18. Как классифицировать угрозы по их источникам и типам? (1 правильный ответ)
a) Технические, программные, аппаратные
b) Внешние, внутренние, случайные
c) Финансовые, юридические, административные
d) Плановые, внеплановые, периодические

19. Какие меры противодействия угрозам информационной безопасности существуют? (Несколько правильных ответов) a) Антивирусное ПО
b) Межсетевые экраны
c) Разработка маркетинговых стратегий
d) Шифрование

20. Какие нормативные акты регулируют защиту информации в РФ? (1 правильный ответ)

a) Трудовой кодекс РФ

b) Гражданский кодекс РФ

c) Федеральный закон «Об информации, информационных технологиях и о защите информации»

d) Налоговый кодекс РФ

21. Какой международный стандарт применяется в области информационной безопасности? (1 правильный ответ) a) ISO 9001

b) IEEE 802.11

c) ISO/IEC 27001

d) ISO 14001

22. Какие документы входят в систему сертификации РФ по защите информации? (Несколько правильных ответов) a) Нормативные акты

b) Финансовые отчеты

c) Стандарты

d) Сертификаты соответствия

23. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов) a) Аутентификация

b) Шифрование

c) Планирование

d) Контроль доступа

24. Какие программные средства используются для защиты информации? (Несколько правильных ответов) a) Антивирусы

b) Текстовые редакторы

c) Системы обнаружения вторжений

d) Браузеры

25. Что такое инженерно-техническая защита объектов информатизации? (1 правильный ответ)

a) Программное обеспечение для защиты данных

b) Резервное копирование

c) Физическая защита объектов и оборудования

d) Обучение персонала

26. Какие принципы лежат в основе организационно-распорядительной защиты информации? (Несколько правильных ответов) a) Законность

b) Системность

c) Скорость

d) Комплексность

27. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов) a) Планирование
b) Реализация
c) Финансовый аудит
d) Корректировка

28. Какие российские стандарты регулируют защиту информации? (1 правильный ответ)
a) ГОСТ Р ИСО 9001
b) ГОСТ Р 52001
c) ГОСТ Р ИСО/МЭК 27001
d) ГОСТ Р 14001

29. Какие носители защищаемой информации существуют? (Несколько правильных ответов) a) Жесткие диски
b) Бумажные документы
c) Рекламные буклеты
d) Флеш-накопители

30. Какие методы анализа угроз информационной безопасности существуют? (Несколько правильных ответов) a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

Вариант 1		**Вариант 2**		**Вариант 3**		**Вариант 4**	
Вопрос	**Правильный ответ**	**Вопрос**	**Правильный ответ**	**Вопрос**	**Правильный ответ**	**Вопрос**	**Правильный ответ**
1	b	1	c	1	b	1	c
2	c	2	a, c, d	2	a, c, d	2	a, c, d
3	c	3	d	3	c	3	d
4	a, c	4	a, b, d	4	a, c, d	4	a, c
5	a, b, d	5	b, c, d	5	a, b, d	5	a, b, d
6	d	6	b	6	c	6	c
7	b	7	c	7	d	7	b
8	c	8	b	8	c	8	c
9	c	9	c	9	c	9	b
10	a, c, d	10	c	10	a, c, d	10	c
11	b	11	d	11	c	11	d

12	b	12	c	12	c	12	b
13	d	13	c	13	c	13	c
14	b	14	c	14	a, c, d	14	c
15	c	15	d	15	c	15	c
16	a, b	16	b, c	16	a, b, d	16	a, b, d
17	a, b, d	17	b, c, d	17	a, b, d	17	a, b, d
18	b	18	b	18	b	18	b
19	a, b, d	19	b, c, d	19	a, b, d	19	a, b, d
20	b	20	b	20	c	20	c
21	b	21	c	21	c	21	c
22	a, c	22	a, c, d	22	c	22	a, c, d
23	b	23	b, c	23	a, b, d	23	a, b, d
24	a, b, d	24	a, b, d	24	a, b, d	24	a, c
25	a, b, d	25	c	25	b	25	c
26	b	26	a, b, d	26	a, b, d	26	a, b, d
27	a, b, d	27	a, b, d	27	a, b, d	27	a, b, d
28	a, b, d	28	b	28	a, b, d	28	c
29	b	29	b	29	c	29	a, b, d
30	a, b, d	30	a, c, d	30	a, b, d	30	a, b, d

Шкала оценки тестов

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

3. Оценочные средства для промежуточной аттестации и критерии оценки

Вопросы к экзамену

1. Основы Российского законодательства в области конфиденциальной информации.
2 Концепция IA*3.
3 Аудит информационной безопасности организации.
4 Внешний и внутренний аудит организации.
5 Конфиденциальная информация организации.
6 Криптографические методы защиты информации.

7 Персональные данные граждан.
8 Конфиденциальная информация банковской организации.
9 Общедоступные корпоративные информационные ресурсы.
10 Аудит конфиденциальных и персональных данных организации кредитно-финансовой системы РФ.
11 Стандарт безопасности Банка России.
12 Международный стандарт PCI DSS.
13 Специальные нормативные документы ФСТЭК.
14 Закон “О лицензировании отдельных видов деятельности” 99-ФЗ.
15 Закон “О персональных данных” 152-ФЗ.
16 ФЗ РФ от 29.07.2004 № 149-ФЗ О коммерческой тайне.
17 ФЗ РФ от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации.
18. ФЗ РФ от 27 декабря 2002 г. №184-ФЗ О техническом регулировании.

Критерии оценки

«Отлично» - за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; научнопонятийным аппаратом; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «отлично» предполагает грамотное и логичное изложение ответа, обоснование собственного высказывания с точки зрения известных теоретических положений.

«Хорошо» - обучающийся полно освоил учебный материал, владеет научнопонятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«Удовлетворительно» - обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«Неудовлетворительно» - обучающийся имеет разрозненные, бессистемные знания по разделу/теме, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Номер задания	Содержание вопроса	Правильный ответ	Компетенция
1.	Информационные технологии хранения, отбора и сортировки информации - это а) база данных б) электронные таблицы в) экспертные системы г) электронные редакторы	+: а) база данных	ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

2.	Информационные технологии обработки знаний - это а) база данных б) электронные таблицы в) экспертные системы г) электронные редакторы	+: в) экспертные системы	ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
3.	Информация, закодированная в пучке света, передается по сети с помощью кабеля а) витая пара б) телефонный в) коаксиальный г) оптико – волоконный	+: г) оптико – волоконный	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
4.	Топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу называется а) шина б) кольцо в) звезда г) смешанная	+: в) звезда	ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

5.	Домен – это а) часть адреса, определяющая адрес компьютера пользователя в сети б) название программы, для осуществления связи между компьютерами	+: а) часть адреса, определяющая адрес компьютера пользователя в сети	ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации

	в) название устройства, осуществляющего связь между компьютерами г) единица скорости информационного обмена		

6.	E-mail – это а) поисковая программа б) название почтового сервера в) почтовая программа г) обмен письмами в компьютерных сетях (электронная почта)	+: г) обмен письмами в компьютерных сетях (электронная почта)	ПК 2.4 Выполнять тестирование и отладку программного обеспечения.
7.	Задан адрес электронной почты в сети Интернет: user_name@mtu-net.ru. Каково имя домена верхнего уровня? а) ru; б) mtu-net.ru; в) mtu-net; г) user_name.	+: а) ru	ПК 2.4 Выполнять тестирование и отладку программного обеспечения.
8.	Задан адрес электронной почты в сети Интернет: user_name@mtu-net.ru. Каково имя владельца этого электронного адреса а) ru б) mtu-net.ru в) mtu-net	+: г) user_name	ПК 2.4 Выполнять тестирование и отладку программного обеспечения.

	г) user-name		
9.	Выберите корректный адрес электронной почты а) ivanpetrov@mail б) ivan_petrov.mail.ru в) ivan petrov.mail.ru г) ivan_petrov@mail.ru	+: г) ivan_petrov@mail.ru	ПК 2.4 Выполнять тестирование и отладку программного обеспечения.
10.	Задан адрес электронной почты в сети Интернет: fortuna@list.ru. Каково имя почтового сервера а) fortuna@list.ru	+: в) list.ru	ПК 2.4 Выполнять тестирование и отладку программного обеспечения.
	б) fortuna в) list.ru г) list.		
11.	Для просмотра WEB-страниц предназначены а) поисковые серверы б) браузеры в) телеконференции г) провайдеры	+: б) браузеры	ПК 3.8 Производить оценку информационной системы для выявления возможности ее модернизации.
12.	WWW – это а) название электронной почты б) совокупность Web – страниц, принадлежащих одному пользователю или организации	+: г) информационно – поисковая система сети Интернет	ПК 3.8 Производить оценку информационной системы для выявления возможности ее модернизации.

	в) доступ к документам на компьютерах, подключённых к сети Интернет г) информационно – поисковая система сети Интернет		
13.	Расположите единицы измерения в порядке их возрастания а) Гбайт б) Тбайт в) Мбайт г) Байт д) Кбайт	+: 1) Г) Байт 2) Д) Кбайт 3) В) Мбайт 4) А) Гбайт 5) Б) Тбайт	ПК 3.8 Производить оценку информационной системы для выявления возможности ее модернизации.
14.	По назначению виды информационных систем выделяют а) информационно-управляющие, информационнопоисковые б) экономические, математические, офисные, управленческие	+: а) информационноуправляющие, информационно-поисковые +: в) системы поддержки принятия решений, информационносправочные *	ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации

	в) системы поддержки принятия решений, информационно-справочные г) одиночные, групповые, корпоративные		

15.	К видам информационных технологий относятся а) информационные технологии обработки данных б) информационные технологии распределения ресурсов в) информационные технологии проведения экономических расчетов г) информационные технологии экспертных систем	+: а) информационные технологии обработки данных; г) информационные технологии экспертных систем*	ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации

Критерии оценки:

Тест оценивается по пяти бальной шкале следующим образом: стоимость каждого вопроса 1 балл. За правильный ответ студент получает 1 балл. За неверный ответ или его отсутствие баллы не начисляются.

Оценка «отлично» выставляется студенту, если он правильно ответил на 90-100% от общего числа вопросов тестовых заданий.

Оценка «хорошо» выставляется студенту, если он правильно ответил на 70-89% от общего числа вопросов тестовых заданий.

Оценка «удовлетворительно» выставляется студенту, если он правильно ответил на 50-69% от общего числа вопросов тестовых заданий.

Оценка «неудовлетворительно» выставляется студенту, если он правильно ответил менее чем на 50% от общего числа вопросов тестовых заданий.