

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

Код модуля	Модуль
<i>1156888(1)</i>	<i>Государственная итоговая аттестация</i>

Екатеринбург

Оценочные материалы по итоговой (государственной итоговой) аттестации составлены авторами:

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр "Информационная безопасность"
2	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ

Т.Г. Комарова

1. СТРУКТУРА И ОБЪЕМ ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

В рамках государственной итоговой аттестации проверяется уровень сформированности результатов освоения образовательной программы – компетенций

Таблица 1.

№ п/п	Перечень государственных аттестационных испытаний	Объем государственных аттестационных испытаний в зачетных единицах	Форма итоговой промежуточной аттестации по ГИА
1	Подготовка к сдаче и сдача государственного экзамена	1	Экзамен
2	Подготовка к процедуре защиты и защита выпускной квалификационной работы	8	Экзамен

2. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – КОМПЕТЕНЦИИ НА ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

2.1 Для государственных аттестационных испытаний применяются утвержденные на кафедре/институте критерии (признаки) оценивания учебных достижений студентов по образовательной программе на соответствие указанным в табл.2 результатам освоения образовательной программы – компетенциям.

Таблица 2

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений обучающихся на соответствие компетенциям
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения по компетенциям на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения.

	Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.
--	--

2.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении государственных аттестационных испытаний) используется универсальная шкала.

Таблица 3

Шкала оценивания достижения результатов обучения (индикаторов) по компетенциям по уровням

Характеристика уровней достижения результатов обучения (индикаторов) по компетенциям				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (индикаторов) по компетенциям	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Все результаты обучения (индикаторы) по компетенции достигнуты в полном объеме, замечаний нет, компетенция сформирована	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) по компетенции в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) по компетенции достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения по компетенции не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно но (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения по компетенции не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ИТоговым (ГОСУДАРСТВЕННЫМ ИТоговым) АТТЕСТАЦИОННЫМ ИСПЫТАНИЯМ

3.1. Перечень вопросов для подготовки к сдаче государственного экзамена

1. Преобразование Фурье и его свойства. Применение к анализу линейных систем

2. Преобразование случайного процесса в линейных системах: преобразование функции корреляции, спектра
3. Задача выделения сигнала из смеси с шумом, понятие и критерии оптимальной фильтрации; согласованная фильтрация и согласованные фильтры. "Сжатие" сигналов.
4. Информационные основы передачи сообщений. Пропускная способность канала связи. Кодирование источников и каналов связи, виды помехоустойчивых кодов
5. Принципы помехоустойчивого кодирования. Классификация помехоустойчивых кодов. Линейные блочные коды.
6. Быстрое преобразование Фурье (БПФ). Алгоритмы БПФ с прореживанием по времени и частоте. Коэффициент ускорения вычисления.
7. Общая структурная схема системы передачи информации. Основная терминология, назначение основных устройств.
8. Классификация компьютерных сетей. Топологии. Среда передачи данных.
9. Сетевой уровень в сети Интернет. IP-протокол. Адресация, IP-адрес, подсети, адресные пространства. Классы IP-адресов, зарезервированные адреса. Назначение адресов, методы CIDR и NAT. Управляющие протоколы сети Интернет: ICMP, ARP, RARP, BOOTP, DHCP. Недостатки IPv4, протокол IPv6. Формат кадра протокола IP
10. Эксплуатация автоматизированных систем в защищенном исполнении. Общие положения по эксплуатации аппаратуры, оборудования, расходных материалов и программного обеспечения. Организационные и технические мероприятия по эксплуатации, их содержание и общая характеристика. Понятие, содержание и виды технического обслуживания
11. Администрирование и безопасность АИС в защищенном исполнении. Планирование и организация работы пользователей. Обеспечение целостности и сохранности информационной базы. Управление функционированием средств защиты информации. Технологические процедуры парольной политики, использования других средств идентификации и аутентификации, криптографических средств. Мониторинг, контроль, аудит безопасности в АИУС.
12. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки. Степени секретности сведений, составляющих государственную тайну, гриф секретности и реквизиты их носителей. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Правовой режим защиты государственной тайны. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Система контроля за состоянием защиты государственной тайны. Ответственность за нарушения правового режима защиты государственной тайны.
13. Правовой режим защиты служебной, коммерческой тайны и персональных данных. Принципы защиты информации ограниченного доступа. Режим защиты профессиональных тайн; основные виды тайн; установленные требования и правила защиты.

14. Лицензирование и техническое регулирование деятельности в сфере защиты информации; организационная структура и общая характеристика систем лицензирования. Цели и принципы сертификации. Органы добровольной и обязательной сертификации; их аккредитация. Системы сертификации в сфере защиты информации; особенности разработки, производства и эксплуатации средств защиты информации.

15. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Характеристика объективной стороны преступлений, предусмотренных гл. 28 УК РФ. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации, нейтрализации средств ее защиты. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ.

16. Реализация технологии разграничения доступа в ОС Windows. Понятие механизмов идентификации и аутентификации, их реализация в ОС Windows. Хранение парольной информации в ОС Windows. Алгоритм сетевой аутентификации в ОС Windows.

17. Возможности СЗИ по криптографическому преобразованию информации. Способы формирования ключевой информации. Контроль и удаление «технологического мусора». Организация виртуальных логических дисков. Структура файл-образа виртуального зашифрованного диска. Способы формирования электронной подписи. Основные возможности СКЗИ «КриптоПро CSP».

18. Аудит безопасности компьютерных систем. Цели, стандарты, подходы. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

19. Характеристика технических каналов утечки информации, возникающих при использовании средств вычислительной техники. Особенности образования каналов утечки компьютерной информации. Каналы утечки конфиденциальной информации при ее клавиатурном вводе в ЭВМ. Виды и возможности аппаратного перехвата клавиатурного ввода.

20. Способы перехвата компьютерной информации при ее выводе на печать. Побочные электромагнитные и акустические излучения при печати на струйных и лазерных принтерах. Каналы утечки информации из компьютерных мониторов и видеоадаптеров. Меры по снижению электромагнитной утечки из СВТ. Пассивные компоненты, используемые техническими разведками для увеличения уровня побочных излучений. Утечка информации, передаваемой по проводным каналам ЛВС.

21. Высокочастотное навязывание в телефонных системах. Механизмы взаимодействия акустического сигнала с высокочастотным сигналом навязывания. Методика оценки опасности канала утечки за счет высокочастотного навязывания. Аппаратура для проведения измерений. Параметры аппаратуры, определяющие чувствительность метода.

3.2. Перечень тем выпускных квалификационных работ

1. Сбор статистики по заданному worklist'у. Распределение длин паролей, распределение по наборам символов, определение случайности пароля, языка и т.д. Определение популярных паттернов
2. Подобрать оптимальную методику взлома паролей в условиях, когда нам известна скорость перебора на имеющемся оборудовании, и ограничено время на перебор
3. Разработка защищённой контейнеризированной среды в КИИ
4. Криминалистическое исследование ФС ReFS и разработка ПО по извлечению информации с нее
5. Разработка лабораторного пособия по анализу кода на безопасность
6. Разработка сниффера и исследование трафика
7. Экспертно-аналитическая оценка технико-экономической эффективности обеспечения ИБ