Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной деятельности
_______________ С.Т. Князев
«_07_» июля 2021 г.

ПРОГРАММА ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ (ГИА)

Код программы
10.04.01/22.01

Екатеринбург, 2021

Программа государственной итоговой аттестации составлена авторами:

№	ФИО	Ученая степень, ученое звание	Должность	Кафедра
1	Поршнев Сергей Владимирович	д.т.н., профессор	профессор	Учебно-научный центр «Информационной безопасности»
2	Пономарева Ольга Алексеевна		Старший преподаватель	Учебно-научный центр «Информационной безопасности»

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Цель государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовленности обучающегося, осваивающего образовательную программу магистратуры выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования (требованиям образовательного стандарта, разрабатываемого и утверждаемого университетом самостоятельно) и ОП по направлению подготовки высшего образования, разработанной на основе образовательного стандарта. В рамках государственной итоговой аттестации проверяется уровень сформированности следующих результатов освоения образовательной программе, заявленных в ОХОП.

1.2. Структура государственной итоговой аттестации:

- государственный экзамен;
- защита выпускной квалификационной работы в форме магистерской диссертации

.

1.2.1.Форма проведения государственного экзамена

Форма государственного экзамена: устный

1.3. Трудоемкость государственной итоговой аттестации:

Общая трудоемкость государственной итоговой аттестации составляет 9 з.е.

1.4. Время проведения государственной итоговой аттестации

Итоговая государственная аттестация проводится в сроки, установленные учебно-производственным графиком, утвержденным в УрФУ

1.5.Требования к процедуре государственной итоговой аттестации.

Требования к порядку планирования, организации и проведения ГИА, к структуре и форме документов по организации ГИА сформулированы в утвержденной в УрФУ документированной процедуре «Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры» (СМК-ПВД-6.1-01-65-2015), введенной в действие приказом ректора от 01.12.2015 №899/03.

1.6. Требования к оцениванию результатов освоения ОП в рамках государственной итоговой аттестации

Объективная оценка уровня соответствия результатов обучения требованиям к освоению ОП обеспечивается системой разработанных критериев (показателей) оценки освоения знаний, сформированности умений и опыта выполнения профессиональных задач.

Количество баллов	Критерии оценки
5 (отлично)	Полный безошибочный ответ, в том числе на дополнительные вопросы членов экзаменационной комиссии. Студент должен правильно определять понятия и категории, выявлять основные тенденции и противоречия, свободно ориентироваться в теоретическом и практическом материале.
4 (хорошо)	Правильные и достаточно полные, не содержащие ошибок и упущений ответы. Оценка может быть снижена в случае затруднений студента при ответе на дополнительные вопросы членов экзаменационной комиссии. При выполнении практической работы и решении профессиональных задач допущены отдельные несущественные ошибки.
3 (удовлетворительно)	Недостаточно полный объем ответов, наличие ошибок и некоторых пробелов в знаниях
2 (неудовлетворительно)	Неполный объем ответов, наличие ошибок и пробелов в знаниях.

2. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Тематика государственного экзамена

Список примерных экзаменационных вопросов и заданий, соответствующих ОХОП, и выявляющих сформированность комплекса результатов обучения:

1. Линейные системы. Сигналы и системы. Условия линейности. Статическая характеристика и передача гармонических сигналов. Примеры линейных и нелинейных систем.
2. Преобразование Фурье и его свойства. Применение к анализу линейных систем
3. Свойства преобразования Фурье. Линейность. Свойства фазовой характеристики. Периодичность. Сжатие и расширение.
4. Преобразование случайного процесса в линейных системах: преобразование функции корреляции, спектра.
5. Задача выделения сигнала из смеси с шумом, понятие и критерии оптимальной фильтрации; согласованная фильтрация и согласованные фильтры. "Сжатие" сигналов.
6. Информационные основы передачи сообщений. Пропускная способность канала связи. Кодирование источников и каналов связи, виды помехоустойчивых кодов.
7. Принципы помехоустойчивого кодирования. Классификация помехоустойчивых кодов. Линейные блочные коды.
8. Быстрое преобразование Фурье (БПФ). Алгоритмы БПФ с прореживанием по времени и частоте. Коэффициент ускорения вычисления.
9. Общая структурная схема системы передачи информации. Основная терминология, назначение основных устройств.
10. Классификация компьютерных сетей. Топологии. Среда передачи данных.
11. 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.
12. 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.

13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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».
20. 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.
21. 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.
22. 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.

23. 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.
24. Рекурсивные и нерекурсивные фильтры. Специальные фильтры. Фильтры с амплитудно-частотной характеристикой произвольной формы. Коррекция частотной характеристики. Оптимальная фильтрация.
25. Дискретное преобразование Фурье (ДПФ). Действительное ДПФ. Базисные функции ДПФ. Синтез сигнала при помощи обратного ДПФ. Анализ сигналов на основе ДПФ. Дуальность ДПФ.

2.2. Тематика выпускных квалификационных работ

1 Исследование потенциально опасных программ по виду, статистике и последовательности системных вызовов.
2 Методика безопасного динамического исследования кода неизвестных и потенциально опасных исполняемых программ.
3 Методика статического исследования кода неизвестных и потенциально опасных исполняемых программ.
4 Исследование современных механизмов самозащиты вредоносных программ. Деобфускация
5 Новые и нестандартные способы внедрения и запуска ВП.
6 Разработка алгоритмов и программ–анализаторов для выявления ВП функционального назначения (шпионских программ, вирусов и др.).
7 Разработка принципов современной классификации ВП.
8 Исследование механизмов вирусного инфицирования, а также внедрения, запуска и сокрытия ВП в ОС Linux, FreeBSD, MacOS X.
9 Автоматическое выявление образцов информационно–психологического оружия (звуковые файлы).
10 Автоматическое выявление образцов информационно–психологического оружия (видеофайлы).
11 Исследование опасностей порчи аппаратуры вредоносными программами.
12 Программы–шутки и программы–мистификаторы: сбор, описание, классификация, оценка опасности.
13 Криминалистическое исследование системного реестра с извлечением, интерпретацией и занесением данных в табличные формы.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

3.1. Рекомендуемая литература

3.1.1. Основная литература

1. Бакланов В.В., Пономарев М.Э. Опасная компьютерная информация : учеб. пособие / - Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2007. -146 с.

2. Бакланов В. В. Защита компьютерной информации в клиентских приложениях: учеб. пособие / В. В. Бакланов. – Екатеринбург: ГОУ ВПО УГТУ - УПИ, 2006. – 80 с.
3. Барсуков В. С., Водолазский В. В. Современные технологии безопасности. Интегральный подход. М.: «Нолидж», 2000, 496 с.
4. Барсуков В.С. Обеспечение информационной безопасности. М.: ТЭК, 1996.
5. Бэндл Д. Защита и безопасность в сетях Linux. Для профессионалов / Д. Бэндл. СПб.: Питер, 2002. 480 с.
6. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие/ Под ред. профессора Н.Г.Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2001. 88 с.
7. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. — М.: Гелиос АРВ, 2002. — 368 с.
8. Гайдамакин Н.А. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Законодательные акты РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ / авт. – сост. Н.А.Гайдамакин. Екатеринбург: Издательский дом «Гриф», 2006. 658 с.
9. Гайдамакин Н.А. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Ведомственные нормативные правовые акты и руководящие документы / авт. – сост. Н.А.Гайдамакин. Екатеринбург: Издательский дом «Гриф», 2006. 740 с.
10. Гарсиа М. Проектирование и оценка систем физической защиты. Пер. с англ. –М.: ООО «Издательство АСТ», 2002, -386 с.
11. Гедзберг Ю.М. Охранное телевидение. М.: Горячая линия – Телеком, 2005. 312 с.
12. ГОСТ Р 50862-96. Сейфы и хранилища ценностей. Требования и методы испытаний и огнестойкость. М.: Госстандарт России, 1996.
13. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М.: Госстандарт России, 1996.
14. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.
15. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. М., 1992.
16. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992
17. Гражданский кодекс РФ. Часть четвертая. ТК Велби, Изд-во Проспект, 2007. 176 с.
18. Гук М. Дисковая подсистема ПК. –СПб.: Питер, 2001. –336 с.
19. Цифровая обработка сигналов. Автор Ричард Лайонс. Издательство Бином-пресс. Год 2013. Количество страниц 656.
20. Цифровая обработка сигналов. Авторы Рональд В. Шафер, Алан В. Оппенгейм. Издательство Техносфера. Год 2012. Страниц 1048.
21. Цифровая обработка сигналов. Автор Александр Сергиенко. Издательство БХВ-Петербург. Год 2013. Страниц 768.
22. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников. Автор Стивен Смит. Издательство: Додэка-XXI. Год 2008. Страниц 720.
23. Современные операционные системы. 4-е издание Автор: Таненбаум Э., Бос Х. Издательство: Питер Год: 2015 Страниц: 1120
24. Архитектура компьютера. 6-е издание. Автор: Таненбаум Э., Остин Т. Издательство: Питер. Год 2016. Страниц 816.

25. Ядро Cortex-M3 компании ARM. Полное руководство. Автор Джозеф Ю. Издательство: Додэка-XXI. Год 2015. Страниц 552.
26. Современные микроконтроллеры. Архитектура, программирование, разработка устройств. Автор Магда Ю. Издательство ДМК Пресс. Год выпуска 2012. Количество страниц 224.
27. UNIX. Профессиональное программирование. 3-е издание. Автор Раго С., Стивенс У. Издательство Символ-Плюс. Год 2014.
28. Операционные системы. Разработка и реализация. 3-е издание. Автор: Таненбаум Э., Вудхалл А. Издательство: Питер, Год 2007. Страниц: 704.
29. Разработка приложений в среде Linux. Автор: Троан. Э., Джонсон М. Издательство: Мильямс. Год выпуска 2007. Количество страниц 544.
30. Александр Косяков, Уильям Н. Свит,Сэмюэль Дж. Сеймур, Стивен М. Бимер, Системная инженерия. Принципы и практика, Издательство ДМК Пресс, 2014.
31. ГОСТ Р ИСО/МЭК 15288-2005 «Системная инженерия. Процессы жизненного цикла систем» - базовый стандарт в области проектирования систем.
32. Форсайт Д.А., Понс Ж. Компьютерное зрение. Современный подход.: Пер. с англ. – М.: издательский дом «Вильямс», 2004 – 928 с.
33. Гонсалес Р., Вудс Р. Цифровая обработка изображений / Пер. с англ. под ред. П.А. Чочиа – М.: ТЕХНОСФЕРА. 2005 1070 с.
34. Шапиро Л., Стокман Дж.. Компьютерное зрение / Пер. с англ. под ред. С.М.Соколова.- М.: БИНОМ. Лаборатория знаний. 2006 752 с
35. Лабунец, В. Г. Цифровая обработка цветных и гиперспектральных изображений / Лабунец В.Г.УМК 2008 .УМК
36. Рубин, А. Б. Биофизика. 2-е изд. - М.: МГУ, 1999. - 448 с.
37. Кореневский Н.А., Попечителев Е.П. Биотехнические системы медицинского назначения: учеб. пособие для вузов / Старый Оскол: ТНТ, 2013. 685 с.
38. Рангайян Р. М. Анализ биомедицинских сигналов: учеб. пособие / М.: Физматлит, 2010. 439 с.
39. Соловьева О.Э. и др. Математическое моделирование живых систем. Учебное пособие, УрФУ, Екатеринбург, 2013
40. Курашов В.И. Начала философии науки: Учебное пособие. – М., КДУ, 2007.
41. История и философия науки /под редакцией А.С. Мамзина. – СПб., 2008.
42. Финогентов В.Н. Философия науки. – Орел. 2011.
43. Финогентов В.Н. Введение в философию. – Орел. 2010.
44. Мамчур Е.А. Образы науки в современной культуре. – М., 2008.
45. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения : учеб. пособие для втузов / Вентцель Е. С., Овчаров Л. А. - 5-е изд., стер. - М.: Кнорус, 2014. - 441 с.
46. Биология человека и животных для инженеров : учеб. пособие для вузов / Гафиятуллина Г. Ш., Каплунова О. А., Кондрашев А. В. [и др.] ; ред. Омельченко В. П. - М. : Высш. шк., 2010. - 566 с.
47. Ключарев П. Г., Жуков Д. А. Введение в теорию алгоритмов : учеб. пособие / Ключарев П. Г., Жуков Д. А. ; МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2012. - 37 с.
48. Гмурман В.Е. Теория вероятностей и математическая статистика. - М.: Высшая школа, 1999. - 479 с.

3.1.2. Дополнительная литература

Операционные системы. Разработка и реализация. 3-е издание. Автор: Таненбаум Э.,

Вудхалл А. Издательство: Питер, Год 2007 Страниц: 704.

2. Разработка приложений в среде Linux. Автор: Троан. Э., Джонсон М. Издательство: Мильямс. Год выпуска 2007 Количество страниц 544.
3. Волькенштейн, М.В.. Биофизика. - М.:Наука, 1988. - 592 с. https://e.lanbook.com/book/3898
4. А.А. Хорев - Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки
5. Защита от утечки информации по техническим каналам Год выпуска: 2005 Автор: Г.А. Бузов, С.В. Калинин, А.В. Кондратьев Издательство: Горячая Линия - Телеком ISBN: 5-93517-204-6
6. Защита объектов и информации от технических средств разведки Год выпуска: 2002 Автор: Ю. К. Меньшаков Издательство: РГГУ ISBN: 5-7281-0487-8
7. Бендат Дж., Пирсол А. Прикладной анализ случайных данных. - М.: Мир, 1989.-540 с

3.2. Методические разработки

3.2. Программное обеспечение

Прикладное программное обеспечение общего назначения (MS PowerPoint, MS Word, MS Excel).

3.3. Базы данных, информационно-справочные и поисковые системы

http://lib.urfu.ru/ - ЗНБ УрФУ

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://www.nlr.ru - Российская национальная библиотека

http://www.rasl.ru - Библиотека Академии Наук

http://www.gpntb.ru - Государственная публичная научно-техническая библиотека

3.5.Электронные образовательные ресурсы

Портал информационно-образовательных ресурсов Уральского федерального университета: http://study.urfu.ru

Официальный сайт Института радиоэлектроники и информационных технологий: http://rtf.urfu.ru/

4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Компьютерный класс: 15 персональных ЭВМ, объединенных в локальную вычислительную сеть Ethernet. Минимальные требования к персональным компьютерам: платформа x86-64, тактовая частота центрального процессора не ниже 2 ГГц, оперативная память объемом не менее 2 Гбайт, жесткие магнитные диски с интерфейсом Serial ATA и емкостью не менее 500 Гбайт.
Персональный компьютер преподавателя с мультимедиа-проектором и экраном — 1 комплект.