

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Хабаровский институт инфокоммуникаций (филиал)
Федерального государственного бюджетного образовательного учреждения
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(ХИИК СибГУТИ)

СОГЛАСОВАНО

Директор ДИТ
Должность
ООО «МАСКОМ-ТЕХЛАЙН»
название организации
М.П. / Попов
(подпись/ Ф.И.О.) М.П.
г. Хабаровск



«25» 09 2024г.



УТВЕРЖДАЮ
И.о. директора

/Маслов Г.Ф./
2024 г.

ПРИНЯТО

на ученом совете ХИИК СибГУТИ
от «25» сентября 2024г. протокол № 2

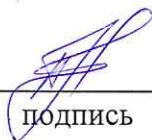
ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по направлению
11.03.02 Инфокоммуникационные технологии и системы связи,
Направленность (профиль) – Защищенные сети связи,
квалификация (степень) – бакалавр
очной и заочной форм обучения
на 2024-2025 уч. год

Хабаровск
2024 г.


Разработчик рабочей программы:

К.т.н., доцент кафедры ИТ


_____ / В.О. Прокопцев /
подпись


Рассмотрена на заседании кафедры 11 сентября 2024г., протокол № 2

И.о. зав. кафедрой ИТ


_____ / Р.М. Данилов /
подпись

Основная и дополнительная литература, указанная в п.6. рабочей программы, имеется в наличии в библиотеке университета и ЭБС.

Заведующий библиотекой


_____ / Д.С. Ерохова /
Подпись

СОДЕРЖАНИЕ

1. Введение	4
2. Цель и задачи государственной итоговой аттестации	4
3. Виды и объем государственной итоговой аттестации	4
4. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы.....	4
5. Перечень вопросов и заданий государственного экзамена (при наличии)	6
6. Содержание государственного экзамена	9
7. Учебно-методическое и информационное обеспечение государственного экзамена (при наличии).....	9
8. Материалы, определяющие процедуру оценивания результатов освоения образовательной программы с помощью государственного экзамена (при наличии)	12
9. Перечень тем выпускных квалификационных работ	12
10. Материалы, определяющие процедуру оценивания результатов освоения образовательной программы с помощью защиты ВКР	15
11. Материально-техническое и программное обеспечение государственной итоговой аттестации	17
12. Особенности проведения ГИА для лиц с ограниченными возможностями здоровья.....	18

1. Введение

Государственная итоговая аттестация (ГИА) является завершающим этапом процесса обучения и служит для результирующей оценки качества освоения обучающимся образовательной программы высшего образования по направлению 11.03.02 Инфокоммуникационные технологии и системы связи, направленность (профиль) – Защищенные сети связи. ГИА позволяет установить соответствие между требованиями к результатам освоения образовательной программы и фактическими знаниями, умениями и навыками выпускников, полученными в процессе обучения.

Государственная итоговая аттестация выпускника является обязательной и осуществляется после освоения образовательной программы в полном объеме. Проведение ГИА регулируется Порядком проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры, утвержденным приказом Минобрнауки России от 29 июня 2015 г. № 636, «Положением о проведении в СибГУТИ государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», утверждённый приказом СибГУТИ от 30.12.2022 года, а также федеральным государственным образовательным стандартом по направлению 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденным приказом от 19.09.2017г. №930.

Государственная итоговая аттестация может проводиться с применением дистанционных образовательных технологий.

2. Цель и задачи государственной итоговой аттестации

Цель государственной итоговой аттестации – установление соответствия уровня профессиональной подготовки выпускника требованиям федерального государственного образовательного стандарта высшего образования по направлению 11.03.02 Инфокоммуникационные технологии и системы связи (далее – ФГОС ВО).

Основные задачи ГИА:

- комплексная оценка уровня подготовки и знаний выпускника, необходимых для самостоятельного выполнения им профессиональных обязанностей на момент окончания вуза, в соответствии с критериями востребованности знаний и ФГОС ВО;
- контроль эффективности индивидуальных траекторий обучения и самостоятельной навигации студентов в информационных ресурсах;
- оценка соответствия обучающей технологии ее целевому назначению – подготовке выпускника новой формации.

3. Виды и объем государственной итоговой аттестации

Государственные аттестационные испытания включают:

- государственный экзамен;
- защиту выпускной квалификационной работы (в виде бакалаврской работы).

Объем (продолжительность):

- Подготовка к сдаче и сдача государственного экзамена 3 ЗЕ (2 недели),
- Выполнение и защита выпускной квалификационной работы; включая подготовку к процедуре защиты и процедуру защиты 6 ЗЕ (4 недели).

Сроки проведения: 6 недель 4 курса в очной форме обучения, 6 недель 5 курса в заочной форме обучения.

4. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

4.1. При сдаче государственного экзамена

УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою
------	--

	роль в команде
УК-5	Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
ОПК-1	Способен использовать положения, законы и методы естественных наук и математики для решения задач инженерной деятельности
ОПК-2	Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных
ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
ПК-1	Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных
ПК-3	Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

4.2. При защите выпускной квалификационной работы

УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК-10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

ОПК-4	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения
ПК-1	Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных
ПК-3	Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

5. Перечень вопросов и заданий государственного экзамена

1. ТЕОРИЯ СВЯЗИ

1. Процессы передачи информации. Системы и каналы связи.
2. Методы цифрового представления и передачи непрерывных сообщений в системах связи.
3. Монопозиционная и многопозиционная модуляции.
4. Теория оптимального приема дискретных сообщений.
5. Теория информации. Основные информационные характеристики.
6. Помехоустойчивость частотно-модулированных сигналов.
7. Теоремы Шенонна. Теория Котельникова о преобразовании (АЦП).
8. Помехоустойчивость ИКМ к шумам квантования и помехам.
9. Построение систем радиосвязи, соответствующих современным требованиям качества и информационной безопасности.
10. Импульсно кодовая модуляция. Оптимальное кодирование.
11. Дифференциальные и дельта ИКМ. Линейные и нелинейные преобразования сообщений.
12. Аналоговые способы модуляции АМ, ЧМ, ФМ. Спектр сигналов.
13. Современные многопозиционные квадратурные модуляции (4,16,64, и т.п.).
14. Анализ потенциальной помехоустойчивости систем передачи непрерывных сообщений с различными видами модуляции.
15. Защита информации в системах связи. Основы теории шифрования

2. МНОГОКАНАЛЬНЫЕ ЦИФРОВЫЕ СИСТЕМЫ ПЕРЕДАЧИ И СРЕДСТВА ИХ ЗАЩИТЫ

1. Принципы построения систем передачи (разделение каналов, характеристики каналов)
2. Аналого-цифровое преобразование.
3. Цифро-аналоговое преобразование.
4. Генераторное оборудование ЦСП.
5. Синхронизация в ЦСП
6. Методы закрытия речевых сигналов.
7. Плезеохронная цифровая иерархия (ПЦИ).
8. Синхронная цифровая иерархия (СЦИ)
9. Принцип построения тактовой сетевой синхронизации (ТСС)
10. Архитектура сетей SDH.
11. Обобщённая схема синхронного мультиплексора.
12. Технология оптического мультиплексирования
13. Особенности построения волоконно-оптических систем передачи (ВОСП)

14. Физические принципы формирования каналов утечки информации в ВОЛС
15. Методы защиты информации от НДС

3. НАПРАВЛЯЮЩИЕ СРЕДЫ В СЕТЯХ ЭЛЕКТРОСВЯЗИ И МЕТОДЫ ИХ ЗАЩИТЫ

1. Общие принципы построения сетей электросвязи РФ. Классификация сетей электросвязи.
2. Электрические кабели связи, их классификация и характеристики.
3. Электромагнитные процессы в симметричных электрических кабелях связи.
4. Электромагнитные процессы в коаксиальных электрических кабелях связи.
5. Причины возникновения взаимных влияний между цепями связи и меры защиты от влияний.
6. Типы и конструкции оптических кабелей в зависимости от применения. Полное внутреннее отражение.
7. Конструкции и параметры оптических волокон.
8. Понятие ступенчатого и градиентного профиля показателя преломления.
9. Режимы работы световода. Понятие нормированной и критической частоты.
10. Дисперсионные искажения и их влияние на передачу сигналов.
11. Параметры передачи оптического волокна.
12. Затухание в кабелях связи.
13. Методы измерения затухания.
14. Определение длины участка регенерации.
15. Общая схема системы волоконно-оптической связи. Основные компоненты ВОЛП.

4. ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

1. Структура узлов ЗТКС. Основные принципы построения узлов связи.
2. Основные и возможные каналы утечки информации при эксплуатации узлов защищенных телекоммуникационных сетей. Методы технической защиты абонентских и соединительных линий на узлах связи.
3. Организация технической эксплуатации на узлах защищенных телекоммуникационных сетей. Документы, регламентирующие порядок эксплуатации.
4. Основы теории надежности систем связи. Факторы, влияющие на надежность защищенных телекоммуникационных систем.
5. Модели надежности и оценка показателей надежности
6. Основы технической диагностики ЗТКС. Задачи и основные понятия технической диагностики. Классификация видов контроля.
7. Методы обслуживания. Автоматизированные системы технического обслуживания.
8. Перспективные сети связи и технологии защиты информации.
9. Защита информации в беспроводных сетях пакетной коммутации.
10. Понятия ключа, шифра, атаки, защищенного и незащищенного канала.
11. Классическая схема криптосистемы с секретным ключом.
12. Блочные шифры. Понятие стойкости шифра.
13. Поточковые шифры.
14. Криптографические протоколы
15. Цифровая подпись

5. СЕТИ И СИСТЕМЫ РАДИОСВЯЗИ И МЕТОДЫ ИХ ЗАЩИТЫ

1. Регламент радиосвязи РФ. Стандарты на аналоговые и цифровые системы радиосвязи.
2. Общие принципы построения систем радиосвязи. Архитектура сетей.
3. Системы фиксированной и подвижной радиосвязи.
4. Радиорелейные линии связи прямой видимости: принципы построения, методы разделения каналов, методы защиты передаваемой информации.
5. Технические средства обеспечения информационной безопасности радиоэлектронных средств.
6. Защита информации в сетях IEEE 802.11.
7. Безопасность сетей радиодоступа.
8. Методы модуляции в сетях радиодоступа: ОФМ и КАМ.
9. Методы помехоустойчивого кодирования в сетях радиодоступа: сверточные коды, коды Рида-Соломона, коды LDPC.
10. Технические основы проектирования сетей радиодоступа. Модели расчета зон покрытия.
11. Сети радиодоступа стандарта DECT: технические параметры, топологии, принципы функционирования.
12. Сети радиодоступа стандарта IEEE 802.11: технические параметры, топологии, принципы функционирования.
13. Сети радиодоступа стандарта IEEE 802.15: технические параметры, топологии, принципы функционирования.
14. Сети радиодоступа стандарта IEEE 802.16: технические параметры, топологии, принципы функционирования.
15. Алгоритмы аутентификации в сетях сотовой связи.

6. Содержание государственного экзамена.

Государственный экзамен преследует цель произвести комплексную оценку полученных за период обучения знаний, умений и навыков, сформированных компетенций.

Государственный экзамен проводится по нескольким дисциплинам образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников. Государственный экзамен проводится устно по билетам.

К ГИА допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по ОП.

Порядок и форма проведения государственного экзамена:

- Перед государственным экзаменом проводятся консультации по дисциплинам, включенным в программу экзамена.
- Каждый экзаменационный билет содержит три вопроса
- Для подготовки выпускнику предоставляется один академический час времени, и пятнадцать минут для ответов на вопросы.
- Результаты государственного экзамена, определяются ГЭК оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного аттестационного испытания.
- Принятые ГЭК решения объявляются в день оформления протокола заседания. В протоколе заседания ГЭК по приему государственного экзамена отражаются перечень заданных обучающемуся вопросов и характеристика ответов на них, мнения членов ГЭК о выявленном в ходе экзамена уровне подготовленности обучающегося к решению профессиональных задач, а также о выявленных недостатках в теоретической и практической подготовке обучающегося.

7. Учебно-методическое и информационное обеспечение государственного экзамена

7.1 Список основной литературы

1. Аверченков В.И. Защита персональных данных в организации [Электронный ресурс]: монография/ Аверченков В.И., Рыгов М.Ю., Гайнулин Т.Р.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 124 с.— Режим доступа: <http://www.iprbookshop.ru/6993>.— ЭБС «IPRbooks», по паролю
2. Аверченков В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 187 с. — 5-89838-357-3. — Режим доступа: <http://www.iprbookshop.ru/7000>.— ЭБС «IPRbooks», по паролю
3. Аверченков В.И. Структура системы обеспечения безопасности Российской Федерации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 140 с.— Режим доступа: <http://www.iprbookshop.ru/7011>.— ЭБС «IPRbooks», по паролю
4. Алексеев Е.Б. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей [Электронный ресурс]: учебное пособие для вузов. Под ред. В.Н. Гордиенко, М.С. Тверецкого / Алексеев Е.Б., Гордиенко В.Н., Крухмалев В.В., Моченов А.Д., Тверецкий М.С. — Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2017.— 392 с.— Режим доступа: <http://www.iprbookshop.ru/12033>.— ЭБС «IPRbooks», по паролю
5. Ананьин А.В. Проектирование защищенных сетей и систем радиосвязи: Учебное пособие к выполнению курсовых и дипломных проектов. – Хабаровск: ХИИК ГОУ ВПО СибГУТИ, 2012. – 73с
6. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые

данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: <http://www.iprbookshop.ru/10677>.— ЭБС «IPRbooks», по паролю

7. Колосовский Е.А. Устройства приема и обработки сигналов [Электронный ресурс]: учебное пособие / Колосовский Е.А.— М.: Горячая линия - Телеком, 2012. 456с. – Режим доступа: <http://www.iprbookshop.ru/12062>. - ЭБС «IPRbooks», по паролю

8. Крук Б.И. Телекоммуникационные системы и сети. Современные технологии [Электронный ресурс]: учебное пособие/ Крук Б.И., Попантонопуло В.Н., Шувалов В.П.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 620 с.— Режим доступа: <http://www.iprbookshop.ru/12047>.— ЭБС «IPRbooks», по паролю

9. Крухмалев В.В. Синхронные телекоммуникационные системы и транспортные сети [Электронный ресурс]: учебное пособие/ Крухмалев В.В., Моченов А.Д.— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2012.— 288 с.— Режим доступа: <http://www.iprbookshop.ru/16137>.— ЭБС «IPRbooks», по паролю

10. Носкова Н.В. Стандарты беспроводных телекоммуникационных сетей. Учебное пособие -Новосибирск: «СибГУТИ»,2012

11. Портнов Э.Л. Оптические кабели связи их монтаж и измерение [Электронный ресурс]: учебное пособие/ Портнов Э.Л.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 448 с.— Режим доступа: <http://www.iprbookshop.ru/12011>.— ЭБС «IPRbooks», по паролю

12. Субботин Е.А. Методы и средства измерения параметров оптических телекоммуникационных систем [Электронный ресурс]: учебное пособие для вузов/ Субботин Е.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 224 с.— Режим доступа: <http://www.iprbookshop.ru/37187>.— ЭБС «IPRbooks», по паролю

13. Фокин В.Г. Когерентные оптические сети [Электронный ресурс]: учебное пособие/ Фокин В.Г.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2015.— 371 с.— Режим доступа: <http://www.iprbookshop.ru/40534>.— ЭБС «IPRbooks», по паролю

14. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/29257>.— ЭБС «IPRbooks», по паролю

15. Кришталюк А.Н. Управление безопасностью бизнеса [Электронный ресурс]: курс лекций/Кришталюк А.Н.- Электрон. текстовые данные.- Орел: Межрегиональная Академия безопасности и выживания (МАБИ13), 2014.- 116 с.- Режим доступа: <http://www.iprbookshop.ru/33445>.- ЭБС «IPRbooks» [Лицензия: весь срок охраны авторского права]

16. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.-Электрон. текстовые данные.-М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.- 212 с.-Режим доступа:<http://www.iprbookshop.ru/52182>.-ЭБС «IPRbooks» [Лицензия: до 01.12.2019

17. Заика А.А. Локальные сети и интернет [Электронный ресурс]/ Заика А.А.- Электрон. текстовые данные.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.- 323 с.-Режим доступа: <http://www.iprbookshop.ru/52150.html>.-ЭБС «IPRbooks»

18. Беспроводные сети Wi-Fi [Электронный ресурс]/ А.В. Пролетарский [и др.].- Электрон. текстовые данные.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.-284 с.-Режим доступа: <http://www.iprbookshop.ru/52183.html>.-ЭБС «IPRbooks»

7.2 Список дополнительной литературы

1. Фомин, Д. В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. - Электрон. текстовые

данные. - Саратов : Вузовское образование, 2018. - 54 с. - 978-5-4487- 0298-3. - Режим доступа: <http://www.ip1-bookshop.ru/77320.html> - ЭБС «IPRbooks»

2. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. -Электрон. текстовые данные. -Саратов: Профобразование, 2017. 702 с. 978-5-4488-0070-2. Режим доступа: <http://www.ip1-bookshop.ru/63594.html> .-ЭБС «IPRbooks»

3. Носкова Н.В. Стандарты беспроводных телекоммуникационных сетей [Электронный ре-сурс]: учебное пособие/ Носкова Н.В.- Электрон. текстовые данные.-Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2012.- 201 с.-Режим доступа: <http://www.ip1-bookshop.ru/45489.html>.-ЭБС «IPRbooks»

4. Кокорева Е.В. Основы беспроводной связи [Электронный ресурс]: учебно-методическое пособие/ Кокорева Е.В., Белезекова А.С.- Электрон. текстовые данные.-Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2015.-. 70 с.- Режим доступа: <http://www.ip1-bookshop.ru/55489.html>.-ЭБС «IPRbooks»

7.3 Информационное обеспечение (в т.ч. интернет-ресурсы).

1. Обеспечение информационной безопасности бизнеса [Электронный ресурс]/ В.В. Андрианов [и др.]-Электрон. текстовые данные.-М.: ЦИПСИР, 2011.-373 с.-Режим доступа: <http://www.ip1-bookshop.ru/38525.html>.-ЭБС «IPRbooks»

2. Чибисов О.В. Организация и управление безопасностью в финансово-кредитных организациях [Электронный ресурс]: учебное пособие/ Чибисов О.В.-Электрон. текстовые данные.-М.: Евразийский открытый институт, 2011.-115 с.-Режим доступа: <http://www.ip1-bookshop.ru/10737.html>.-ЭБС «IPRbooks»

3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.-Электрон. текстовые данные.-Брянск: Брянский государственный технический университет, 2012.-268 с.-Режим доступа: <http://www.ip1-bookshop.ru/6991.html>.-ЭБС «IPRbooks»

4. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.]-Электрон. текстовые данные.-Брянск: Брянский государственный технический университет, 2012.-100 с.-Режим доступа: <http://www.ip1-bookshop.ru/6992.html>.-ЭБС «IPRbooks»

5. Ситнов А.А. Аудит информационной инфраструктуры [Электронный ресурс]: учебное пособие/ Ситнов А.А.-Электрон. текстовые данные.-М.: Евразийский открытый институт, 2011.-144 с.-Режим доступа: <http://www.ip1-bookshop.ru/10615.html>.-ЭБС «IPRbook»

6. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). -URL: <http://fstec.ru/> (дата обращения: 22.01.2019).

7. Официальный сайт ОАО Инфотекст» -URL: <https://infotecs.ru/>

8. Информационный портал компании Positive Technologies -URL: <http://secshitylab.ru/>

9. Официальный сайт Института криптографии, связи и информатики при Академии ФСБ России. -URL: <http://www.sc1-f.gov.ru/>

10. Новостной сайт об информационной безопасности от Kaspersky Lab. -URL: <https://thleatpos/>

11. Информационно-аналитический центр, посвященный информационной безопасности. URL: <https://www.anti-malware.ru/>

12. Информационный портал ассоциации по вопросам защиты информации BISA - URL: <http://bis-expert.ru/>

13. Интернет-портал ISO27000.RU -URL: <http://www.iso27000.ru/>

14. Информационный портал журнала «Information Security»-URL: <http://bis-expert.ru/>

15. Берлин А.Н. Сотовые системы связи [Электронный ресурс]/ Берлин А.Н.-Электрон. текстовые данные.-М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.-430 с.-Режим доступа: <http://www.ip1-bookshop.ru/52177.html>.-ЭБС «IPRbooks»

16. Алексеев В.А. Беспроводные локальные сети IEEE 802.11 Wi-Fi [Электронный ресурс]: методические указания I< проведению лабораторных работ по курсу «Сети ЭВМ и теле-коммуникации»/ Алексеев . В.А.-Электрон. текстовые данные.-Липецк: Лишцкий государственный технический университет, ЭБС АСВ, 2012.-26 с.-Режим-доступа: <http://www.ip1-bookshop.ru/17720.html>.-ЭБС «IPRbooks»

8. Материалы, определяющие процедуру оценивания результатов освоения образовательной программы с помощью государственного экзамена

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций представлен в таблице:

Компетенция	Форма контроля
Государственный экзамен	
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	теоретический вопрос, практико-ориентированный вопрос
УК -5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	теоретический вопрос, практико-ориентированный вопрос
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	теоретический вопрос, практико-ориентированный вопрос
ОПК-1 Способен использовать положения, законы и методы естественных наук и математики для решения задач инженерной деятельности	практическое задание
ОПК-2 Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных	практическое задание
ОПК- 3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	практическое задание
ПК-1 Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных	практическое задание
ПК -3 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	практическое задание

9. Перечень тем выпускных квалификационных работ

1. Разработка нейронной сети для компьютерного зрения в системе «Цифровой двойник будущего офицера» с использованием технологии искусственного интеллекта.

2. Разработка модуля кроссплатформенного мобильного приложения по отслеживанию почтовых отправлений фельдъегерско- почтовой связи ВС РФ.
3. Конструирование блока управления адаптивной антенной решеткой, предназначенной для размещения на подвижном объекте и для приёма сигнала в условиях различных дестабилизирующих факторов.
4. Разработка математической модели алгоритма управления адаптивной антенной решёткой, размещённой на подвижном объекте и предназначенной для приёма сигнала в условиях различных дестабилизирующих факторов.
5. Разработка аппаратной части блока управления адаптивной антенной решеткой, размещённой на подвижном объекте и предназначенной для приёма сигнала в условиях различных дестабилизирующих факторов.
6. Разработка 3D модели адаптивной антенной решетки, предназначенной для приёма сигнала в условиях различных дестабилизирующих факторов, и получение её диаграммы направленности.
7. Разработка способа выбора оптимального набора адаптивных параметров радиолинии тактического звена управления.
8. Разработка модели функционирования самоорганизующейся радиосети тактического звена управления в условиях помех.
9. Разработка методики оценки влияния параметров БПЛА на элементы АФАР, размещаемые на его корпусе, используя программный комплекс моделирования.
10. Разработка унифицированного макета программного обеспечения «Информационная система Главного управления связи Вооружённых Сил Российской Федерации» и его совершенствование.
11. Разработка нейронной сети для компьютерного зрения в системе «Цифровой двойник будущего офицера» с использованием технологии искусственного интеллекта.
12. Разработка математической матричной модели алгоритма управления адаптивной антенной с множественным доступом, на основе технологий ММО устанавливаемой на БПЛА для интеллектуализации процессов управления и повышения помехоустойчивости.
13. Разработка программного модуля тренажёрно-обучающей системы для изучения станций спутниковой связи Р-441 ЛМ (П-230 есть в AR).
14. Разработка программного модуля тренажёрно-обучающей системы для изучения цифровой радиорелейной станции Р-431 АМ (П-230 есть ВАР).
15. Разработка комплексной системы защиты информации коммерческой организации на примере
16. Анализ уязвимостей в социальных сетях
17. Исследование безопасности мобильных платформ
18. Разработка рекомендаций по использованию средств защиты от DDOS-атак в корпоративных сетях
19. Исследование уязвимостей медицинских отраслевых протоколов и серверов в РФ
20. Разработка рекомендаций по организации защиты информационной системы малого предприятия
21. Разработка лаборатории для изучения веб-уязвимостей
22. Разработка рекомендаций по использованию СЗИ в облачной среде применительно к банковской сфере
23. Разработка безопасного децентрализованного сервиса, работающего на базе смарт-контрактов
24. Исследование возможности создания СОВ на платформе ОССН Астра Линукс
25. Анализ защищенности КСЗИ и обнаружение атак
26. Кибертерроризм как угроза современности
27. Исследование безопасности контактных и бесконтактных смарт-карт
28. Разработка практикума по расследованию инцидентов информационной безопасности

29. Безопасность пользователя при взаимодействии с Android-приложениями
30. Разработка рекомендаций по повышению уровня информационной безопасности госбюджетной организации
31. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему
32. Анализ возможностей платформы R-Vision IRP в реагировании на инциденты ИБ
33. Исследование возможностей создания защищенной инфраструктуры малого предприятия
34. Совершенствование системы защиты информации производственного предприятия
35. Исследование методов анонимизации конфиденциальной информации
36. Анализ возможностей обеспечения безопасности кроссплатформенных мобильных приложений.
37. Анализ возможностей программного комплекса «Efros Config Inspector» для аудита ИТ-инфраструктуры предприятия
38. Разработка лаборатории для обучения навыкам тестирования на проникновение
39. Интеграция SIEM системы на предприятии энергетической отрасли
40. Автоматизация процессов управления информационной безопасностью
41. Разработка модели защиты персональных данных клиентов букмекерских компаний
42. Исследование возможностей шлюза C-Терра для создания надежных каналов удаленного доступа в различных операционных средах
43. Применение алгоритмов машинного обучения к задаче выявления мошенничества при пользовании банковскими услугами
44. Организация безопасного доступа в Интернет с помощью шлюза Idesco UTM
45. Разработка модели компании занимающийся аутсорсингом информационной безопасности
46. Разработка системы распознавания бесхозных предметов, несущих угрозу, с использованием нейронных сетей
47. Анализ развития и возможности использования сетей с нулевым доверием
48. Разработка прототипа системы увеличения дальности связи в ТЗУ путем ретрансляции сигналов через БпЛА
49. Разработка аппаратных решений для ретрансляции сигналов на БпЛА мультироторного типа
50. Разработка конструктивных решений БпЛА мультироторного типа и его модулей для обеспечения ретрансляции сигналов через БпЛА
51. Разработка макета программного обеспечения расчета систем электропитания радиостанций 6-го поколения
Разработка способа проактивного управления кибербезопасностью ИТКС военного назначения путем сокращения времени сетевого контроля безопасности связи и анализа динамики действий нарушителя в условиях СВО
52. Разработка способа управления кибербезопасностью ИТКС военного назначения с прогнозированием на основе сетевого контроля безопасности связи и применением нейронных сетей в условиях СВО
53. Разработка способа повышения информационной безопасности базы данных локальной вычислительной сети подвижного пункта управления отдельной мотострелковой бригады ТЗУ в условиях СВО
54. Разработка способа повышения целостности программного обеспечения в ИТКС военного назначения в условиях преднамеренных помех противника в ходе СВО
55. Разработка макета программного обеспечения «Восстановление объемных изображений системы поддержки принятия решений», основанных на элементах искусственного интеллекта
56. Разработка нейросетевой модели обнаружения уязвимостей и анализа угроз

безопасности в ИТКС военного назначения, построенной на основе элементов искусственного интеллекта

57. Разработка макета программного обеспечения определения радио координат движущегося объекта (в ТЗУ) на сложном подвижном фоне на основе машинного зрения

58. Разработка макета программного обеспечения системы контроля прохождения отправок Главного управления связи Вооруженных Сил Российской Федерации

59. Разработка алгоритма сетевого управления программным обеспечением «Информационная система Главного управления связи Вооруженных Сил Российской Федерации»

60. Разработка прототипа системы доставки отправок ФПС посредством БпЛА

61. Разработка унифицированного макета программного обеспечения «Информационная система Главного управления связи Вооруженных Сил Российской Федерации» на отечество программной платформе

62. Разработка устройства пеленгации радиосигналов для ретранслятора на БпЛА Проектирование макета программного обеспечения энергетической системы питания для привязного БпЛА (тип квазимачта)

63. Разработка составной части программного обеспечения анализа состояния связи на ретрансляторе типа БпЛА

64. Разработка макета программного обеспечения «Использование материальных ресурсов Военной академии связи», на основе применения технологии искусственного интеллекта

65. Разработка макета программного обеспечения системы контроля безопасности сети передачи данных Главного управления связи Вооруженных Сил Российской Федерации

66. Разработка программного модуля тренажерно-обучающей системы по изучению радиостанции Р-187П1

67. Разработка виртуального ассистента для тренажерно-обучающей системы по изучению средств связи П-230Т

68. Разработка макета программного обеспечения «Квантовое распределение ключей на расстояние свыше 500 км от спутника до Земли»

69. Разработка web-модуля программного обеспечения «Диагностика функциональных структур элементов техники связи»

10. Материалы, определяющие процедуру оценивания результатов освоения образовательной программы с помощью защиты ВКР

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций представлен в таблице:

Компетенция	Форма контроля
Выпускная квалификационная работа	
УК -1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	доклад
УК -2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	доклад
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	оформление пояснительной записки

УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	оформление пояснительной записки
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	оформление пояснительной записки
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	оформление пояснительной записки
УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	оформление пояснительной записки
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	доклад
ОПК-5 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	доклад
ПК-1 Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных	оформление пояснительной записки
ПК -3 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	оформление пояснительной записки

Результаты защиты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после оформления в установленном порядке протокола заседания ГЭК.

- *Оценка «5» (отлично):* тема для выпускной квалификационной работы актуальна, и актуальность ее обоснована; сформулированы цель, задачи, предмет, объект исследования, методы, используемые в работе; содержание и структура исследования соответствуют поставленным целям и задачам; изложение текста работы отличается логичностью, смысловой завершенностью и анализом представленного материала; комплексно использованы методы исследования, адекватные поставленным задачам; итоговые выводы обоснованы, четко сформулированы, соответствуют задачам исследования; в работе отсутствуют орфографические и пунктуационные ошибки; ВКР оформлена в соответствии с предъявленными требованиями; отзыв руководителя и внешняя рецензия на работу – положительные; публичная защита выпускной квалификационной работы показала уверенное владение материалом, умение четко, аргументировано и корректно отвечать на поставленные вопросы, отстаивать собственную точку зрения; при защите использован наглядный материал (презентация, таблицы, схемы и др.).

- *Оценка «4» (хорошо):* тема работы актуальна, имеет теоретическое обоснование; содержание работы в целом соответствует поставленной цели и задачам; изложение материала носит преимущественно описательный характер; структура работы логична; использованы методы, адекватные поставленным задачам; имеются итоговые выводы, соответствующие

поставленным задачам исследования; основные требования к оформлению работы в целом соблюдены, но имеют небольшие недочеты; отзыв руководителя и внешняя рецензия на работу – положительные, содержат небольшие замечания; публичная защита ВКР показала достаточно уверенное владение материалом, однако допущены неточности при ответах на вопросы; ответы на вопросы недостаточно аргументированы; при защите использован наглядный материал.

- *Оценка «3» (удовлетворительно):* тема работы актуальна, но актуальность ее, цель и задачи работы сформулированы нечетко; содержание не всегда согласовано с темой и(или) поставленными задачами; изложение материала носит описательный характер, большие отрывки (более двух абзацев) переписаны из источников; самостоятельные выводы либо отсутствуют, либо присутствуют только формально; нарушен ряд требований к оформлению работы; в положительных отзывах и рецензии содержатся замечания; в ходе публичной защиты работы проявились неуверенное владение материалом, неумение отстаивать свою точку зрения и отвечать на вопросы; автор затрудняется в ответах на вопросы членов ГЭК.

- *Оценка «2» (неудовлетворительно):* актуальность исследования автором не обоснована, цель и задачи сформулированы неточно и неполно, либо их формулировки отсутствуют; содержание и тема работы плохо согласуются (не согласуются) между собой; работа носит преимущественно реферативный характер; большая часть работы списана с одного источника либо заимствована из сети Интернет; выводы не соответствуют поставленным задачам (при их наличии); нарушены правила оформления работы; отзыв и рецензия содержат много замечаний; в ходе публичной защиты работы проявилось неуверенное владение материалом, неумение формулировать собственную позицию; при выступлении допущены существенные ошибки, которые выпускник не может исправить самостоятельно.

При выставлении итоговой оценки по защите ВКР учитываются:

- качество устного доклада выпускника;
- качество наглядного материала, иллюстрирующего основные положения ВКР;
- глубина и точность ответов на вопросы;
- оценка рецензента;
- отзыв руководителя.

11. Материально-техническое и программное обеспечение государственной итоговой аттестации

Материально-техническое обеспечение государственной итоговой аттестации предусматривает наличие аудитории для сдачи государственного экзамена и защиты выпускной квалификационной работы. Государственный экзамен проходит в аудиториях, предусматривающих наличие рабочих мест для председателя и членов государственной экзаменационной комиссии и рабочих мест для студентов, допущенных на государственный экзамен. Для защиты выпускной квалификационной работы также требуется аудитория, предусматривающая наличие рабочих мест для председателя и членов государственной экзаменационной комиссии, рабочего места для студента, компьютерной техники с необходимым лицензионным программным обеспечением, мультимедийного проектора, экрана, щитов для размещения наглядного материала.

Наименование аудиторий, кабинетов, лабораторий	Оборудование, программное обеспечение
Учебные аудитории для	Оснащение:

Наименование аудиторий, кабинетов, лабораторий	Оборудование, программное обеспечение
<p>проведения занятий лекционного типа, занятий семинарского типа, текущего контроля и промежуточной аттестации.</p>	<p>1) В кабинете имеются технические средства обучения, служащие для предоставления учебной информации, рабочее место преподавателя, оснащенное персональным компьютером, экран, доска, а также специализированная учебная мебель;</p> <p>2) технические средства обучения: - проектор InFocus IN2128HDX, экран на треноге; - компьютер персональный с характеристиками: процессор Intel Core I3 2200 3,2 ГГц, ОЗУ 4 ГБ, ЖД 500 ГБ, монитор диагональ 19“ с матрицей TFT, клавиатура проводная, мышь оптическая проводная;</p> <p>3) рабочее место, которое оборудовано компьютером, имеет подключение к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду ХИИК;</p> <p>4) при необходимости для проведения занятий аудитория может оснащаться переносными звуковыми колонками</p>
<p>Учебные аудитории для проведения занятий семинарского типа; текущего контроля и промежуточной аттестации; курсового проектирования (выполнения курсовых работ). Компьютерная аудитория</p>	<p>Оснащение:</p> <p>1) рабочее место преподавателя, оснащенное персональным компьютером с выходом в сеть Интернет;</p> <p>2) рабочие места обучающихся – компьютерные столы и стулья, оснащенных персональными компьютерами с характеристиками: - Intel (R) Core (TM) i5-9600K CPU; - накопитель SSD 250 GB; - накопитель HDD 2 TB; - мышь оптическая проводная; - видеокарта GeForce GTX 16060 SUPER;</p> <p>3) сервер в лаборатории (8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткий диск общим объемом 8 Тб, программное обеспечение: Windows Server 2012)</p> <p>4) учебная доска;</p> <p>5) проектор, экран;</p> <p>6) учебные места (учебная мебель на 36 места) для лекционных групповых занятий;</p> <p>7) технические средства обучения, служащие для предоставления учебной информации (стенды, плакаты);</p> <p>8) структурированная кабельная система (СКС) на 15 рабочих мест (локальная сеть на основе медного кабеля витая пара, сеть электропитания). Локальная сеть с доступом в Интернет.</p> <p>9) пакет офисных программных продуктов Microsoft Visio 2016, лицензионный договор № Tr000258304 07.06.2018 г. на предоставление простой (неисключительной) лицензии на право использования программного обеспечения Microsoft Visio 2016 Russian OLP NL AcademicEdition.</p> <p>10) программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО: - EclipseIDEforJavaEEDevelopers, - NETFrameworkJDK 8,</p>

Наименование аудиторий, кабинетов, лабораторий	Оборудование, программное обеспечение
	↯ - MicrosoftSQLServerExpressEdition, ↯ - MicrosoftVisioProfessional, ↯ - MicrosoftVisualStudio, ↯ - MySQLInstallerforWindows,- NetBeans, ↯ - SQLServerManagementStudio, ↯ - MicrosoftSQLServerJavaConnector, ↯ - AndroidStudio, ↯ - IntelliJIDEA - AndroidStudio,
Учебная аудитория для проведения лабораторных занятий.	Оснащение: Лаборатория оснащена: - рабочее место преподавателя; - рабочие места обучающихся – 15 рабочих мест (компьютерные столы и стулья), оснащенных персональным компьютерами с характеристиками: - процессор Intel Core I5 6500 3,2ГГц;- ОЗУ 8 ГБ; - ЖД 1 ТБ;- монитор диагональ 21,5“ с матрицей IPS; - клавиатура проводная; - мышь оптическая проводная; - учебная доска; - технические средства обучения, служащие для предоставления учебной информации (стенды, плакаты); - в кабинете организована структурированная кабельная система (СКС) на 12 рабочих мест (локальная сеть на основе медного кабеля витая пара, сеть электропитания). Локальная сеть с доступом в Интернет и в ЭИОС ХИИК;- ОС Ubuntu 18.4 лицензия GNU GPL.
Учебная аудитория для проведения групповых и индивидуальных консультаций	Оснащение: Лаборатория оснащена: рабочее место преподавателя, доска, а также специализированная учебная мебель. Технические средства обучения: - Ноутбук HP Probook 450 G6 с характеристиками: процессор Intel Core I7 8565U 4,1 ГГц, ОЗУ 16 ГБ, SSD 500 ГБ, монитор диагональ 15.6“ с матрицей IPS.Рабочие места имеют подключение к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду ХИИК. При необходимости для проведения занятий аудитория может оснащаться переносными звуковыми колонками.Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.
Помещение для самостоятельной работы	Оснащение: - рабочие места с компьютерной техникой с подключением к сети Интернет и доступом в электронно-библиотечную систему и электронную информационно-образовательную среду

12. Особенности проведения ГИА для лиц с ограниченными возможностями здоровья

Государственная итоговая аттестация проводится с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья выпускников из числа инвалидов и лиц с ограниченными возможностями здоровья.

При проведении ГИА для выпускников с индивидуальными особенностями

обеспечивается соблюдение следующих общих требований: использование специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего выпускникам необходимую техническую помощь, обеспечение доступа в здания и помещения, где проходит ГИА, и другие условия, без которых невозможно или затруднено проведение ГИА. Ассистентом может быть назначен родитель (законный представитель) участника ГИА, штатный сотрудник Института, в том числе сотрудник специального (коррекционного) образовательного учреждения.

При проведении ГИА обеспечивается соблюдение следующих общих требований: возможность выбора способа проведения ГИА; проведение ГИА для студентов-инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся при прохождении государственной итоговой аттестации; присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей на основании письменного заявления; пользование необходимыми обучающимся техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей.

Продолжительность прохождения ГИА по отношению к установленной продолжительности его сдачи увеличивается по письменному заявлению обучающегося с ограниченными возможностями здоровья: продолжительность государственного экзамена, проводимого в письменной форме - не более чем на 1,5 часа; продолжительность подготовки обучающегося к ответу на государственном экзамене, проводимом в устной форме, – не более чем на 20 минут; продолжительность выступления обучающегося при защите выпускной квалификационной работы – не более чем на 15 минут.