Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Программа

ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ Бурлов В.Г.

Утверждаю
Председатель УМС _____И.И. Палкин

Рекомендована решением
Учебно-методического совета
___ _____2018 г., протокол №____

Рассмотрена и утверждена на заседании кафедры
___ _____ 2018 г., протокол №___
Зав. кафедрой _____ Бурлов В.Г.

Авторы-разработчики:
_____Бурлов В.Г.
_____Миклуш В.А.

Санкт-Петербург 2018

I. Общие положения

Согласно Федеральному государственному образовательному стандарту высшего образования (ФГОС ВО) по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета) государственная итоговая аттестация является завершающим этапом освоения основной образовательной программы специалитета.

Программа государственной итоговой аттестации для студентов, обучающихся по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Разработка защищенных телекоммуникационных систем составлена в соответствии с требованиями:

1. Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 № 273- ФЗ ,
2. Федеральный государственный стандарт высшего образования по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета) утвержденный приказом Министерства образования и науки РФ от 16 ноября 2016 г. № 1426
3. Приказ Министерства образования и науки РФ от 05 апреля 2017 г. № 301 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры";
4. Нормативно-методические документы Министерства образования и науки Российской Федерации.
5. Устав Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российский государственный гидрометеорологический университет».
6. Локальные нормативные акты Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российский государственный гидрометеорологический университет».

Рабочие учебные планы подготовки специалиста по очной форме обучения по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Разработка защищенных телекоммуникационных систем одобрены на заседании Ученого совета ФГБОУ ВО «Российский государственный университет от 27.02.2018 г. протокол №___

Нормативный срок обучения составляет при очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации - 5,5 лет;

Государственная итоговая аттестация по специальности 10.05.02 Информационная безопасность телекоммуникационных систем проводится в форме (и в указанной последовательности:

- Государственный экзамен
- Защита выпускной квалификационной работы.

Государственная итоговая аттестация проводится по окончании теоретического периода обучения в 6-ом семестре.

На проведении государственной итоговой аттестации учебным планом отводится 6 недель (9 з.е.)

- 4 недели (6 з.е., 216 часов) отводится на подготовку к сдаче и сдачу государственного экзамена;
- 2 недели (3 з.е., 108 часов) отводится на подготовку и представление основных результатов выпускной квалификационной работы.

II. Характеристика профессиональной деятельности обучающегося

2.1. Область профессиональной деятельности выпускника

Область профессиональной деятельности выпускников, освоивших программу специалитета, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с проектированием, созданием, исследованием и эксплуатацией систем обеспечения информационной безопасности телекоммуникационных систем в условиях существования угроз в информационной сфере.

2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников, освоивших основную образовательную программу, являются:

– методы, средства и системы обеспечения информационной безопасности информационно-телекоммуникационных сетей и систем;

– управление информационной безопасностью информационно-телекоммуникационных сетей и систем;

– информационно-телекоммуникационные сети и системы различного назначения, их оборудование, принципы построения.

2.3. Виды образовательной деятельности.

Виды профессиональной деятельности выпускников, освоивших основную образовательную программу: Специалист по специальности 10.05.02 Информационная безопасность телекоммуникационных систем готовится к следующим видам профессиональной деятельности:

– научно-исследовательская;
– проектная;
– контрольно-аналитическая;
– организационно-управленческая;
– эксплуатационная.

Выпускник осваивает программу специалитета по специализации «Разработка защищенных телекоммуникационных систем»

2.4. Задачи профессиональной деятельности выпускника

Задачи профессиональной деятельности выпускников, освоивших основную образовательную программу:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности телекоммуникационных систем, выработка предложений по вопросам комплексного обеспечения информационной безопасности таких систем;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

изучение, анализ и обобщение опыта работы учреждений, организаций и предприятий по использованию технических средств и способов защиты информации в телекоммуникационных системах с целью повышения эффективности и совершенствования работ по ее защите;

сопровождение разработки, исследование телекоммуникационных систем, сетей и устройств, технических и программно-аппаратных средств защиты и обработки информации в телекоммуникационных системах;

определение требований по защите информации, анализ защищенности телекоммуникационных систем и оценка рисков нарушения их информационной безопасности;

проектная деятельность:

сбор и анализ исходных данных для проектирования систем и средств защиты информации, обеспечения требуемого качества обслуживания в телекоммуникационных системах;

сравнительный анализ сетей и систем передачи информации по показателям информационной безопасности, обеспечения требуемого качества обслуживания;

разработка проектов, технических заданий, планов и графиков проведения работ по защите информации телекоммуникационных систем и необходимой технической документации;

рациональный выбор элементной базы при проектировании систем и средств защиты информации, обеспечения требуемого качества обслуживания телекоммуникационных систем;

разработка политики безопасности, выбор методов и средств обеспечения информационной безопасности объектов информационно-телекоммуникационных систем;

контрольно-аналитическая деятельность:

проверка работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты информации телекоммуникационных средств и систем;

составление методик расчетов и программ экспериментальных исследований по защите информации телекоммуникационных систем, выполнение расчетов в соответствии с разработанными методиками и программами;

проверка учреждений, организаций и предприятий на соответствие требованиям нормативной правовой базы в области информационной безопасности телекоммуникационных систем;

подготовка отзывов и заключений на нормативно-методические материалы и техническую документацию;

участие в проведении аттестации телекоммуникационных систем, технических средств защиты информации по требованиям соответствующих классов (уровней) безопасности;

организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;

разработка предложений по совершенствованию и повышению эффективности комплекса мер по обеспечению информационной безопасности телекоммуникационной системы;

организация работ по выполнению требований режима защиты информации ограниченного доступа;

разработка методических материалов и организационно-распорядительных документов по обеспечению информационной безопасности телекоммуникационных систем на предприятиях;

эксплуатационная деятельность:

эксплуатация специальных технических и программно-аппаратных средств защищенных телекоммуникационных сетей и систем;

документационное обеспечение эксплуатации защищенных телекоммуникационных сетей и систем;

инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания;

выявление возможных источников и технических каналов утечки информации;

обеспечение восстановления работоспособности телекоммуникационных систем, в том числе подсистемы защиты информации, при сбоях и нарушении функционирования;

в соответствии со специализацией:

разработка алгоритмов преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов;

разработка аппаратного и программного обеспечения узлов и устройств защищенных телекоммуникационных систем на базе сигнальных процессоров;

участие в разработке систем управления информационной безопасностью телекоммуникационных систем, в том числе выбор методов и разработка алгоритмов принятия решений;

III. Требования к уровню подготовки обучающегося

Цель государственной итоговой аттестации – оценка уровня сформированных компетенций выпускника и установление соответствия уровня подготовленности обучающегося к решению профессиональных задач требованиям федерального государственного образовательного стандарта направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем.

Результаты освоения ОПОП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

В результате освоения данной ОПОП ВО выпускник должен обладать следующими компетенциями:

общекультурными компетенциями (ОК):

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

общепрофессиональными компетенциями (ОПК):

способностью анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности (ОПК-1);

способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации (ОПК-4);

способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач (ОПК-5);

способностью применять методы научных исследований в профессиональной деятельности (ОПК-6);

способностью применять нормативные правовые акты в своей профессиональной деятельности (ОПК-7);

способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-8).

профессиональными компетенциями (ПК):

научно-исследовательская деятельность:

способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1);

способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов (ПК-2);

способностью оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств (ПК-3);

способностью участвовать в разработке компонентов телекоммуникационных систем (ПК-4);

проектная деятельность:

способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов (ПК-5);

способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6);

способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-7);

контрольно-аналитическая деятельность:

способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем (ПК-8);

способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9);

способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-10);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-11);

способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности (ПК-12);

способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов,

регламентирующих работу но обеспечению информационной безопасности телекоммуникационных систем (ПК-13);

эксплуатационная *деятельность:*

способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14);

способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-15).

профессионально-специализированными компетенциями (ПСК)

способностью разрабатывать алгоритмы преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов (ПСК-7.1);

способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных телекоммуникационных системах (ПСК-7.2);

способностью разрабатывать аппаратное и программное обеспечение узлов и устройств защищенных телекоммуникационных систем на базе сигнальных процессоров (ПСК-7.3);

способностью участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем (ПСК-7.4);

способностью обеспечивать защиту программных средств защищенных телекоммуникационных систем (ПСК-7.5);

В ходе проведения государственной итоговой аттестации проводится контроль сформированности всех компетенций. В таблице 1 показано распределение компетенций по формам проведения государственной итоговой аттестации.

Компетенция	Форма ГИА	
	Государственный экзамен	Защита выпускной квалификационной работы
ОК-1		+
ОК-2		+
ОК-3		+
ОК-4		+
ОК-5		+
ОК-6		+
ОК-7		+
ОК-8	+	+
ОК-9		+
ОПК-1	+	+
ОПК-2	+	+
ОПК-3	+	+
ОПК-4	+	+
ОПК-5	+	+
ОПК-6		+
ОПК-7	+	+
ОПК-8		+

ПК-1	+	+
ПК-2	+	+
ПК-3	+	+
ПК-4	+	+
ПК-5	+	+
ПК-6	+	+
ПК-7	+	+
ПК-8	+	+
ПК-9	+	+
ПК-10	+	+
ПК-11		+
ПК-12	+	+
ПК-13	+	+
ПК-14	+	+
ПК-15	+	+
ПСК-7.1	+	+
ПСК-7.2	+	+
ПСК-7.3	+	+
ПСК-7.4	+	+
ПСК-7.5	+	+

IV. Программа государственного экзамена

Государственная итоговая аттестация относится к базовой части программы подготовки Б3. Объем государственной итоговой аттестации составляет 9 зачетных единиц или 324 часа.

Итоговая государственная аттестация направлена на установление соответствия уровня подготовки выпускников требованиям ФГОС ВО.

Итоговая государственная аттестация состоит из двух этапов:

- сдачи государственного экзамена;
- защиты выпускной квалификационной работы в форме

Порядок проведения и программа государственного экзамена по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» определяются вузом на основании методических рекомендаций и соответствующей примерной программы, разработанных УМО по образованию в области информационной безопасности, Положения об итоговой государственной аттестации выпускников высших учебных заведений, утвержденного Минобрнауки РФ, и Федерального государственного образовательного стандарта по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»**.**

Итоговый междисциплинарный экзамен является составной частью обязательной государственной итоговой аттестации и проводится с целью определения соответствия знаний, умений и навыков студентов по комплексу специальных дисциплин (включая дисциплины специализации) требованиям федерального государственного образовательного стандарта по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Перечень вопросов, выносимых на итоговый междисциплинарный экзамен по специальным дисциплинам, определяются вузом с учетом особенностей реализуемой образовательной программы.

Перечень примерных вопросов для подготовки к государственному экзамену

№ п/п	Наименование дисциплины (цикл по учебному плану)	Вопросы
1.	Организационное и правовое обеспечение информационной безопасности	1. Правовой режим защиты государственной тайны 2. Лицензирование в области защиты информации 3. Сертификация средств защиты информации и вычислительной техники 4. Электронная подпись 5. Классификация автоматизированных систем 6. Правовой режим защиты персональных данных 7. Правовой режим защиты коммерческой тайны
2.	Техническая защита информации	1. Технический канал утечки информации (ТКУИ). Классификация ТКУИ. Причины и источники образования ТКУИ. 2. Скрытие речевой информации в аналоговых каналах связи. Обобщенная структурная схема скремблера. Сравнительный анализ скремблеров различных видов. 3. Защита информации от утечки по акустическим каналам. 4. Электрические каналы утечки информации. Классификация, краткая характеристика. Паразитные емкостные, индуктивные связи. 5. Защита линий связи от утечки информации по электрическим каналам. 6. Энергетическая, структурная и информационная скрытность. Активные технические средства для обеспечения энергетической скрытности.
3.	Сети и системы передачи информации	1. Преимущества и недостатки аналоговой и цифровой связи. Связь теорем Шеннона и Найквиста 2. Увеличение точности воспроизведения, ширина полосы и задержки при использовании ИКМ. 3. Центральная частота сигнала. Потенциальная скорость передачи данных. Минимальная теоретическая ширина полосы системы, требуемая для определения R сигналов с/без ISI 4. Виды модуляции. Цели применения полосовой модуляции. Смеситель частот. 5. Согласованные и оптимальные фильтры. 6. Виды замирания, параметры их описания.. 7. Способы распределения ресурсов связи. Сравнительный анализ уплотнения и множественного доступа. 8. Методы расширения спектра. 9. Мобильные системы связи на примере систем стандарта. Устойчивость прямого и обратного каналов при приеме.

		10. Каналы с памятью. Примеры. Идея чередования битов кодирования сообщения. Код Грэя. Цель и принцип решетчатого кодирования.
4.	Криптографические методы защиты информации	1. Типы криптоанализа шифрованных сообщений. Понятие защищенности шифрованных сообщений. 2. Классификация шифров по ключевой информации. 3. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть, KASLT-сеть. 4. Аппаратное шифрование DES: структура, перестановки, сеть Файштеля, расширение ключа. 5. Ассиметричная криптография и электронная цифровая подпись. Понятия. 6. Алгоритм RSA (асимметричная криптография).
5.	Программно-аппаратные средства обеспечения информационной безопасности	1. Использование eToken Network Logon для кардинального решения проблемы «слабых» паролей? 2. Использование электронных ключей Sentinel для защиты программного обеспечения. Назначение ключей Master Key и Developer Key. Варианты построения защиты. 3. Основное назначение продукта Рутокен Web. Рутокен Web: модели, описание характеристик, преимущества, внедрение. 4. Использование электронных ключей Guardant для защиты программного обеспечения. Guardant: модели, описание характеристик, преимущества использования. 5. Система защиты информации ViPNet - назначение и структура. ViPNet: Administrator, Coordinator, Client.
6.	Проектирование защищенных телекоммуникационных систем	1. Понятие процесса проектирования, постановка задачи управления процессом проектирования 2. Модель взаимодействия открытых систем, размещение услуг и механизмов защиты на уровнях модели. 3. Уровневая архитектура мультисервисной сети. 4. Общи принципы проектирования VPN для сети на базе технологии многопротокольной коммутации по меткам (MPLS). 5. Общие принципы автоматизации процесса проектирования, общие требования к применению инструментальных программных средств 6. Нормативно-методическое обеспечение разработки защищённых телекоммуникационных систем. 7. Разработка условия системной интеграции базовых процессов обеспечения безопасности ТКС

		8. Разработка модели образования угрозы. Место модели в системной интеграции процессов обеспечения безопасности ТКС. 9. Разработка модели идентификации угрозы. Место модели в системной интеграции процессов обеспечения безопасности ТКС. 10. Разработка модели нейтрализации угрозы. Место модели в системной интеграции процессов обеспечения безопасности.
7.	Теория радиотехнических сигналов	1. Математические модели и классификация радиотехнических сигналов 2. Основные свойства преобразований Фурье и их использование при определении спектров сигналов. 3. Динамическое представление сигналов посредством функций включения и дельта-функций, понятие обобщенных функций. 4. Автокорреляционные функции периодического и непериодического сигналов, их взаимосвязь с соответствующими энергетическими спектрами. 5. Энергетический спектр сигнала: физический смысл, распределение мощности в спектре сигнала, соотношение между длительностью сигнала и шириной его спектра. 6. Взаимная корреляционная функция двух сигналов, ее свойства и взаимосвязь с взаимным энергетическим спектром этих сигналов.
8.	Теория информации и кодирования	1. Совокупность каких объектов составляют систему. передачи информации? 2. Теорема Котельникова и ее применение в теории информации. 3. Связь между понятиями количества информации и энтропии. 4. Характеристики дискретного канала связи. 5. Пропускная способность канала передачи информации. 6. Теорема Шеннона о кодировании канала связи без помех и с помехами.
9.	Теория принятия решений в условиях информационных конфликтов	1. Экспертное оценивание при принятии решения в условиях информационных конфликтов. Метод Дельфи. 2. Основные положения применения марковских процессов для синтеза модели решения. 3. Структуризация причинно-следственных связей при формировании решения в условиях информационного конфликта. 4. Разработка модели решения при обеспечении безопасности телекоммуникационных систем.

		5. Сетевое планирование для синтеза модели решения.
10.	Аппаратные средства телекоммуникационных систем	1. Архитектура микроконтроллера. Средства поддержки разработок микропроцессорных систем на базе микроконтроллеров 2. Система прерываний микроконтроллера 3. АЦП и ЦАП микроконтроллера 4. Устройства памяти микроконтроллера. Режимы адресации и система команд микроконтроллера 5. Последовательные интерфейсы UART и SPI 6. Назначение, режимы работы и функции счетчиков/таймеров 7. Аналоговый компаратор микроконтроллера
11.	Управление информационной безопасностью телекоммуникационных систем	1. Обеспечение информационной безопасности. Основные понятия и определения. Угрозы безопасности в телекоммуникационных системах. Три подхода к информационной безопасности. 2. Нормативный подход. Классические стандарты информационной безопасности. 3. Управление доступом. Теоретический подход. Модель Харрисона – Руззо - Ульмана. 4. Система шифрования с открытым ключом. Стандарты хэширования и цифровой подписи. Управление криптографическими ключами 5. Защита сетей от удаленных атак с помощью межсетевых экранов 6. Технология виртуальных корпоративных сетей. 7. Основные понятия управления информационной безопасности (УИБ). 8. Основные этапы управления информационной безопасности(УИБ). 9. Система управления информационной безопасности (ИБ)организации . 10. Политика систем управления информационной безопасности (СУИБ) 11. Стратегия построения и внедрения систем управления информационной безопасности (СУИБ)
12.	Защита программных средств защищенных телекоммуникационных систем	1. Защита и лицензирование приложений с помощью программных ключей Sentinel. 2. Защита программного обеспечения с использованием привязки к конфигурации оборудования. 3. Электронные цифровые сертификаты. Протокол https. 4. Программные и аппаратные кейлоггеры. Виды информации, которые могут контролироваться. Методы защиты от несанкционированно установленных кейлоггеров. 5. Разработка защищенных программ.

		Защищенное программирование. Типичные ошибки. Уязвимости форматной строки. Аутентификация.
13.	Операционные системы	1. Управление потоками и процессами в современной, многозадачной ОС 2. Оперативная память, как управляемый ресурс операционной системы 3. Какими операционными системами поддерживаются файловые системы: ext3, ext4, proc, sysfs, fat16, fat32 и ntfs. 4. Виды разделяемых библиотек в операционных системах. 5. Политика безопасности в операционных системах: Unix-подобные и Windows.
14.	Телекоммуникационные системы	1. Структурная схема типовой ТКС. Диапазоны волн, виды модуляции используемые в ТКС. 2. Радиорелейные и тропосферные линии связи. Структурные схемы. Принцип работы. 3. Спутниковые ТКС. Принцип работы. Функциональные схемы. 4. Сотовая мобильная радиосвязь. Принцип построения систем сотовой связи. Оценка числа пользователей на одну сторону.

К итоговому междисциплинарному экзамену допускаются студенты, полностью выполнившие учебный план, включая все виды практик.

Для подготовки студентов к сдаче государственного экзамена по отдельным разделам выносимых на экзамен дисциплин проводятся установочные лекции. Экзаменационные вопросы предварительно сообщаются студентам в виде электронного файла не менее чем за две недели до экзамена.

Порядок проведения государственного экзамена

Государственный междисциплинарный экзамен принимается государственной экзаменационной комиссией, входящей в состав государственной аттестационной комиссии. Государственная экзаменационная комиссия формируется из преподавателей кафедры Информационных технологий и систем безопасности, а также сторонних специалистов.

Для ответа на билеты студентам предоставляется возможность подготовки в течение не менее 30 минут. Для ответа на вопросы билета каждому студенту предоставляется время для выступления (не более 15 минут), после чего председатель государственной экзаменационной комиссии предлагает ее членам задать студенту дополнительные вопросы в рамках тематики вопросов в билете. Если студент затрудняется при ответе на дополнительные вопросы, члены комиссии могу задать вопросы в рамках тематики программы государственного междисциплинарного экзамена. По решению председателя государственной экзаменационной комиссии студента могут попросить отвечать на дополнительные вопросы членов комиссии и после его ответа на отдельный

вопрос билета, а также ответить на другие вопросы, входящие в программу государственного междисциплинарного экзамена.

Ответы студентов оцениваются каждым членом комиссии, а итоговая оценка по пятибалльной системе выставляется в результате закрытого обсуждения. При отсутствии большинства в решении вопроса об оценке, решающий голос принадлежит председателю государственной экзаменационной комиссии по приему междисциплинарного экзамена.

Результаты государственного междисциплинарного экзамена объявляются в день его проведения после оформления протокола заседания государственной аттестационной комиссии.

Критерии оценки ответа обучающегося на экзаменационные вопросы

Оценка знаний студента производится по следующим критериям:

- **оценка «отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, причем не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения;

- **оценка «хорошо»** выставляется студенту, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;

- **оценка «удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;

- **оценка «неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

V. Требования, порядок и критерии оценки результатов защиты ВКР

Выпускная квалификационная работа является одним из видов аттестационных испытаний выпускников, завершающих обучение по основной профессиональной образовательной программе высшего профессионального образования, и проводится в соответствии с Положением об государственной итоговой аттестации выпускников высших учебных заведений Российской Федерации. В соответствии с учебным планом университета подготовка и защита выпускной квалификационной работы осуществляется на завершающем этапе обучения и является основным элементом итоговой аттестации. Выпускная квалификационная работа подводит итог обучения студента в высшем учебном заведении. Она призвана выявить уровень профессиональных знаний, умений, навыков студента, полученных им в течение всего срока обучения, а также

способность студента на основе полученных знаний самостоятельно решать конкретные практические задачи.

Темы выпускных квалификационных работ определяются кафедрой, и утверждаются приказом ректора университета. Студенту предоставляться право выбора темы выпускной квалификационной работы в порядке, установленном университетом, вплоть до предложения своей темы с необходимым обоснованием целесообразности ее разработки. Для подготовки выпускной квалификационной работы студенту назначается руководитель и, при необходимости, консультанты.

Выпускная квалификационная работа выполняется студентом самостоятельно под руководством дипломного руководителя в форме дипломной работы. По структуре состоит из теоретической и практической части. В теоретической части дается теоретическое освещение темы на основе анализа имеющейся литературы. Практическая часть может быть представлена методикой, расчетами, анализом экспериментальных данных, продуктом творческой деятельности в соответствии с видами профессиональной деятельности.

Выпускная квалификационная работа должна быть выполнена на актуальную тему, иметь научную новизну и практическую значимость.

Выпускные квалификационные работы подлежат рецензированию. Порядок рецензирования устанавливается университетом.

Условия и сроки выполнения выпускных квалификационных работ устанавливаются Ученым советом университета.

На защиту квалификационной работы отводится до 25 минут. Процедура защиты устанавливается председателем государственной аттестационной комиссии по согласованию с членами комиссии и, как правило, включает доклад студента (не более 10–15 минут), чтение отзыва и рецензии, вопросы членов комиссии, ответы студента.

Порядок оформления выпускной квалификационной работы, требования к структуре и содержанию, процедура защиты представлены в Методических указаниях по выполнению выпускных квалификационных работ.

Примерная тематика выпускных квалификационных работ

№ п/п	Темы для ВКР
1.	Подготовка методики проведения аудита информационной безопасности
2.	Проблемы и уязвимости современного Интернета вещей, методы противодействия им
3.	Угрозы и уязвимости промышленного Интернета вещей, методы противодействия им
4.	Проблемы и уязвимости современных Wi-Fi сетей, методы обнаружения и противодействия им
5.	Разработка технологии управления процессами обеспечения информационной безопасности и функционирования сайта
6.	Технология управления процессами обеспечения безопасности виртуальной сети
7.	Модель системы обеспечения безопасности на основе применения алгоритмов шифрования
8.	Методика обеспечения безопасности на основе двухфакторной защиты
9.	Анализ безопасности сети организации
10.	Анализ безопасности веб-сайта предприятия
11.	Получение конфиденциальных данных методами социальной инженерии
12.	Практические методы и средства тестирования на проникновение в корпоративные

	сети
13.	Применение нейронных сетей для обнаружения атак на сеть предприятия
14.	Эксплуатация уязвимостей wi-fi сетей
15.	Разработка устройств для тестов на проникновение
16.	Перехват данных в защищенной беспроводной сети
17.	Проникновение в информационно-вычислительную сеть предприятия с использованием методов социальной инженерии
18.	Внедрение вредоносных кодов в информационно-вычислительную сеть предприятия посредством методов социальной инженерии
19.	Система журналирования как основа для расследования киберпреступлений
20.	Расследование киберпреступлений с помощью DLP систем
21.	Защита распределённых данных предприятия с использованием ассиметричной криптографии
22.	Разработка распределенной системы обнаружения вторжений
23.	Разработка методики обеспечения безопасности распознавания биометрических характеристик личности
24.	Разработка методики обеспечения информационной безопасности деятельности в условиях цифровой экономики
25.	Методика обеспечения информационной безопасности при реализации технологии облачных вычислений
26.	Методика комплексного обеспечения информационной безопасности организации
27.	Построение модели действия злоумышленника при удаленной атаке
28.	Методика оценивания алгоритмов обнаружения вторжений в компьютерные сети
29.	Разработка методики аутентификации в сетях связи корпоративного назначения
30.	Разработка защищённого информационного портала организации с применением API сторонних сервисов
31.	Проектирование защищенной локальной вычислительной сети предприятия на базе Cisco Packet Tracer
32.	Проектирование защищенной локальной вычислительной сети на базе управляемого сетевого оборудования компаний Plink, Zuxel и Cisco
33.	Принципы построения защищенной сети предприятия на базе технологии VPN
34.	Моделирование систем анализа проектных решений баз персональных данных
35.	Использование нечетко-нейросетевых методов в задачах защиты персональных данных
36.	Обеспечение информационной безопасности объекта посредством беспроводной передачи энергии
37.	Обеспечение информационной безопасности объекта с помощью сейсмоакустических датчиков
38.	Информационная безопасность в IoT-устройстве
39.	Защита сетевого оборудования от взлома
40.	Безопасность гипервизора и его реализация на ARM процессоре
41.	Проектирование защищённой системы управления автоматизированными сооружениями по защищённому каналу связи
42.	Безопасность контейнера и способы его реализации

Критерии оценки результатов защиты ВКР

Оценка результата защиты выпускной квалификационной работы студента производится на закрытом заседании ГАК. За основу принимаются следующие критерии:

- актуальность темы;
- научно-практическое значение темы;
- качество выполнения работы;
- содержательность доклада и ответов на вопросы;

- наглядность представленных результатов в форме иллюстраций.

Обобщенная оценка защиты выпускной квалификационной работы определяется с учетом отзыва научного руководителя и оценки рецензента.

Результаты защиты выпускной квалификационной работы оцениваются по четырехбалльной системе:

-**оценка «отлично»** присваивается за глубокое раскрытие темы, качественное оформление работы, содержательность доклада и презентации;

-**оценка «хорошо»** присваивается при соответствии вышеперечисленным критериям, но при наличии в содержании работы и ее оформлении небольших недочетов или недостатков в представлениирезультатов к защите;

-**оценка «удовлетворительно»** присваивается за неполное раскрытие темы, выводов и предложений, носящих общий характер, отсутствие наглядного представления работы и затруднения при ответах на вопросы;

-**оценка «неудовлетворительно»** присваивается за слабое и неполное раскрытие темы, несамостоятельность изложения материала, выводы и предложения, носящие общий характер, отсутствие наглядного представления работы и ответов на вопросы.

VI. Информационное методическое обеспечение ГИА

В соответствии с ФГОС ВО библиотечный фонд университета укомплектован необходимым количеством печатных изданий основной и дополнительной литературы по всем дисциплинам (модулям) и практикам образовательной программы. Кроме того, обучающиеся обеспечиваются индивидуальным неограниченным доступом к электронно-библиотечным системам (ЭБС).

В университете функционирует электронная информационно-образовательная среда (ЭИОС), представляющая совокупность электронных информационных и образовательных ресурсов, информационных и телекоммуникационных технологий и соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ или их частей, а также взаимодействие обучающихся с научно-педагогическими работниками.

ЭБС и ЭИОС доступны для каждого студента из любой точки, в которой имеется доступ к сети Интернет, как на территории университета, так и вне его.

Университет обеспечен необходимым комплектом лицензионного программного обеспечения.

Обучающимся в процессе освоения образовательной программы предоставляется доступ к современным профессиональным база данных и информационным справочным системам.

VII. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. —

(Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.

2. Щеглов, А. Ю. Защита информации: [Электронный ресурс] основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2018. — 309 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5.- Режим доступа https://biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E/zaschita-informacii-osnovy-teorii

3. Теория передачи дискретных сообщений [Текст] : конспект лекций / Е. А. Чернецова ; РГГМУ. - Санкт-Петербург : РГГМУ, 2007. - 163 с. - 86.00 р.

4. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422.

5. Ананченко, И.В., Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие / И.В Ананченко, П.И. Смирнов, Ю.М. Шапаренко. – СПб.: РГГМУ, – 2016. – 24 с., ил. - Режим доступа: http://elib.rshu.ru/files_books/pdf/rid_934e2a15ca2e4a408df0517464e9941f.pdf

6. Методология проектной деятельности инженера-конструктора : учебное пособие для бакалавриата и магистратуры / А. П. Исаев [и др.] ; под ред. А. П. Исаева, Л. В. Плотникова, Н. И. Фомина. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 211 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-05408-8. — Режим доступа : www.biblio-online.ru/book/A67869E0-BF44-427A-9B45-607F9EA8D61C

7. Осокин, А. Н. Теория информации : учебное пособие для прикладного бакалавриата / А. Н. Осокин, А. Н. Мальчуков. — М. : Издательство Юрайт, 2018. — 205 с. — (Серия : Университеты России). — ISBN 978-5-9916-7064-7. — Режим доступа : www.biblio-online.ru/book/1D5E1FA9-0F42-4040-A1F4-269E2063616F.

8. Теория принятия решений в 2 т. Том 1 : учебник и практикум для бакалавриата и магистратуры / В. Г. Халин [и др.] ; под ред. В. Г. Халина. — М. : Издательство Юрайт, 2018. — 250 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03486-8. — Режим доступа : www.biblio-online.ru/book/A018513D-5154-4C62-A55D-A980760C0FF4

9. Сажнев, А. М. Цифровые устройства и микропроцессоры : учебное пособие для академического бакалавриата / А. М. Сажнев. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 139 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-04946-6. — Режим доступа : www.biblio-online.ru/book/1BE9378D-3F7B-44A0-A1BC-79B0C8B2EFAE

10. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. «Основы управления информационной безопасностью» Издательство: Горячая линия-Телеком. 2014г. 244с.

11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0.- Режим доступа: https://biblio-online.ru/viewer/E458AFCD-826E-4A1F-9BAB-68BB83EA616F

12. Гостев, И. М. Операционные системы : учебник и практикум для академического бакалавриата / И. М. Гостев. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 164 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-04520-8. — Режим доступа : www.biblio-online.ru/book/A14759F4-CD1C-441C-A929-64B9D29C6010

13. Романюк, В. А. Основы радиосвязи : учебник для вузов / В. А. Романюк. — М. : Издательство Юрайт, 2018. — 288 с. — (Серия : Специалист). — ISBN 978-5-534-00675-9.- Режим доступа: https://biblio-online.ru/viewer/CC68C413-4FDC-42E2-A711-CC528D1778BA/os (сделана ссылка)

14. Телекоммуникационные системы и сети: Учебное пособие. Телекоммуникационные системы и сети. Том 2. Радиосвязь, радиовещание, телевидение[Электроный ресурс] /Катунин Г. П., Мамчев Г. В., Попантонопуло В. Н., Шувалов В. П., 3-е изд., стереотип. - М.: Гор. линия-Телеком, 2014. - 672 с.: 60x90 1/16. - (Специальность) (Обложка) ISBN 978-5-9912-0338-8 - Режим доступа: http://znanium.com/bookread2.php?book=490318

б) дополнительная литература:

1. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. - ISBN 978-5-98704-513-8. - Режим доступа: http://znanium.com/bookread2.php?book=469026

2. Технические средства и методы защиты информации: Учебник для вузов [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - М.: Гор. линия-Телеком, 2012. - 442с.; 60x90 1/16 - (Уч. для вузов). (о) ISBN 978-5-9912-0233-6 -Режим доступа: http://znanium.com/bookread2.php?book=390284

3. Системы и сети передачи информации. В 2-х ч. [Текст] : учебное пособие. Ч. 1. Системы передачи информации. / РГГМУ ; РГГМУ. - Санкт-Петербург : [б. и.], 2008. - 199(3) с. - 124.19 р.

4. Криптографические методы защиты информации. Ч. 1. Основы криптографии. [Текст] : учебное пособие / П. П. Бескид, Татарникова Т.М. ; РГГМУ. - Санкт-Петербург : РГГМУ, 2010. - 94 с. - 70.40 р.

5. Программно-аппаратные средства обеспечения информационной безопасности [Текст] : учебное пособие / А. В. Душкин [и др.] ; ред. А. В. Душкин. - Москва : Горячая линия -Телеком, 2017. - 247 с. - ISBN 978-5-9912-0470-5 : 619.00 р.

6. Трухин, М. П. Основы компьютерного проектирования и моделирования радиоэлектронных средств. Лабораторный практикум : учебное пособие для вузов / М. П. Трухин ; под науч. ред. В. Э. Иванова. — М. : Издательство Юрайт, 2018. — 134 с. — (Серия : Университеты России). — ISBN 978-5-9916-9925-9. — Режим доступа : www.biblio-

online.ru/book/9C4DFDB0-AD84-42B0-827D-0DDCCBDED541

7. Иванов, И. В. Теория информационных процессов и систем + доп. Материалы в ЭБС : учебное пособие для академического бакалавриата / И. В. Иванов. — 3-е изд., пер. и доп. — М. : Издательство Юрайт, 2018. — 228 с. — Режим доступа: https://biblio-online.ru/book/0FC64B65-4A23-4530-84FD-E0E281C849C7/teoriya-informacionnyh-processov-i-sistem-dop-materialy-v-ebs

8. Кравченко, Т. К. Системы поддержки принятия решений : учебник и практикум для академического бакалавриата / Т. К. Кравченко, Д. В. Исаев. — М. : Издательство Юрайт, 2018. — 292 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-8563-4. — Режим доступа : www.biblio-online.ru/book/B2FF1983-705C-49F2-BE27-1362F66D576E

9. Макуха, В. К. Микропроцессорные системы и персональные компьютеры : учебное пособие для вузов / В. К. Макуха, В. А. Микерин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 175 с. — (Серия : Университеты России). — ISBN 978-5-534-04791-2. — Режим доступа : www.biblio-online.ru/book/4F29CE67-3B2B-4289-BA38-9FDE247F3D62

10. Бурлов В.Г. «Математические методы моделирования в экономике. Часть 1» Издательство НПО «Стратегия будущего», 2008, СПБ, 330с.

11. Проектирование защищенных информационных систем [Текст] : учебное пособие. Ч. 1. Конструкторское проектирование. Защита от физических полей. . П. П. Бескид, В. Ю. Суходольский, Ю. М. Шапаренко. – СПб.: Изд-во РГГМУ, 2008. – 195 с.

12. Плескунов, М. А. Операционное исчисление : учебное пособие для вузов / М. А. Плескунов ; под науч. ред. А. И. Короткого. — М. : Издательство Юрайт, 2018. — 141 с. — (Серия : Университеты России). — ISBN 978-5-534-05500-9. — Режим доступа : www.biblio-online.ru/book/6C01AABE-577C-408E-8E0B-A2789BAD11ED

13. Радиотехнические цепи и сигналы. Лабораторный практикум/Баскей В.Я., Меренков В.М., Соколова Д.О. и др. - Новосиб.: НГТУ, 2014. - 113 с.: ISBN 978-5-7782-2395-0. - Режим доступа: http://znanium.com/bookread2.php?book=546203

14. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для академического бакалавриата / К. Е. Самуйлов [и др.] ; под ред. И. А. Шалимова. — М. : Издательство Юрайт, 2017. — 363 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-00256-0. — Режим доступа : www.biblio-online.ru/book/D02057C8-9C8C-4711-B7D2-E554ACBBBE29

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web

Интернет-ресурсы

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум

- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

VIII. Особенности ГИА для инвалидов и лиц с ограниченными возможностями здоровья

ГИА обучающихся с ограниченными возможностями здоровья при необходимости осуществляется с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При проведении ГИА с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для сдающих ГИА из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

IX. Материально-техническое обеспечение ГИА

Аудитории для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Аудитории для проведения государственной итоговой аттестации - укомплектована специализированной (учебной) мебелью, техническими средствами для представления результатов выпускной квалификационной работы.

Рассмотрено и рекомендовано к использованию в учебном процессе на 2019/2020 учебный год без изменений.

Протокол заседания кафедры ИТиСБ от 07.05.2019 №5