МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ ИММАНУИЛА КАНТА

Институт физико-математических наук и информационных технологий

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ В.И.Бурмистров
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«20» марта 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Подготовка к процедуре защиты выпускной квалификационной работы»

для студентов 4 курса
очной формы обучения

направления подготовки 10.03.01.
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.

Лист согласования

Составители: доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно–методического совета института физико-математических наук и информационных технологий.

Протокол № __/__ от «__» _____ 20__ г.

Председатель учебно-методического совета _____первый заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) _____

Протокол №____ от «___ »_____20_ г.

Ведущий менеджер ООП _____Бурмистров В. И.

СОДЕРЖАНИЕ
ПРОГРАММЫ ПОДГОТОВКИ К ПРОЦЕДУРЕ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по направлению подготовки 10.03.01 «Информационная безопасность», уровень высшего образования - бакалавриат…….……...4
1.1. Общие положения……..…..4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы……5
1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся……...37
2. Порядок подготовки к защите выпускной квалификационной работы …..…37
2.1. Процессы подготовки защиты выпускной квалификационной работы……37
2.2. Требования и нормы подготовки выпускной квалификационной работы…38
2.3. Описание показателей и критериев оценивания компетенций……..43
2.4. Шкала оценивания степени сформированности компетенций……..…44
3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины…….....….46
4. Фонд оценочных средств для проведения ГИА ……..….49
4.1. Примерная тематика выпускных квалификационных работ по направлению подготовки 10.03.01 «Информационная безопасность»……82
4.2. Примеры формулировки тем и содержания выпускных квалификационных работ……...84
Приложения……...……87

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по направлению подготовки 10.03.01 «Информационная безопасность», уровень высшего образования – бакалавриат

1.1. Общие положения

Программа ГИА является частью основной профессиональной образовательной программы в соответствии с ФГОС ВО в части государственных требований к минимуму содержания и уровню подготовки выпускников по направлению подготовки 10.03.01 «Информационная безопасность».

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по основной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные утвержденным учебным планом направления подготовки 10.03.01 «Информационная безопасность».

Видом ГИА в соответствии с п. 2.7 ФГОС ВО и учебным планом является защита выпускной квалификационной работы.

Аттестацию проводит Государственная Экзаменационная Комиссия (ГЭК). Председатель ГЭК и состав ГЭК утверждаются в установленном порядке.

Выпускная квалификационная работа выполняется в обязательном порядке, в установленные сроки, проходит рецензирование (в необязательном порядке) и защищается в ГЭК.

Государственная итоговая аттестация (ГИА) включает в себя два основных этапа - этап подготовки к процедуре защиты выпускной квалификационной работы (Б3.01(Д)) и процедуру защиты выпускной квалификационной работы Б3.02(Д).

Наименование дисциплины (модуля) - «Подготовка к процедуре защиты выпускной квалификационной работы».

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины «Подготовка к процедуре защиты выпускной квалификационной работы» является подготовка к защите выпускной квалификационной работы.

При выполнении выпускной квалификационной работы, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Выпускник направления подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Организация и технология защиты информации» в соответствии с целями основной образовательной программы и типами задач профессиональной деятельности в результате освоения данной дисциплины должен обладать компетенциями, представленными в таблице

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ОК-1	Способностью использовать основы философских знаний для формирования мировоззренческой позиции	**Знать**: современные представления о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека, о многообразии форм человеческого знания, соотношении истины и заблуждения, знания и веры, рационального и иррационального в человеческой жизнедеятельности, особенностях функционирования знания в современном обществе, духовных ценностях, их значении в творчестве и повседневной жизни, научиться ориентироваться в них **Уметь**: характеризовать культурно-исторические явления и памятники; формулировать гипотезы о причинах и особенностях развития исторических процессов; систематизировать факты, явления, объекты,

		изученные в курсе; систематизировать факты, явления, объекты, изученные в курсе; выделять периоды в истории развития региональных и общеисторических процессов; условия формирования личности, ее свободы, ответственности за сохранение жизни, природы, культуры, понимать роль насилия и ненасилия в истории и человеческом поведении нравственных обязанностей человека по отношению к другим и самому себе. рассмотреть представления о сущности сознания, его взаимоотношении с бессознательным, роли сознания и самосознания в поведении, общении и деятельности людей, формировании личности. **Владеть**: навыками критического мышления
ОК-2	Способностью использовать основы экономических знаний в различных сферах деятельности	**Знать**: содержание основных экономических проблем, происходящих современном обществе и подходы к их решению **Уметь**: принимать самостоятельные эффективные решения на основе анализа и оценки конкретной экономической ситуации **Владеть**: навыками создания простейших эконометрических моделей
ОК-3	Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально

		профессионального характера
ОК-4	Способностью использовать основы правовых знаний в различных сферах деятельности	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера
ОК-5	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	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования
ОК-6	Способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать**: определения базовых понятий и категорий теориикоммуникации; формы, уровни и виды коммуникации; структуру коммуникационного процесса; специфику массовой коммуникации; основные положения теорий взаимодействия иаудитории; **Уметь**: дифференцировать, характеризовать и оцениватьформы, уровни и виды коммуникации; выстраивать (моделировать) коммуникацию позаданным моделям

		и видам; отличать массовую коммуникацию от других видовкоммуникации по основным параметрам – адресант, адресат, сообщение, каналы, код, эффект; дифференцировать, характеризовать и оцениватьотдельные компоненты, составляющие структуру коммуникационного процесса; дифференцировать, характеризовать и оценивать основные положения теорий взаимодействия СМК иаудитории; использовать и при необходимости трансформироватьтеоретические модели в соответствии с конкретной (реальной) коммуникативной ситуацией; оценивать особенности аудитории, удерживать иактивировать ее внимание; **Владеть**: навыками деловой коммуникации; способностью к обобщению, анализу, восприятиюинформации; базовыми навыками, составляющими коммуникативную компетентность личности, включаянавык оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и вотношении собственной личности
ОК-7	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	**Знать**: базовую лексику общего языка, лексику представляющую нейтральный научный стиль, а также основную техническую терминологию; наиболее употребительную (базовую) грамматику и основные грамматические явления, характерные для регистра научной речи лексику и фразеологию, отражающую основные направления технической науки в области радиофизики; основные элементы понимания делового письма; основные приемы аннотирования, реферирования и перевода научно-технической литературы **Уметь**: понимать устную (монологическую и диалогическую) речь на бытовые и специальные темы воспринимать на слух и участвовать в обсуждении тем, связанных со специальностью; читать и понимать со словарем научную литературу по общим и специальным вопросам **Владеть**:

		навыками разговорно-бытовой речи (владеть нормативным произношением и ритмом речи и применять их для беседы на бытовые и специальные темы) навыками чтения научной литературы с целью извлечения информации; основными навыками (неофициального и делового) письма; основными навыками публичной речи – делать научные сообщения, доклады (с предварительной подготовкой)
ОК-8	Способностью к самоорганизации и самообразованию	**Знать**: научно-психологические основы выбора, процессуально-структурные компоненты психологического феномена «выбор», основныенаправления современной этики, базовые элементы и приемы, применяемые в подготовленной публичной речи **Уметь**: составлять перспективный план жизни, с учетом возможных препятствий, решать конфликтные ситуации, опираясь на знания о стратегиях поведения, аргументированно излагать свои моральные убеждения и составлять хорошее самостоятельное публичное выступление **Владеть**: приемами самооценки, эффективного общения и слушания, позитивного общения, конгруэнтного поведения, анализа собственныхнравственных ценностей и поступков, подготовки, корректировки выступления
ОК-9	Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	**Знать**: влияние физической культуры на укрепления здоровья, профилактику профессиональных заболеваний и вредных привычек; основные средства и методы физического воспитания; основы здорового образа жизни; методы оценки физического развития, физической подготовленности средствами физической культуры и спорта в студенческом возрасте **Уметь**: использовать средства и методы физической культуры в регулировании своего психофизического состояния; выполнять комплексы упражнений оздоровительной и профессионально прикладной направленности; **Владеть**: навыком самостоятельно применять средства

		и методы физического воспитания в укреплении здоровья, методами контроля состояния организма при нагрузках; навыками ведения здорового образа жизни, участия в физкультурно-оздоровительной деятельности.
ОПК-1	Способностью анализировать физические явления и процессы для решения профессиональных задач	**Знать**: основные физические величины и понятия механики; основные физические законы, описывающие динамику материальной точки и систем материальных точек основные физические законы, описывающие динамику твердого тела основные физическиепредставления механики колебаний и волн; основные физическиепредставления гидрогазодинамики; основные понятия, законы и модели молекулярной физики основные законы классической электродинамики; основные методы электрическихизмерений фундаментальную базу теоретических знаний по оптике, основные понятия, законы и модели атомной и ядерной физики, методы математического анализа объектов и явлений микромира на основе уравнений квантовой механики; возможные сферы приложения законов имоделей атомной и ядерной физики; негативные факторы техносферы, их воздействие на человека **Уметь**: правильно соотносить содержание конкретных задач с законами физики, эффективно применять общие законы физики для решения конкретных задач в области физики и на междисциплинарных границах физики с другими областями знаний; пользоваться физическими приборами, ставить и решать простейшие экспериментальные задачи, обрабатывать, анализировать и оценивать полученные результаты; строить математическиемодели простейших физических явлений и использовать для изучения этих моделей доступный ему математический аппарат, включая методы вычислительнойматематики; использовать при работе справочную и учебную литературу, находить другие необходимые источники информации и

		работать с ними; понимать, излагать и критически анализировать базовую общефизическую информацию применять основные законы и методы электродинамики для решения прикладных задач применять основные законы и методы оптики для решения прикладных задач; студенты должны овладеть приемами и методами решения практических задач оптики, требующих использования разнообразных математических методов **владеть**: навыками использования основных законов механики и молекулярной физики для анализа различных механических и физических систем; навыками оценки на основе физических законов характера механических и физических процессов для различных систем и сред; навыками использованиематематического аппарата для решения физических задач навыками и методиками проведения электрических и магнитных измерений, конструирования контрольно-измерительных устройств и экспериментальных установок использования технических средств для определения основных параметров техно-логического процесса, изучения свойств физико-технических объектов, изделий и материалов методами обработки данных измерений физических величин, навыками работы с современным экспериментальным оборудованием, методами защиты человека от опасных и вредных факторов; способностью к правильному использованию общенаучной и специальной терминологии в профессиональной области; математическими методами и моделямидля описания физических явлений, физического эксперимента, включая методы оценки точности экспериментальных измерений
ОПК-2	Способностью применять соответствующий математический аппарат для решения профессиональных задач	**знать**: основные положения теории пределов функций, основныетеоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; основы векторного анализа основы аппарата теории обыкновенных

		дифференциальных уравнений, необходимых для решения теоретических и практических задач **уметь**: ориентироваться в постановках задач; строго доказывать математическое утверждение; определятьвозможности применения методов математического анализа; пользоваться библиотеками прикладных программ и пакетами программ для решения прикладных математическихзадач использовать математические методы при решении прикладных задач, приводящих к обыкновенным дифференциальным уравнениям **владеть**: практическими навыками решения основных задач теории пределов функций, дифференцирования, интегрирования навыками решения типовых задач с применением изучаемого теоретического материала; навыками математического исследования динамическихпроблем из различных областей физики
ОПК-3	Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	**Знать**: - принципы работы изучаемых электронных устройств ипонимать физические процессы, происходящих в них; основные законы и методы расчета электрических цепей; - назначение, принцип работы, основные характеристики и обозначение полупроводниковых элементов, операционных усилителей, интегральных сборок и устройств на их основе; - принципы построения различных вариантов схем электронных устройств с отрицательной и/или положительной обратными связями (ОС), понимать причинывлияния ОС на основные показатели и стабильность параметров изучаемых устройств; понимать причины возникновения неустойчивой работы усилителей с отрицательной ОС; - способы оценки устойчивости электронных устройствс внешними цепями ОС; - принципы и алгоритмы работы устройств формирования и генерирования сигналов; - принципы и алгоритмы работы радиоприемных - - устройств и устройств обработки сигналов; принципиальные схемы и элементную базу

		устройств, осуществляющих модуляцию и детектирование сигналов. **Уметь**: - объяснять физическое назначение элементов и влияниеих параметров на электрические параметры и частотные свойства базовых каскадов аналоговых схем; - применять на практике методы исследования аналоговых электронных устройств, основанных на аналитических и графо-аналитических процедурах анализа; - выполнять расчеты, связанные с выбором режимов работы и определением параметров изучаемых электронных устройств; - формировать цепи ОС с целью улучшения качественных показателей и получения требуемых форм характеристик аналоговых электронных устройств; - проводить компьютерное моделирование и проектирование аналоговых и инфокоммуникационных электронных устройств, а также иметь представление о методах компьютерной оптимизации таких устройств; - пользоваться справочными материалами («Datasheet») на аналоговые и цифровые элементы и ИС при проектировании телекоммуникационных устройств; - определять причины неисправностей инфокоммуникационных устройств и выбраковывать неисправные элементы; составлять, подготавливать и заполнять техническую документацию, требуемую в порядке эксплуатации инфокоммуникационного оборудования **Владеть**: - навыками чтения и изображения электронных схем на основе современной элементной базы; - навыками составления эквивалентных схем на базепринципиальных электрических схем изучаемых устройств; - навыками проектирования и расчета простейших аналоговых и цифровых схем; - навыками работы с контрольно-измерительной аппаратурой; - навыками компьютерного моделирования и проектирования аналоговых и цифровых телекоммуникационных устройств; навыками поиска и устранения простых неисправностей
ОПК-4	Способностью понимать	**Знать**:

	значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования
ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	**Знать**: структуру системы управления информационной безопасность; приемы управлению информационной безопасностью методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз **Уметь**: выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте. **Владеть**: правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления
ОПК-6	Способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций,	**Знать**: правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности» поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу

	организовать мероприятия по охране труда и технике безопасности	радиоактивных веществ (РВ) и ХОВ, современных средств поражения анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов методы прогнозирования и оценки ЧС сигналы оповещения ГО и порядок действий населения по сигналам порядок и содержание работ руководителей предприятий, учреждений, организаций, независимо от их организационно-правовой формы, а также их подразделений по управлению действиями подчиненных в ЧС в соответствии с получаемой специальностью средства и методы повышения безопасности, экологичности и устойчивости технических средств и технологических процессов **Уметь**: проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям эффективно применять средства защиты от негативных воздействий разрабатывать мероприятия по повышению безопасности и экологичности производственнойдеятельности планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных и других неотложных работ при ликвидации последствий чрезвычайных ситуаций составлять планы мероприятий по повышению собственной адаптивности анализировать, выявлять и конструировать собственные адаптивные стратегии четко действовать по сигналам оповещения, практически выполнять основные мероприятия защиты от опасностей, возникающих при ведении военных действий или вследствие этих действий, атак же от ЧС природного и техногенного характера **Владеть**: методами прогнозирования чрезвычайных ситуаций и предотвращения их негативных последствий методами повышения безопасности, экологичностии устойчивости технических средств и технологических процессов

		некоторыми методами повышения стрессоустойчивости. способами управления эмоциями в экстремальных ситуациях
ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**Знать**: основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования особенности различных подходов к организации информационного обеспечения особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне **Уметь**: вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач проектировать, оценивать и реализовывать информационное обеспечение информационных систем осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне **Владеть**: основными методами кодирования и декодирования информации для различных задач средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом

		уровне
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать**: способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; **Уметь**: классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения **Владеть**: навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	**Знать**: основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;

	профессиональных задач	защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; **Уметь**: определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий **Владеть**: методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	**Знать**: задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Уметь**: применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Владеть**: средствами защиты информации в процессе хранения и передачи данных и методами их тестирования;

		методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знать**: этапы и модели жизненного цикла информационных систем; корпоративные стандарты и методики; принципы хранения, защиты, передачи и получения информации в корпоративных сетях **Уметь**: разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных **Владеть**: навыками защиты информации в корпоративных сетях связи
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**Знать**: правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности **Уметь**: применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицироватьзащищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем **Владеть**: навыками работы с нормативными правовыми актами; навыкамиработы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на

		компонентах информационных систем на русском и иностранном языках
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры;

	проведении технико-экономического обоснования соответствующих проектных решений	принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать**: терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере **Уметь**: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации **Владеть**: навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять	**Знать**: направления создания правовой базы в области информационной безопасности; области применениянолученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при

	обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	обработке информации,составляющей государственную тайну **Уметь**: разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **Владеть**: навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**Знать**: основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности **Уметь**: определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач **Владеть**: способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками

		освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать**: физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; **Уметь**: использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач

		Владеть: навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать**: основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации **Уметь**: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью

		информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации **Владеть**: методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**Знать**: типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; **Уметь**: определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и

		оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать**: назначение, виды и принципы построения организации и управления службы защиты информации **Уметь:** применять современные компьютерные технологии для решения профессиональных задач; ориентироваться в сети научных и образовательных порталов сети Интернет; обрабатывать результаты полученных измерений с помощью математических программных продуктов **Владеть**: навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать**: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии **Уметь**: осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и

		унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации **Владеть**: навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации
ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	**Знать**: теоретические основы построения клиент-серверных веб-приложений, общие методы программирования механизмы реализации сетевых угроз по протоколам передачи данных HTTP, FTP, а также известные уязвимости веб-серверов **Уметь**: использовать полученные теоретические знания для решения конкретных прикладных задач, программировать клиент-серверные приложения с применением СУБД для обработки данных, находить и исправлять ошибки в программном коде конфигурировать клиент-серверное программное обеспечение с учетом требуемых параметров сетевой безопасности, анализировать возможные каналы утечки информации **Владеть**: практическими навыками конфигурирования и администрирования веб-серверов, а также навыками настройки систем управления контентом практическими навыками, по оценке защищенности веб-приложений

1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Подготовка к процедуре защиты выпускной квалификационной работы» составляет 6 зачетных единиц и 216 академических часов. Контактная работа обучающихся с преподавателем (по видам учебных занятий) 2 часа, Самостоятельная работа обучающихся 214 академических часов

Место и время проведения государственной итоговой аттестации

Порядок и сроки проведения аттестационных испытаний устанавливаются в соответствии с графиком учебного процесса по направлению подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации» на основании положения об организации выполнения и защиты выпускной квалификационной работы обучающимися (студентами) от 15.05.2014 г., утвержденного Ученым советом БФУ (протокол № 10 от 12 мая 2014 г.).

2. Порядок подготовки к защите выпускной квалификационной работы

2.1. Процессы подготовки защиты выпускной квалификационной работы

1. Методический руководитель направления подготовки 10.03.01 «Информационная безопасность» распределяет руководство подготовкой выпускных квалификационных работ (ВКР) среди преподавателей Института физико-математических наук и информационных технологий с требуемым уровнем квалификации и образования.
2. Обучающийся выбирает тему ВКР и совместно с научным руководителем готовит календарный план-график работы над ВКР, который подписывается студентом, научным руководителем и утверждается методическим руководителем направления.

3. На заседании Учебно-методического совета Института физико-математических наук и информационных технологий обсуждаются темы ВКР, закрепляются научные руководители. Методический руководитель направления вносит представление в приказ об утверждении тем и научных руководителей ВКР.

4. Приказом ректора утверждаются темы ВКР и закрепляются научные руководители.

5. После завершения работы над ВКР заверенная обучающимся ВКР передаётся научному руководителю для проверки.

6. Научный руководитель принимает решение о допуске к защите, которое подтверждается методическим руководителем направления.

7. Защита ВКР организуется в соответствии с графиком учебного процесса.

8. Защита ВКР проводится на открытых заседаниях ГЭК с участием не менее двух третей ее состава.

2.2. Требования и нормы подготовки выпускной квалификационной работы

2.2.1. *Общие требования к выпускной квалификационной работе*

Изложение материала в выпускной квалификационной работе должно быть последовательным и логичным. Все разделы должны быть связаны между собой. Следует обращать внимание на логические переходы от одной главы к другой, от параграфа к параграфу, а внутри параграфа – от вопроса к вопросу.

Написание текста ВКР необходимо начинать с введения и первой главы, последовательно прорабатывая все разделы, включенные в план. Изложение материала в ВКР должно быть конкретным и опираться на результаты практик, при этом важно не просто описание, а критический разбор и анализ полученных данных.

Введение – важная часть ВКР. Во введении обосновываются актуальность выбранной темы, цель и содержание поставленной задачи, формулируются объект и предмет исследования, указываются избранные методы исследования,

определяется значимость полученных результатов.

Обзор литературы – должен показать знакомство студента со специальной литературой и Интернет-источниками, его умение систематизировать материалы, критически их рассматривать, выделять существенное, оценивать ранее сделанное другими исследователями, определять главное в современном состоянии изученности темы. Результаты такого обзора следует систематизировать в определенной логической последовательности. Поскольку выпускная квалификационная работа обычно посвящается достаточно узкой теме, то обзор работ предшественников следует делать только по вопросам выбранной темы, а не по всей проблеме в целом. Обычно сюда же включается обзор предварительных сведений, на которые имеются ссылки в основной части ВКР.

При изложении в ВКР спорных вопросов темы необходимо приводить мнения различных авторов. Если в работе критически рассматривается точка зрения какого-либо автора, при изложении его мысли следует приводить цитаты, только при этом условии критика может быть объективной. Обязательным, при наличии различных подходов к решению изучаемой проблемы, является сравнение рекомендаций, содержащихся в действующих инструктивных материалах и работах различных авторов. Только после этого следует обосновывать свое мнение по спорному вопросу или соглашаться с одной из уже имеющихся точек зрения, выдвигая в любом случае соответствующие аргументы.

В главах *основной части* выпускной квалификационной работы подробно рассматриваются и обобщаются результаты исследования. Для выпускных квалификационных работ в области компьютерной безопасности и математических методов защиты информации в основную часть включается описание применяемых логических схем, математических методов и моделей, структура компьютерных программ, планы и результаты компьютерных экспериментов, способы их использования для решения поставленной задачи. Содержание глав основной части должно точно соответствовать теме работы и

полностью её раскрывать. Эти главы должны показать умение автора сжато, логично и аргументировано излагать материал.

Отдельные положения ВКР должны быть иллюстрированы соответствующими моделями и результатами расчетов, компьютерных экспериментов, цифровыми данными из справочников, монографий и других литературных источников, при необходимости оформленными в справочные или аналитические таблицы. При составлении аналитических таблиц используемые исходные данные выносятся в приложение к выпускной квалификационной работе, а в тексте приводятся расчёты отдельных показателей. Таблица должна занимать не более одной страницы. Если аналитическая таблица по размеру превышает одну страницу, её следует включать в приложение. В отдельных случаях можно заимствовать некоторые таблицы из литературных источников. Ссылаться на таблицу нужно в том месте текста, где формулируется положение, подтверждаемое или иллюстрируемое ею. В тексте, анализирующем или комментирующем таблицу, не следует пересказывать её содержание, а уместно формулировать основной вывод, к которому подводят табличные данные, или вводить дополнительные показатели, более отчётливо характеризующие то или иное явление или его отдельные стороны.

Логические и структурные схемы, а также графические модели могут оформляться в виде рисунков. Рисунок должен занимать не более одной страницы. Если рисунок по размеру превышает одну страницу, его следует включать в приложение. Ссылаться на рисунок нужно в том месте текста, где формулируется положение, подтверждаемое или иллюстрируемое им.

Все материалы, не являющиеся необходимыми для решения поставленных в работе задач, также выносятся в приложения.

Заключение – последовательное логически стройное изложение итогов работы и их соотношение с общей целью и конкретными задачами, поставленными и сформулированными во введении, а также возможных перспектив дальнейших исследований и направлений практического использования результатов работы.

Законченные главы ВКР сдаются научному руководителю на проверку в установленные планом-графиком сроки.

Проверенные главы дорабатываются в соответствии с полученными от научного руководителя замечаниями, после чего студент приступает к оформлению работы.

2.2.2. *Порядок оформления выпускной квалификационной работы*

Тексты ВКР оформляются в соответствии с едиными требованиями:

- Выпускная квалификационная работа должна быть напечатана, шрифт Times New Roman, размер шрифта 14, через 1,5-й интервал, поля: слева – 3 см, справа – 1,5 см, сверху, снизу – 2 см. Объем ВКР может быть в пределах 40-50 страниц стандартного печатного текста (без приложений). Все страницы работы (включая список литературы и приложения) последовательно нумеруются. Листы работы прошиваются.

- Каждый раздел текста ВКР начинается с новой страницы.

- Заголовки глав и разделов выделяются жирным шрифтом.

- Таблицы и рисунки могут располагаться как непосредственно в тексте ВКР, так и в приложениях. Таблицы и рисунки должны содержать заголовки и названия, достаточно полно отражающие их содержание и специфику.

2.2.3. Порядок составления отзыва и рецензии на выпускную квалификационную работу

Законченная и оформленная в соответствии с указанными выше требованиями выпускная квалификационная работа подписывается студентом и консультантами (при их наличии) и не позднее двух недель до защиты представляется научному руководителю, который даёт письменный отзыв на работу и подписывает её. ВКР, представленная позднее указанного срока, к защите не допускается.

Отзыв научного руководителя. После получения окончательного варианта ВКР научный руководитель, в недельный срок составляет письменный

отзыв, в котором всесторонне характеризует качество работы, отмечает положительные стороны, особое внимание обращает на отмеченные ранее недостатки, не устранённые студентом, обосновывает возможность или нецелесообразность представления выпускной квалификационной работы в ГЭК. В отзыве руководитель отмечает также ритмичность выполнения работы в соответствии с планом-графиком, добросовестность, определяет степень самостоятельности, активности и творческого подхода, проявленные студентом в период написания выпускной квалификационной работы, степень соответствия требованиям, предъявляемым к выпускным квалификационным работам, и рекомендует оценку. Форма отзыва представлена в приложении №4

Переплетённая работа вместе с положительным письменным отзывом научного руководителя передаётся методическому руководителю специальности на рассмотрение. Методический руководитель принимает решение о допуске работы к защите, о чём ставит соответствующую резолюцию на титульном листе работы. Образец титульного листа представлен в приложении №1.

В случае, если методический руководитель, исходя из содержания отзывов научного руководителя, а также содержания и оформления работы, не считает возможным допустить студента к защите выпускной квалификационной работы в ГЭК, вопрос об этом должен рассматриваться на заседании Учебно-методического совета Института с привлечением научного руководителя и автора работы. Решение Учебно-методического совета Института является окончательным.

Выпускные квалификационные работы, выполняемые по завершении освоения программы подготовки бакалавра, не обязательно подлежат рецензированию.

Полностью оформленная выпускная квалификационная работа, допущенная к защите методическим руководителем, направляется на рецензию.

Рецензия. В рецензии должен быть дан квалифицированный анализ существа и основных положений рецензируемой работы, оценка актуальности избранной темы, самостоятельности подхода к её раскрытию, наличия

собственной точки зрения автора, умения пользоваться методами сбора и обработки информации, степени обоснованности выводов и рекомендаций, достоверности полученных результатов, их новизну и практическую значимость. Наряду с положительными сторонами работы отмечаются недостатки, в частности, указываются отступления от логичности и грамотности изложения материала, выявляются фактические ошибки. В заключение рецензент излагает свою точку зрения об общем уровне выпускной квалификационной работы и оценивает её, после чего подписывает титульный лист работы. Объём рецензии должен составлять от одной до трех страниц машинописного текста. Рецензия должна быть получена не позднее, чем за три дня до защиты. Форма рецензии представлена в приложении №5.

После получения положительного отзыва рецензента работа передается в Государственную экзаменационную комиссию (ГЭК).

2.3. Описание показателей и критериев оценивания компетенций

Степень сформированности компетенций в ходе подготовки к защите выпускной квалификационной работы осуществляется научным руководителем и членами комиссии при знакомстве с текстом ВКР.

1. В качестве критериев для оценки ВКР научные руководители и члены ГЭК должны иметь в виду:

- актуальность темы и задач работы;
- соответствие тематики направлению подготовки «Информационная безопасность»;
- обоснованность результатов и выводов;
- определенную оригинальность и новизну полученных данных;
- самостоятельность (личный вклад студента);
- возможности практического использования полученных результатов.

2. Обоснованность результатов и выводов определяются с позиций:

- соответствия известным научным положениям и фактам;
- логичности в изложении и обсуждении собственных данных;

- корректности постановки опыта, эксперимента;
- корректности использования математических методов.

При этом должны учитываться:

- уровень устного доклада на защите;
- соответствие оформления работы установленным требованиям;
- качество иллюстративного материала к докладу.

3. Оригинальность и новизна полученных данных определяется как:

- установление нового научного факта или подтверждение известного факта для новых условий;
- получение сведений, приводящих к формулировке проверяемых гипотез, которые требуют дальнейшей проверки;
- разработка оригинального метода решения известной задачи;
- применение известных методик для решения новых задач;
- введение в научный оборот новых данных;
- обоснованное решение поставленной задачи.

4. Личный вклад студента определяется: степенью самостоятельности в выборе темы, постановке задач, планировании и организации исследования, обработке и осмыслении полученных результатов.

5. Возможность практического использования данных, полученных в ВКР, определяется в отношении НИР, выполняемых в университете или в других организациях; задачами совершенствования учебного процесса; возможностью публикации в печати.

2.4. Шкала оценивания степени сформированности компетенций

Выпускная квалификационная работа оценивается по четырёхбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

ВКР, получающая по мнению руководителя или рецензента оценку «неудовлетворительно», может быть в отдельных случаях направлена на дополнительное рецензирование по распоряжению председателя ГЭК.

Оценка «Отлично» выставляется за выпускную квалификационную работу, которая имеет исследовательский характер, грамотно изложенную теоретическую часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. ВКР имеет положительный отзыв научного руководителя и рецензента.

Оценка «Хорошо» выставляется за выпускную квалификационную работу, которая содержит элементы научного исследования, грамотно изложенную теоретическую часть, последовательное изложение материала соответствующими выводами, однако с не вполне обоснованными предложениями. ВКР имеет положительный отзыв научного руководителя и рецензента.

Оценка «Удовлетворительно» выставляется за выпускную квалификационную работу, которая имеет технический характер. ВКР базируется на практическом материале, но анализ выполнен поверхностно, в ней просматривается непоследовательность изложения материала. Представлены необоснованные предложения. ВКР имеет реферативный или обзорный характер с элементами анализа и оригинальности. В отзывах научного руководителя и рецензента имеются замечания по содержанию работы и методике анализа.

Оценка «Неудовлетворительно» выставляется за выпускную квалификационную работу, которая не носит исследовательского характера, не отвечает требованиям, изложенным в методических рекомендациях. В работе нет выводов, либо они носят декларативный характер. В отзывах научного руководителя и рецензента имеются серьезные критические замечания.

Итоговая оценка ГЭК выводится по принципу учета оценок большинства членов ГЭК, а также руководителя. Оцениваемые компетенции и оценочный лист приведены в приложениях 2 и 3, соответственно.

3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/13931.html

Дополнительная литература

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р.

Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)

4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/ В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего

/all 15: УБ(14), ч.з.N3(1)

Перечень интернет-источников

1. «Национальная электронная библиотека» (http://xn--90ax2c.xn--p1ai/).
2. ЭБС Кантиана (https://elib.kantiana.ru/).
3. ЭБС IPR BOOKS (https://www.iprbookshop.ru/78574.html).
4. ЭБС Znanium (https://znanium.com/catalog/document?id=333215).

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта http://lms-3.kantiana.ru/.
2. Использование электронной образовательной среды БФУ им. И. Канта https://teams.microsoft.com/

4. Фонд оценочных средств для проведения ГИА

Компетенция	Перечень планируемых результатов	Диагностический инструмент	Критерии оценки
ОК-1 Способностью использовать основы философских знаний для формирования мировоззренческой позиции	**Знать**: современные представления о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека, о многообразии форм человеческого знания, соотношении истины и заблуждения, знания и веры, рационального и иррационального в человеческой жизнедеятельности, особенностях функционирования знания в современном обществе, духовных ценностях, их значении в творчестве и повседневной жизни, научиться ориентироваться в них **Уметь**: характеризовать культурно-исторические явления и памятники; формулировать гипотезы о причинах и особенностях развития исторических процессов; систематизировать факты, явления, объекты, изученные в курсе; систематизировать факты, явления, объекты, изученные в курсе; выделять периоды в истории развития региональных и общеисторических процессов; условия формирования личности, ее свободы, ответственности за сохранение жизни, природы, культуры, понимать роль насилия и ненасилия в истории и человеческом поведении нравственных обязанностей человека по отношению к другим и самому себе. рассмотреть представления о сущности сознания, его взаимоотношении с бессознательным, роли сознания и самосознания в поведении, общении и деятельности людей, формировании личности. **Владеть**: навыками критического мышления	1. Актуальность тематики работы и её соответствие профилю ОП 2. Степень полноты обзора состояния вопроса и корректность постановки задачи. 3. Уровень и корректность использования в работе методов исследований, математического моделирования, расчетов. 3. Степень комплексности работы, применение в ней знаний общепрофессиональных и специальных дисциплин. 5. Ясность, четкость, последовательность и обоснованность изложения. 6. Применение современного математического и программного обеспечения, компьютерных технологий в работе. 7. Качество оформления (общий уровень грамотности, стиль изложения, качество	Глубокое раскрытие темы, качественное оформление работы, обоснованность сделанных выводов и их аргументированность, оригинальность и новизна полученных результатов.

ОК-2 Способностью использовать основы экономических знаний в различных сферах деятельности	**Знать**: содержание основных экономических проблем, происходящих современном обществе и подходы к их решению **Уметь**: принимать самостоятельные эффективные решения на основе анализа и оценки конкретной экономической ситуации **Владеть**: навыками создания простейших эконометрических моделей	иллюстраций, соответствие требованиям стандартов). 8. Объем и качество выполнения графического материала, его соответствие тексту. 9. Обоснованность и доказательность выводов работы. 10. Оригинальность и новизна полученных результатов, научно-исследовательских, технических или методических решений.	
ОК-3 Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера		
ОК-4 Способностью использовать основы правовых знаний в различных сферах деятельности	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей		

	России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера		
ОК-5 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	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования		
ОК-6 Способностью	**Знать**: определения базовых понятий и категорий теории		

работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	коммуникации; формы, уровни и виды коммуникации; структуру коммуникационного процесса; специфику массовой коммуникации; основные положения теорий взаимодействия иаудитории; **Уметь**: дифференцировать, характеризовать и оценивать формы, уровни и виды коммуникации; выстраивать (моделировать) коммуникацию по заданным моделям и видам; отличать массовую коммуникацию от других видов коммуникации по основным параметрам – адресант, адресат, сообщение, каналы, код, эффект; дифференцировать, характеризовать и оценивать отдельные компоненты, составляющие структуру коммуникационного процесса; дифференцировать, характеризовать и оценивать основные положения теорий взаимодействия СМК и аудитории; использовать и при необходимости трансформировать теоретические модели в соответствии с конкретной (реальной) коммуникативной ситуацией; оценивать особенности аудитории, удерживать и активировать ее внимание; **Владеть**: навыками деловой коммуникации; способностью к обобщению, анализу, восприятию информации; базовыми навыками, составляющими коммуникативную компетентность личности, включая навык оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и вотношении собственной личности		
ОК-7	**Знать**:		

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	базовую лексику общего языка, лексику представляющую нейтральный научный стиль, а также основную техническую терминологию; наиболее употребительную (базовую) грамматику и основные грамматические явления, характерные для регистра научной речи лексику и фразеологию, отражающую основные направления технической науки в области радиофизики; основные элементы понимания делового письма; основные приемы аннотирования, реферирования и перевода научно-технической литературы **Уметь**: понимать устную (монологическую и диалогическую) речь на бытовые и специальные темы воспринимать на слух и участвовать в обсуждении тем, связанных со специальностью; читать и понимать со словарем научную литературу по общим и специальным вопросам **Владеть**: навыками разговорно-бытовой речи (владеть нормативным произношением и ритмом речи и применять их для беседы на бытовые и специальные темы) навыками чтения научной литературы с целью извлечения информации; основными навыками (неофициального и делового) письма; основными навыками публичной речи – делать научные сообщения, доклады (с предварительной подготовкой)		
ОК-8 Способностью к самоорганизации и самообразованию	**Знать**: научно-психологические основы выбора, процессуально-структурные компоненты психологического феномена «выбор», основныенаправления современной этики, базовые элементы и приемы, применяемые в подготовленной публичной речи **Уметь**:		

	составлять перспективный план жизни, сучетом возможных препятствий, решать конфликтные ситуации, опираясь на знания о стратегиях поведения, аргументированно излагать свои моральные убеждения и составлять хорошее самостоятельное публичное выступление **Владеть**: приемами самооценки, эффективного общения и слушания, позитивного общения, конгруэнтного поведения, анализа собственныхнравственных ценностей и поступков, подготовки, корректировки выступления		
ОК-9 Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	**Знать**: влияние физической культуры на укрепления здоровья, профилактику профессиональных заболеваний и вредных привычек; основные средства и методы физического воспитания; основы здорового образа жизни; методы оценки физического развития, физической подготовленности средствами физической культуры и спорта в студенческом возрасте **Уметь**: использовать средства и методы физической культуры в регулировании своего психофизического состояния; выполнять комплексы упражнений оздоровительной и профессионально прикладной направленности; **Владеть**: навыком самостоятельно применять средства и методы физического воспитания в укреплении здоровья, методами контроля состояния организма при нагрузках; навыками ведения здорового образа жизни, участия в физкультурно-оздоровительной деятельности.		
ОПК-1 Способностью анализировать	**Знать**: основные физические величины и понятия механики; основные физические законы, описывающие динамику		

физические явления и процессы для решения профессиональных задач	материальной точки и систем материальных точек основные физические зако ны, описывающие динамику твердого тела основные физическиепредставления механики колебаний и волн; основные физическиепредставления гидрогазодинамики; основные понятия, законы и модели молекулярной физики основные законы классической электродинамики; основные методы электрическихизмерений фундаментальную базу теоретических знаний по оптике, основные понятия, законы и модели атомной и ядерной физики, методы математического анализа объектов и явлений микромира на основе уравнений квантовой механики; возможные сферы приложения законов и моделей атомной и ядерной физики; негативные факторы техносферы, их воздействие на человека **Уметь**: правильно соотносить содержание конкретных задач с законами физики, эффективно применять общие законы физики для решения конкретных задач в области физики и на междисциплинарных границах физики с другими областями знаний; пользоваться физическими приборами, ставить и решать простейшие экспериментальные задачи, обрабатывать, анализировать иоценивать полученные результаты; строить математические модели простейших физических явлений и использовать для изучения этих моделей доступныйему математический аппарат, включая методы вычислительноймате матики; использовать при работе справочную и учебную литературу, находить другие необходимые источники информации и работать с ними; понимать, излагать и критически анализировать базовую общефизическую информацию		

	применять основные законы и методы электродинамики для решения прикладных задач применять основные законы и методы оптики для решения прикладных задач; студенты должны овладеть приемами и методами решения практических задач оптики, требующих использования разнообразных математических методов **владеть**: навыками использования основных законов механики и молекулярной физики для анализа различных механических и физических систем; навыками оценки на основе физических законов характера механических и физических процессов для различных систем и сред; навыками использованияматематического аппарата для решения физических задач навыками и методиками проведения электрических и магнитных измерений, конструирования контрольно-измерительныхустройств и экспериментальных установок использования технических средств для определения основных параметров техно-логического процесса, изучения свойств физико-технических объектов, изделий и материалов методами обработки данных измерений физических величин, навыками работы с современным экспериментальным оборудованием, методами защиты человека от опасных и вредных факторов; способностью к правильному использованию общенаучной и специальной терминологии в профессиональной области; математическими методами и моделями для описания физических явлений, физического эксперимента, включая методы оценки точности экспериментальных измерений		
ОПК-2 Способностью применять	**знать**: основные положения теории пределовфункций, основные теоремы дифференциального и интегрального исчисления		

соответствующий математический аппарат для решения профессиональных задач	функций одного и нескольких переменных; основы векторного анализа основы аппарата теории обыкновенных дифференциальных уравнений, необходимых для решения теоретических и практических задач **уметь**: ориентироваться в постановках задач; строго доказывать математическое утверждение; определять возможности применения методов математического анализа; пользоваться библиотеками прикладных программ и пакетами программ для решения приклад ных математическихзадач использовать математические методы при решении прикладных задач, приводящих к обыкновенным дифференциальным уравнениям **владеть**: практическими навыками решения основных задач теории пределов функций, дифференцирования, интегрирования навыками решения типовых задач с применением изучаемого теоретического материала; навыками математического исследования динамических проблем из различных областей физики		
ОПК-3 Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	**Знать**: - принципы работы изучаемых электронных устройств и понимать физические процессы, происходящих в них; основные законы и методы расчета электрических цепей; - назначение, принцип работы, основные характеристики и обозначение полупроводниковых элементов, операционных усилителей, интегральных сборок и устройств на их основе; - принципы построения различных вариантов схем электронных устройств с отрицательной и/или положительной обратными связями (ОС), понимать		

	причиныВлияния ОС на основные показатели и стабильность параметров изучаемых устройств; понимать причины возникновения неустойчивой работы усилителей с отрицательной ОС; - способы оценки устойчивости электронных устройствс внешними цепями ОС; - принципы и алгоритмы работы устройств формирования и генерирования сигналов; - принципы и алгоритмы работы радиоприемных - - устройств и устройств обработки сигналов; принципиальные схемы и элементную базу устройств, осуществляющих модуляцию и детектирование сигналов. **Уметь**: - объяснять физическое назначение элементов и влияние их параметров на электрические параметры и частотные свойства базовых каскадов аналоговых схем; - применять на практике методы исследования аналоговых электронных устройств, основанных на аналитических и графо-аналитических процедурах анализа; - выполнять расчеты, связанные с выбором режимов работы и определением параметров изучаемых электронных устройств; - формировать цепи ОС с целью улучшения качественных показателей и получения требуемых форм характеристик аналоговых электронных устройств; - проводить компьютерное моделирование и проектирование аналоговых и инфокоммуникационных электронных устройств, а также иметь представление о методах компьютерной оптимизации таких устройств; - пользоваться справочными материалами («Datasheet») на аналоговые и цифровые элементы и ИС при проектировании телекоммуникационных устройств; - определять причины неисправностей		

	инфокоммуникационных устройств и выбраковывать неисправные элементы; составлять, подготавливать и заполнять техническую документацию, требуемую в порядке эксплуатации инфокоммуникационного оборудования **Владеть**: - навыками чтения и изображения электронных схем на основе современной элементной базы; - навыками составления эквивалентных схем на базе принципиальных электрических схем изучаемых устройств; - навыками проектирования и расчета простейших аналоговых и цифровых схем; - навыками работы с контрольно-измерительной аппаратурой; - навыками компьютерного моделирования и проектирования аналоговых и цифровых телекоммуникационных устройств; навыками поиска и устранения простых неисправностей		
ОПК-4 Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования		
ОПК-5 Способностью	**Знать**: структуру системы управления информационной		

использовать нормативные правовые акты в профессиональной деятельности	безопасность; приемы управлению информационной безопасностью методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз **Уметь**: выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте. **Владеть**: правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления		
ОПК-6 Способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных	**Знать**: правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности» поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу радиоактивных веществ (РВ) и ХОВ, современных средств поражения анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов методы прогнозирования и оценки ЧС		

ситуаций, организовать мероприятия по охране труда и технике безопасности	сигналы оповещения ГО и порядок действийнаселения по сигналам порядок и содержание работ руководителей предприятий, учреждений, организаций, независимо от их организационно-правовой формы, а также их подразделений по управлению действиями подчиненных в ЧС в соответствии с получаемой специальностью средства и методы повышения безопасности, экологичности и устойчивости технических средств и технологических процессов **Уметь**: проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям эффективно применять средства защиты от негативных воздействий разрабатывать мероприятия по повышению безопасности и экологичности производственнойдеятельности планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных идругих неотложных работ при ликвидации последствий чрезвычайных ситуаций составлять планы мероприятий по повышению собственной адаптивности анализировать, выявлять и конструировать собственные адаптивные стратегии четко действовать по сигналам оповещения, практически выполнять основные мероприятиязащиты от опасностей, возникающих при ведении военных действий или вследствие этих действий, атак же от ЧС природного и техногенного характера **Владеть**: методами прогнозирования чрезвычайных ситуаций и		

	предотвращения их негативных последствий методами повышения безопасности, экологичности устойчивости технических средств и технологических процессов некоторыми методами повышения стрессоустойчивости. способами управления эмоциями в экстремальных ситуациях		
ОПК-7 Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**Знать**: основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования особенности различных подходов к организации информационного обеспечения особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне **Уметь**: вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования;		

	выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач проектировать, оценивать и реализовывать информационное обеспечение информационных систем осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне **Владеть**: основными методами кодирования и декодирования информации для различных задач средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне		
ПК-1 Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать**: способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; **Уметь**: классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути		

	их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения **Владеть**: навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		
ПК-2 Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать**: основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; **Уметь**: определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий **Владеть**:		

	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей		
ПК-3 Способностью администрировать подсистемы информационной безопасности объекта защиты	**Знать**: задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Уметь**: применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Владеть**: средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков		
ПК-4 Способностью	**Знать**: этапы и модели жизненного цикла информационных		

участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	систем; корпоративные стандарты и методики; принципы хранения, защиты, передачи и получения информации в корпоративных сетях **Уметь**: разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных **Владеть**: навыками защиты информации в корпоративных сетях связи		
ПК-5 Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**Знать**: правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности **Уметь**: применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем **Владеть**:		

	навыками работы с нормативными правовыми актами; навыкамиработы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках		
ПК-6 Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита		

	информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации		
ПК-7 Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования		
ПК-8 Способностью оформлять рабочую техническую документацию с учетом действующих	**Знать**: терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере **Уметь**:		

нормативных и методических документов	пользоваться современной научно-технической информацией по исследуемымпроблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации **Владеть**: навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках		
ПК-9 Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	**Знать**: направления создания правовой базы в области информационной безопасности; области применениянолученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну **Уметь**: разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **Владеть**: навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации		
ПК-10 Способностью	**Знать**: основные нормативные правовые акты в области		

проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности **Уметь**: определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач **Владеть**: способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации		

ПК-11 Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать**: физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; **Уметь**: использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач **Владеть**:		

	навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну		
ПК-12 Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать**: основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации **Уметь**:		

	разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации **Владеть**: методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации		
ПК-13 Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	**Знать**: типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного		

обеспечению информационной безопасности, управлять процессом их реализации	копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; **Уметь**: определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования		
ПК-14 Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать**: назначение, виды и принципы построения организации и управления службы защиты информации **Уметь:** применять современные компьютерные технологии для решения профессиональных задач; ориентироваться в сети научных и образовательных порталов сети Интернет; обрабатывать результаты полученных измерений с помощью математических программных продуктов **Владеть**: навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации		

ПК-15 Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать**: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии **Уметь**: осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации **Владеть**: навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки		

	источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации		
ПКУ-1 Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	**Знать**: теоретические основы построения клиент-серверных веб-приложений, общие методы программирования механизмы реализации сетевых угроз по протоколам передачи данных HTTP, FTP, а также известные уязвимости веб-серверов **Уметь**: использовать полученные теоретические знания для решения конкретных прикладных задач, программировать клиент-серверные приложения с применением СУБД для обработки данных, находить и исправлять ошибки в программном коде конфигурировать клиент-серверное программное обеспечение с учетом требуемых параметров сетевой безопасности, анализировать возможные каналы утечки информации **Владеть**: практическими навыками конфигурирования и администрирования веб-серверов, а также навыками настройки систем управления контентом практическими навыками, по оценке защищенности веб-приложений		

4.1. Примерная тематика выпускных квалификационных работ по направлению подготовки 10.01.01 «Информационная безопасность» (профиль подготовки «Организация и технология защиты информации»).

1. Построение виртуальной защищённой сети с учетом требований безопасного хранения ключевой информации в организации
2. Разработка комплекса процедур аудита информационной безопасности Scada систем
3. Разработка методики управления инцидентами и событиями информационной безопасности
4. Модель защиты веб ресурсов на основе CMS
5. Модернизация системы защиты информации на предприятии
6. Автоматическая атака Wi-Fi «Twincy»
7. Исследование ПЭМИН от видеосредств при обработке конфиденциальной информации программно-аппаратным комплексом "Навигатор-П5М"
8. Разработка подсистемы фильтрации электронных почтовых сообщений от спама и вредоносного содержимого с использованием машинного обучения
9. Защита информации при использовании электронной почты
10. Разработка системы защиты информации для систем видеонаблюдения
11. Организация системы контроля и управления доступом с применением биометрических персональных данных
12. Разработка системы защиты обмена электронными почтовыми отправлениями
13. Разработка системы информационной безопасности для лаборатории защиты информации
14. Разработка системы обеспечения информационной безопасности корпоративной сети
15. Разработка системы обеспечения информационной безопасности на примере предприятия
16. Исследование распространения виброакустических колебаний в

инженерных коммуникациях АПК «Смарт»

17. Разработка системы обеспечения информационной безопасности удалённого доступа к внутренним информационным ресурсам для коммерческой организации

18. Разработка средства обнаружения сетевой разведки

19. Совершенствование системы защиты информации в ООО «МечелБизнессервис»

20. Разработка спам-фильтра для сервера корпоративных сетей

21. Разработка проекта системы защиты оконных проемов и решеток специальных помещений

22. Инструментальный аудит удаленного автоматизированного рабочего места

23. Разработка системы защиты конфиденциальной информации от несанкционированного разглашения

24. Разработка системы защищенного документооборота в организации с обработкой персональных данных в автоматизированных системах

25. Организация защиты персональных данных в организации

26. Разработка проекта комплексной защиты информации (обеспечения ИБ) хлебзавод ООО"TURON-NON"

27. Методы защиты автоматизированной системы учета оплаты проезда в муниципальной системе пассажирских перевозок города Калининграда

28. Разработка механизмов защиты диспетчерских компонентов сетей АСУ ТП

29. Разработка проекта системы защиты периметра корпоративный сети коммерческой организации

30. Разработка проекта системы защиты от утечки конфиденциальной информации регионального органа исполнительной власти

31. Разработка программного обеспечения для выявления снифинга в локальных вычислительных сетях

32. Разработка методики измерения экранирующих свойств альтернативных

измерительных площадок программно-аппаратным комплексом «Навигатор 5»

33. Разработка систем обеспечения информационной безопасности промышленного предприятия.

34. Проектирование системы центра реагирования на инциденты информационной безопасности на примере образовательного учреждения

35. Разработка проекта защиты конфиденциальной информации помещения ситуационного центра правительства Калининградской области

36. Разработка программного обеспечения для повышения уровня защищенности конфиденциальной информации

37. Оценка уровня информационной безопасности предприятия и пути совершенствования комплексной системы защиты от информационных угроз

38. Модернизация аппаратного комплекса ситуационного центра правительства Калининградской области

39. Разработка механизмов защиты сетей компьютерных классов общеобразовательной школы

40. Разработка методики измерения затухания альтернативных измерительных площадок программно-аппаратным комплексом «Навигатор 5»

4.2. Примеры формулировки тем и содержания выпускных квалификационных работ

Тема: Разработка механизма защиты диспетчерских компонентов сетей АСУ ТП

Введение

Глава 1. Теоретическая часть.

1.1 Особенности построения и функционирования распределенной многоуровневой АСУ ТП

1.2 Структура многоуровневой АСУ ТП на базе MasterSCADA

1.3 SCADA-система и особенности ее защиты

Глава 2 Повышение защищенности подсистем диспетчерского уровня АСУ ТП.

2.1 Определение архитектуры разрабатываемых механизмов выявления и

блокирования программ.

2.2 Разработка алгоритмов выявления и блокирования вредоносных программ.

2.3 Определение особенностей эксплуатации разработанных механизмов.

Глава 3. Определение эффективности разработанных механизмов защиты.

Заключение.

Список использованных источников

1. ГОСТ Р МЭК 61131-3-2016 Национальный стандарт Российской Федерации. Контроллеры программируемые. Часть 3. Языки программирования" (утв. и введен в действие Приказом Росстандарта от 13.05.2016 N 313-ст) из информационного банка "Отраслевые технические нормы" «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru
2. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 09.08.2018) "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (Зарегистрировано в Минюсте России 30.06.2014 N 32919)
3. Байрс Э. IT-безопасность в промышленности. Глубокий анализ пакетов данных для SCADA-систем // Современные технологии автоматизации. - 2013.-№4. – с.12-16.
4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] – URL:http://window.edu.ru/
5. Антивирусная утилита [Электронный ресурс] – URL:http://z-oleg.com/
6. Втюрин В.А. Автоматизированные системы управления технологическими процессами. Основы АСУ ТП: учебное пособие для студентов высшего учебного заведений // -СПб.: Санкт-Петербургская Государственная Лесотехническая Академия имени С.М. Кирова, 2006. -152
7. «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru

8. Зайцев О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. – СПб.: БХВ-Петербург, 2006. – 304 с.
9. Котенко И. В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. – 2004. – № 1. – с. 56–72.
10. MasterSCADA-система для АСУ ТП [Электронный ресурс] – URL:https://masterscada.insat.ru/
11. Определение эффективности [Электронный ресурс] – URL:https://dsec.ru/
12. Подтопельный В. В. Особенности информационной защиты систем управления на промышленных объектах // III БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2015 г., с. 74-78.
13. Подтопельный В. В. Уязвимости системы информационного сопровождения судов // II БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2014 г., с. 70-74.
14. Фаулер, М. UML. Основы. Учебное пособие [Текст] / М. Фаулер. – Символ-Плюс, 2007. – 192 с.: ил. – 2000 экз. – ISBN: 5-93286-060-5
15. Щербаков А. Сеть CAN: популярные прикладные протоколы // ChipNews,1999, №5.

ПРИЛОЖЕНИЯ

Приложение 1

Титульный лист ВКР

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. И. КАНТА»
Институт физико-математических наук и информационных технологий

Рекомендована к защите:
методический руководитель
направления подготовки
к.т.н., доцент ИФМНиИТ

_____ И.А. Ветров

"____"_____ 20__ г.

Допущена к защите:
первый заместитель директора
ИФМНиИТ
к. ф.-м. н., доцент

_____А.А. Шпилевой

"____"_____ 20__ г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: «XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль подготовки:
«**Организация и технологии защиты информации**»
Квалификация (степень**)**: **бакалавр**

ВКР защищена на оценку:

_____

Выполнил: студент 4 курса

_____ Иванов И.И.

Руководитель: xxxxxxxxxxx ИФМНиИТ

_____ Петров П. П.

Калининград, 20__

Приложение 2

Оценочный лист сформированности компетенций для руководителя ВКР и членов ГЭК

Коды проверяемых компетенций	Текст ВКР	Этап подготовки к процедуре защиты ВКР
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	+	+
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	+	+
ПКУ-1	+	+

Приложение 3

Оценочный лист членов ГЭК

Оценка уровня сформированности компетенций студента _____ направления подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации защиты информации» в процессе защиты выпускной квалификационной работы, выполненной на тему

_____

_____

Коды проверяемых компетенций	**Показатели оценки результата**	**Показатели уровня сформированности компетенций**			
		2 – низкий	**3 – средний**	**4 – достаточный**	**5 – высокий**
ОК-1	Способностью использовать основы философских знаний для формирования мировоззренческой позиции				
ОК-2	Способностью использовать основы экономических знаний в различных сферах деятельности				
ОК-3	Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма				
ОК-4	Способностью использовать основы правовых знаний в различных сферах деятельности				
ОК-5	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-6	Способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия				
ОК-7	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-8	Способностью к самоорганизации и самообразованию				
ОК-9	Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности				
ОПК-1	Способностью анализировать физические явления и процессы для решения профессиональных задач				
ОПК-2	Способностью применять соответствующий математический аппарат для решения профессиональных задач				
ОПК-3	Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач				
ОПК-4	Способностью понимать значение информации в				

	развитии современного общества, применять информационные технологии для поиска и обработки информации				
ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности				
ОПК-6	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-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
ПК-3	Способностью администрировать				

	подсистемы информационной безопасности объекта защиты				
ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов				
ПК-9	Способностью осуществлять подбор, изучение и обобщение				

	научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности				
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов				
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации				
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности				
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими				

	документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики				

Приложение 4

Форма отзыва руководителя

Отзыв
на выпускную квалификационную работу
студента(ки) 4-го курса Института физико-математических наук и информационных технологий
направления подготовки 10.03.01 «Информационная безопасность»
Ф.И.О. студента
«……Тема ВКР…….»

- Формулировка проблемы.
- Актуальность проблемы.
- Состояние решения проблемы на данный момент.
- Конкретная задача, решению которой посвящена данная ВКР, её актуальность.
- Что реально сделано по главам ВКР.
- Достоинства работы: оригинальность, новизна и научная значимость результатов; научный уровень и глубина работы; доказательность и достоверность результатов; широта охвата материала и качество обзора литературы по теме, обоснованность выводов; наличие компьютерной реализации; степень практической реализации.
- Отношение студента к работе: добросовестность, дисциплинированность, систематичность, самостоятельность, активность, глубина и эрудированность, творческий подход.
- Недостатки работы:
  - отступления от утверждённого плана работы _____
  - недостатки содержания _____
  - недостатки оформления _____
- В какой степени студент справился с решением поставленной задачи – оценка соответствия ВКР требованиям, предъявляемым к выпускным квалификационным работам студентов института физико-математических наук и информационных технологий направления подготовки 10.03.01 «Информационная безопасность».
- Предлагаемая оценка.

Научный руководитель,
должность, уч. степень, уч. звание. _____/Ф.И.О.

Приложение 5

Форма рецензии

РЕЦЕНЗИЯ
на выпускную квалификационную работу
студента(ки) 6 курса Института физико-математических наук и информационных технологий
направления подготовки 10.03.01 «Информационная безопасность»
Ф.И.О. студента
«……Тема ВКР……..»

- Формулировка проблемы.
- Актуальность проблемы.
- Состояние решения проблемы на данный момент.
- Конкретная задача, решению которой посвящена данная ВКР, её актуальность.
- Критический анализ общего замысла, основных положений и результатов работы по главам ВКР.
- Достоинства работы: оригинальность, новизна и научная значимость результатов; научный уровень и глубина работы; доказательность и достоверность результатов; широта охвата материала и качество обзора литературы по теме, обоснованность выводов; наличие компьютерной реализации; степень практической реализации.
- Недостатки работы:
  - недостатки содержания: _____
  - недостатки оформления: _____
- Оценка соответствия ВКР требованиям, предъявляемым к выпускным квалификационным работам студентов института физико-математических наук и информационных технологий направления подготовки 10.03.01 «Информационная безопасность».
- Предлагаемая оценка.

Должность, уч. звание, уч. степень
Рецензента _____/Ф.И.О.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ ИММАНУИЛА КАНТА

Институт физико-математических наук и информационных технологий

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ В.И.Бурмистров
«20» марта 2020 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«20» марта 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Процедура защиты выпускной квалификационной работы»

для студентов 4 курса
очной формы обучения

направления подготовки 10.03.01.
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

Калининград, 2020 г.

Лист согласования

Составители: доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно–методического совета института физико-математических наук и информационных технологий.

Протокол № __/__ от «__» _____ 20__ г.

Председатель учебно-методического совета _____первый заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) _____

Протокол №____ от «___ »_____20_ г.

Ведущий менеджер ООП _____Бурмистров В. И.

СОДЕРЖАНИЕ
ПРОГРАММЫ ПРОЦЕДУРЫ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по направлению подготовки 10.03.01 «Информационная безопасность», уровень высшего образования - бакалавриат…….……...4
1.1. Общие положения……..…..4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы……5
1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся……...11
2. Процедура защиты выпускной квалификационной работы в Государственной экзаменационной комиссии …..……..12
2.1. Порядок защиты выпускной квалификационной работы на заседании ГЭК ……12
2.2. Описание показателей и критериев оценивания компетенций…….14
2.2. Шкала оценивания степени сформированности компетенций……..…15
3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины…….....….17
4. Фонд оценочных средств для проведения ГИА ……..….20
4.1. Примерная тематика выпускных квалификационных работ по направлению подготовки 10.03.01 «Информационная безопасность»……28
4.2. Примеры формулировки тем и содержания выпускных квалификационных работ……..30
Приложения……...……33

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по направлению подготовки 10.03.01 «Информационная безопасность», уровень высшего образования – бакалавриат

1.1. Общие положения

Программа ГИА является частью основной профессиональной образовательной программы в соответствии с ФГОС ВО в части государственных требований к минимуму содержания и уровню подготовки выпускников по направлению подготовки 10.03.01 «Информационная безопасность».

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по основной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные утвержденным учебным планом направления подготовки 10.03.01 «Информационная безопасность».

Видом ГИА в соответствии с п. 2.7 ФГОС ВО и учебным планом является защита выпускной квалификационной работы.

Аттестацию проводит Государственная Экзаменационная Комиссия (ГЭК). Председатель ГЭК и состав ГЭК утверждаются в установленном порядке.

Выпускная квалификационная работа выполняется в обязательном порядке, в установленные сроки, проходит рецензирование (в необязательном порядке) и защищается в ГЭК.

Государственная итоговая аттестация (ГИА) включает в себя два основных этапа - этап подготовки к процедуре защиты выпускной квалификационной работы (Б3.01(Д)) и процедуру защиты выпускной квалификационной работы Б3.02(Д).

Наименование дисциплины (модуля) - «Процедура защиты выпускной квалификационной работы».

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины «Процедура защиты выпускной квалификационной работы» является защита выпускной квалификационной работы.

В ходе защиты выпускной квалификационной работы, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, профессионально презентовать результаты своей работы, научно аргументировать и защищать свою точку зрения в ходе презентации.

Выпускник направления подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Организация и технология защиты информации» в соответствии с целями основной образовательной программы и типами задач профессиональной деятельности в результате освоения данной дисциплины должен обладать компетенциями, представленными в таблице

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
ОК-1	Способностью использовать основы философских знаний для формирования мировоззренческой позиции	**Знать**: современные представления о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека, о многообразии форм человеческого знания, соотношении истины и заблуждения, знания и веры, рационального и иррационального в человеческой жизнедеятельности, особенностях функционирования знания в современном обществе, духовных ценностях, их значении в творчестве и повседневной жизни, научиться ориентироваться в них **Уметь**: характеризовать культурно-исторические явления и памятники; формулировать гипотезы о причинах и особенностях развития исторических процессов; систематизировать факты, явления, объекты,

		изученные в курсе; систематизировать факты, явления, объекты, изученные в курсе; выделять периоды в истории развития региональных и общеисторических процессов; условия формирования личности, ее свободы, ответственности за сохранение жизни, природы, культуры, понимать роль насилия и ненасилия в истории и человеческом поведении нравственных обязанностей человека по отношению к другим и самому себе. рассмотреть представления о сущности сознания, его взаимоотношении с бессознательным, роли сознания и самосознания в поведении, общении и деятельности людей, формировании личности. **Владеть**: навыками критического мышления
ОК-2	Способностью использовать основы экономических знаний в различных сферах деятельности	**Знать**: содержание основных экономических проблем, происходящих современном обществе и подходы к их решению **Уметь**: принимать самостоятельные эффективные решения на основе анализа и оценки конкретной экономической ситуации **Владеть**: навыками создания простейших эконометрических моделей
ОК-3	Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально

		профессионального характера
ОК-4	Способностью использовать основы правовых знаний в различных сферах деятельности	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера
ОК-5	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	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования
ОК-6	Способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать**: определения базовых понятий и категорий теориикоммуникации; формы, уровни и виды коммуникации; структуру коммуникационного процесса; специфику массовой коммуникации; основные положения теорий взаимодействия иаудитории; **Уметь**: дифференцировать, характеризовать и оцениватьформы, уровни и виды коммуникации; выстраивать (моделировать) коммуникацию позаданным моделям

		и видам; отличать массовую коммуникацию от других видовкоммуникации по основным параметрам – адресант, адресат, сообщение, каналы, код, эффект; дифференцировать, характеризовать и оцениватьотдельные компоненты, составляющие структуру коммуникационного процесса; дифференцировать, характеризовать и оценивать основные положения теорий взаимодействия СМК иаудитории; использовать и при необходимости трансформироватьтеоретические модели в соответствии с конкретной (реальной) коммуникативной ситуацией; оценивать особенности аудитории, удерживать иактивировать ее внимание; **Владеть**: навыками деловой коммуникации; способностью к обобщению, анализу, восприятиюинформации; базовыми навыками, составляющими коммуникативную компетентность личности, включаянавык оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и вотношении собственной личности
ОК-7	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	**Знать**: базовую лексику общего языка, лексику представляющую нейтральный научный стиль, а также основную техническую терминологию; наиболее употребительную (базовую) грамматику и основные грамматические явления, характерные для регистра научной речи лексику и фразеологию, отражающую основные направления технической науки в области радиофизики; основные элементы понимания делового письма; основные приемы аннотирования, реферирования и перевода научно-технической литературы **Уметь**: понимать устную (монологическую и диалогическую) речь на бытовые и специальные темы воспринимать на слух и участвовать в обсуждении тем, связанных со специальностью; читать и понимать со словарем научную литературу по общим и специальным вопросам **Владеть**:

		навыками разговорно-бытовой речи (владеть нормативным произношением и ритмом речи и применять их для беседы на бытовые и специальные темы) навыками чтения научной литературы с целью извлечения информации; основными навыками (неофициального и делового) письма; основными навыками публичной речи – делать научные сообщения, доклады (с предварительной подготовкой)
ОК-8	Способностью к самоорганизации и самообразованию	**Знать**: научно-психологические основы выбора, процессуально-структурные компоненты психологического феномена «выбор», основныенаправления современной этики, базовые элементы и приемы, применяемые в подготовленной публичной речи **Уметь**: составлять перспективный план жизни, с учетом возможных препятствий, решать конфликтные ситуации, опираясь на знания о стратегиях поведения, аргументированно излагать свои моральные убеждения и составлять хорошее самостоятельное публичное выступление **Владеть**: приемами самооценки, эффективного общения и слушания, позитивного общения, конгруэнтного поведения, анализа собственныхнравственных ценностей и поступков, подготовки, корректировки выступления
ОК-9	Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	**Знать**: влияние физической культуры на укрепления здоровья, профилактику профессиональных заболеваний и вредных привычек; основные средства и методы физического воспитания; основы здорового образа жизни; методы оценки физического развития, физической подготовленности средствами физической культуры и спорта в студенческом возрасте **Уметь**: использовать средства и методы физической культуры в регулировании своего психофизического состояния; выполнять комплексы упражнений оздоровительной и профессионально прикладной направленности; **Владеть**: навыком самостоятельно применять средства

		и методы физического воспитания в укреплении здоровья, методами контроля состояния организма при нагрузках; навыками ведения здорового образа жизни, участия в физкультурно-оздоровительной деятельности.
ОПК-1	Способностью анализировать физические явления и процессы для решения профессиональных задач	**Знать**: основные физические величины и понятия механики; основные физические законы, описывающие динамику материальной точки и систем материальных точек основные физические законы, описывающие динамику твердого тела основные физическиепредставления механики колебаний и волн; основные физическиепредставления гидрогазодинамики; основные понятия, законы и модели молекулярной физики основные законы классической электродинамики; основные методы электрическихизмерений фундаментальную базу теоретических знаний по оптике, основные понятия, законы и модели атомной и ядерной физики, методы математического анализа объектов и явлений микромира на основе уравнений квантовой механики; возможные сферы приложения законов имоделей атомной и ядерной физики; негативные факторы техносферы, их воздействие на человека **Уметь**: правильно соотносить содержание конкретных задач с законами физики, эффективно применять общие законы физики для решения конкретных задач в области физики и на междисциплинарных границах физики с другими областями знаний; пользоваться физическими приборами, ставить и решать простейшие экспериментальные задачи, обрабатывать, анализировать и оценивать полученные результаты; строить математическиемодели простейших физических явлений и использовать для изучения этих моделей доступный ему математический аппарат, включая методы вычислительнойматематики; использовать при работе справочную и учебную литературу, находить другие необходимые источники информации и

		работать с ними; понимать, излагать и критически анализировать базовую общефизическую информацию применять основные законы и методы электродинамики для решения прикладных задач применять основные законы и методы оптики для решения прикладных задач; студенты должны овладеть приемами и методами решения практических задач оптики, требующих использования разнообразных математических методов **владеть**: навыками использования основных законов механики и молекулярной физики для анализа различных механических и физических систем; навыками оценки на основе физических законов характера механических и физических процессов для различных систем и сред; навыками использованиематематического аппарата для решения физических задач навыками и методиками проведения электрических и магнитных измерений, конструирования контрольно-измерительных устройств и экспериментальных установок использования технических средств для определения основных параметров техно-логического процесса, изучения свойств физико-технических объектов, изделий и материалов методами обработки данных измерений физических величин, навыками работы с современным экспериментальным оборудованием, методами защиты человека от опасных и вредных факторов; способностью к правильному использованию общенаучной и специальной терминологии в профессиональной области; математическими методами и моделямидля описания физических явлений, физического эксперимента, включая методы оценки точности экспериментальных измерений
ОПК-2	Способностью применять соответствующий математический аппарат для решения профессиональных задач	**знать**: основные положения теории пределов функций, основныетеоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; основы векторного анализа основы аппарата теории обыкновенных

		дифференциальных уравнений, необходимых для решения теоретических и практических задач **уметь**: ориентироваться в постановках задач; строго доказывать математическое утверждение; определятьвозможности применения методов математического анализа; пользоваться библиотеками прикладных программ и пакетами программ для решения прикладных математическихзадач использовать математические методы при решении прикладных задач, приводящих к обыкновенным дифференциальным уравнениям **владеть**: практическими навыками решения основных задач теории пределов функций, дифференцирования, интегрирования навыками решения типовых задач с применением изучаемого теоретического материала; навыками математического исследования динамическихпроблем из различных областей физики
ОПК-3	Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	**Знать**: - принципы работы изучаемых электронных устройств ипонимать физические процессы, происходящих в них; основные законы и методы расчета электрических цепей; - назначение, принцип работы, основные характеристики и обозначение полупроводниковых элементов, операционных усилителей, интегральных сборок и устройств на их основе; - принципы построения различных вариантов схем электронных устройств с отрицательной и/или положительной обратными связями (ОС), понимать причинывлияния ОС на основные показатели и стабильность параметров изучаемых устройств; понимать причины возникновения неустойчивой работы усилителей с отрицательной ОС; - способы оценки устойчивости электронных устройствс внешними цепями ОС; - принципы и алгоритмы работы устройств формирования и генерирования сигналов; - принципы и алгоритмы работы радиоприемных - - устройств и устройств обработки сигналов; принципиальные схемы и элементную базу

		устройств, осуществляющих модуляцию и детектирование сигналов. **Уметь**: - объяснять физическое назначение элементов и влияниеих параметров на электрические параметры и частотные свойства базовых каскадов аналоговых схем; - применять на практике методы исследования аналоговых электронных устройств, основанных на аналитических и графо-аналитических процедурах анализа; - выполнять расчеты, связанные с выбором режимов работы и определением параметров изучаемых электронных устройств; - формировать цепи ОС с целью улучшения качественных показателей и получения требуемых форм характеристик аналоговых электронных устройств; - проводить компьютерное моделирование и проектирование аналоговых и инфокоммуникационных электронных устройств, а также иметь представление о методах компьютерной оптимизации таких устройств; - пользоваться справочными материалами («Datasheet») на аналоговые и цифровые элементы и ИС при проектировании телекоммуникационных устройств; - определять причины неисправностей инфокоммуникационных устройств и выбраковывать неисправные элементы; составлять, подготавливать и заполнять техническую документацию, требуемую в порядке эксплуатации инфокоммуникационного оборудования **Владеть**: - навыками чтения и изображения электронных схем на основе современной элементной базы; - навыками составления эквивалентных схем на базепринципиальных электрических схем изучаемых устройств; - навыками проектирования и расчета простейших аналоговых и цифровых схем; - навыками работы с контрольно-измерительной аппаратурой; - навыками компьютерного моделирования и проектирования аналоговых и цифровых телекоммуникационных устройств; навыками поиска и устранения простых неисправностей
ОПК-4	Способностью понимать	**Знать**:

	значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования
ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности	**Знать**: структуру системы управления информационной безопасность; приемы управлению информационной безопасностью методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз **Уметь**: выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте. **Владеть**: правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления
ОПК-6	Способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций,	**Знать**: правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности» поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу

	организовать мероприятия по охране труда и технике безопасности	радиоактивных веществ (РВ) и ХОВ, современных средств поражения анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов методы прогнозирования и оценки ЧС сигналы оповещения ГО и порядок действий населения по сигналам порядок и содержание работ руководителей предприятий, учреждений, организаций, независимо от их организационно-правовой формы, а также их подразделений по управлению действиями подчиненных в ЧС в соответствии с получаемой специальностью средства и методы повышения безопасности, экологичности и устойчивости технических средств и технологических процессов **Уметь**: проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям эффективно применять средства защиты от негативных воздействий разрабатывать мероприятия по повышению безопасности и экологичности производственнойдеятельности планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных и других неотложных работ при ликвидации последствий чрезвычайных ситуаций составлять планы мероприятий по повышению собственной адаптивности анализировать, выявлять и конструировать собственные адаптивные стратегии четко действовать по сигналам оповещения, практически выполнять основные мероприятия защиты от опасностей, возникающих при ведении военных действий или вследствие этих действий, атак же от ЧС природного и техногенного характера **Владеть**: методами прогнозирования чрезвычайных ситуаций и предотвращения их негативных последствий методами повышения безопасности, экологичностии устойчивости технических средств и технологических процессов

		некоторыми методами повышения стрессоустойчивости. способами управления эмоциями в экстремальных ситуациях
ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**Знать**: основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования особенности различных подходов к организации информационного обеспечения особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне **Уметь**: вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач проектировать, оценивать и реализовывать информационное обеспечение информационных систем осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне **Владеть**: основными методами кодирования и декодирования информации для различных задач средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом

		уровне
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать**: способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; **Уметь**: классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения **Владеть**: навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	**Знать**: основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;

	профессиональных задач	защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; **Уметь**: определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий **Владеть**: методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	**Знать**: задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Уметь**: применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Владеть**: средствами защиты информации в процессе хранения и передачи данных и методами их тестирования;

		методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знать**: этапы и модели жизненного цикла информационных систем; корпоративные стандарты и методики; принципы хранения, защиты, передачи и получения информации в корпоративных сетях **Уметь**: разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных **Владеть**: навыками защиты информации в корпоративных сетях связи
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**Знать**: правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности **Уметь**: применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицироватьзащищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем **Владеть**: навыками работы с нормативными правовыми актами; навыкамиработы с технической документацией на ЭВМ и вычислительных системах; навыками работы с технической документацией на

		компонентах информационных систем на русском и иностранном языках
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры;

	проведении технико-экономического обоснования соответствующих проектных решений	принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать**: терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере **Уметь**: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации **Владеть**: навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках
ПК-9	Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять	**Знать**: направления создания правовой базы в области информационной безопасности; области применениянолученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при

	обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	обработке информации,составляющей государственную тайну **Уметь**: разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **Владеть**: навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**Знать**: основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности **Уметь**: определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач **Владеть**: способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками

		освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать**: физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; **Уметь**: использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач

		Владеть: навыками организации охраны на объектах информатизации; навыками применения технических средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать**: основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации **Уметь**: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью

		информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации **Владеть**: методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**Знать**: типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; **Уметь**: определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и

		оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать**: назначение, виды и принципы построения организации и управления службы защиты информации **Уметь:** применять современные компьютерные технологии для решения профессиональных задач; ориентироваться в сети научных и образовательных порталов сети Интернет; обрабатывать результаты полученных измерений с помощью математических программных продуктов **Владеть**: навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать**: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии **Уметь**: осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и

		унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации **Владеть**: навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации

1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Процедура защиты выпускной квалификационной работы» составляет 3 зачетных единиц и 108 академических часов. Контактная работа обучающихся с преподавателем (по видам учебных занятий) 1 час, Самостоятельная работа обучающихся 107 академических часов

Место и время проведения государственной итоговой аттестации

Порядок и сроки проведения аттестационных испытаний устанавливаются в соответствии с графиком учебного процесса по направлению подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации» на основании положения об организации выполнения и защиты выпускной квалификационной работы обучающимися (студентами) от 15.05.2014 г., утвержденного Ученым советом БФУ (протокол № 10 от 12 мая 2014 г.).

2. Процедура защиты выпускной квалификационной работы в Государственной экзаменационной комиссии

Защита выпускной квалификационной работы проводится в установленное время на заседании экзаменационной комиссии по соответствующему направлению подготовки ГЭК БФУ им. И. Канта. Кроме членов комиссии на защите необходимо присутствие научного руководителя или рецензента, а также возможно присутствие других студентов, преподавателей и администрации БФУ им. И. Канта.

2.1. Порядок защиты выпускной квалификационной работы на заседании ГЭК

1. Защита начинается с доклада студента по теме выпускной квалификационной работы. На доклад по выпускной квалификационной работе отводится до 8 минут.

Доклад следует начинать с обоснования актуальности избранной темы, описания научной проблемы и формулировки цели работы (не более 2 мин), а затем в последовательности, установленной логикой проведенного исследования, по главам раскрывать основное содержание работы, обращая особое внимание на наиболее важные разделы и интересные результаты, критические сопоставления и оценки (около 5 мин). Заключительная часть доклада строится по тексту заключения выпускной квалификационной работы, перечисляются общие выводы из её текста без повторения частных обобщений, сделанных при характеристике глав основной части, собираются воедино основные рекомендации (примерно 1 мин). Студент должен излагать основное содержание своей выпускной квалификационной работы свободно, не читая письменного текста.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический материал (таблицы, схемы), иллюстрирующий основные положения работы. Все материалы, выносимые на наглядную графику, должны быть оформлены так, чтобы студент мог демонстрировать их без особых затруднений, и они были видны всем присутствующим в аудитории.

В среднем насыщенность одного плаката (слайда) информацией должна быть эквивалентна 10-15 строкам текста, не более. Плакаты (слайды) нумеруются в первом верхнем углу. Весь плакат (слайд) или его части должны иметь заголовок-название: Постановка задачи, Структурная схема системы и т.д. Обычно плакаты (слайды) соответствуют разделам или подразделам работы.

2. После завершения доклада члены ГЭК задают студенту вопросы, как непосредственно связанные с темой ВКР, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой.

3. После ответов студента на вопросы слово предоставляется научному руководителю. В конце своего выступления научный руководитель даёт свою оценку выпускной квалификационной работе.

4. При защите выпускной квалификационной работы после выступления научного руководителя слово предоставляется рецензенту. В случае отсутствия последнего на заседании ГЭК его отзыв зачитывает секретарь ГЭК. В конце своего выступления рецензент даёт свою оценку работе.

5. После выступления рецензента начинается обсуждение работы или дискуссия. В дискуссии могут принять участие как члены ГЭК, так и присутствующие заинтересованные лица.

6. После окончания дискуссии студенту предоставляется заключительное слово. В своём заключительном слове студент должен ответить на замечания рецензента, соглашаясь с ними или давая обоснованные возражения. Признаком хорошего тона являются слова благодарности в адрес членов ГЭК, научного руководителя и рецензента.

Решение ГЭК об итоговой оценке основывается на:

- оценке научного руководителя за работу, включая текущую работу в семестре;
- оценке рецензента за работу в целом;
- оценке членов ГЭК за содержание работы, её защиту, включая доклад, ответы на вопросы и замечания рецензента.

2.2. Описание показателей и критериев оценивания компетенций

Степень сформированности компетенций в результате защиты выпускной квалификационной работы осуществляется комиссией в ходе доклада по теме ВКР и ответах студента на вопросы в дискуссии.

1. В качестве критериев для оценки ВКР научные руководители и члены ГЭК должны иметь в виду:

- актуальность темы и задач работы;
- соответствие тематики направлению подготовки «Информационная безопасность»;
- обоснованность результатов и выводов;
- определенную оригинальность и новизну полученных данных;
- самостоятельность (личный вклад студента);
- возможности практического использования полученных результатов.

2. Обоснованность результатов и выводов определяются с позиций:

- соответствия известным научным положениям и фактам;
- логичности в изложении и обсуждении собственных данных;
- корректности постановки опыта, эксперимента;
- корректности использования математических методов.

При этом должны учитываться:

- уровень устного доклада на защите;
- соответствие оформления работы установленным требованиям;
- качество иллюстративного материала к докладу.

3. Оригинальность и новизна полученных данных определяется как:

- установление нового научного факта или подтверждение известного факта для новых условий;
- получение сведений, приводящих к формулировке проверяемых гипотез, которые требуют дальнейшей проверки;
- разработка оригинального метода решения известной задачи;
- применение известных методик для решения новых задач;

- введение в научный оборот новых данных;
- обоснованное решение поставленной задачи.

4. Личный вклад студента определяется: степенью самостоятельности в выборе темы, постановке задач, планировании и организации исследования, обработке и осмыслении полученных результатов.

5. Возможность практического использования данных, полученных в ВКР, определяется в отношении НИР, выполняемых в университете или в других организациях; задачами совершенствования учебного процесса; возможностью публикации в печати.

2.3. Шкала оценивания степени сформированности компетенций

Выпускная квалификационная работа оценивается по четырёхбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

Выпускная квалификационная работа оценивается членами ГЭК на основании доклада студента и выступления рецензента. Члены ГЭК оценивают уровень работы не только на основе перечисленных критериев (см. предшествующий раздел), а также обязательно принимают во внимание умение выпускника представить свою работу и правильно ответить на вопросы членов ГЭК.

Оценка **«ОТЛИЧНО»** ставится за реализацию всех необходимых компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (высокий уровень сформированных компетенций): выпускная квалификационная работа имеет исследовательский характер, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. При её защите студент показывает глубокие знания вопросов темы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«ХОРОШО»** ставится за частичную реализацию всех необходимых

компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (уровень освоения компетенций достаточный): выпускная квалификационная работа содержит элементы научного исследования, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. При её защите студент показывает знания вопросов темы, оперирует данными исследования, во время доклада использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«УДОВЛЕТВОРИТЕЛЬНО»** ставится в том случае, если студент демонстрирует частичную сформированность компетенций (средний уровень), предусмотренных ФГОС: выпускная квалификационная работа имеет технический характер, базируется на практическом материале, но анализ выполнен поверхностно, в ней просматривается непоследовательность изложения материала. Представлены необоснованные предложения. При её защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полных аргументированных ответов на заданные вопросы. В отзывах научного руководителя и рецензента имеются замечания по содержанию работы и методике анализа.

Оценка **«НЕУДОВЛЕТВОРИТЕЛЬНО»** выставляется, если демонстрируется несформированность (низкий уровень сформированности) соответствующих компетенций, предусмотренных ФГОС ВО: выпускная квалификационная работа не носит исследовательского характера, не отвечает требованиям, изложенным в методических рекомендациях. В работе нет выводов, либо они носят декларативный характер. При защите работы студент затрудняется отвечать на поставленные вопросы, при ответе допускает существенные ошибки. В отзывах научного руководителя и рецензента имеются серьезные критические замечания.

Итоговая оценка ГЭК выводится по принципу учета оценок большинства

членов ГЭК, а также руководителя. Оцениваемые компетенции и оценочный лист приведены в приложениях 1 и 2, соответственно.

Итоговая оценка за защиту ВКР складывается из оценок:

- демонстрационных материалов (презентации результатов работы);
- доклада на защите;
- ответов на вопросы членов комиссии.

Руководитель ВКР и члены ГЭК по итогам защиты ВКР оценивают уровень сформированности компетенций по:

- качеству демонстрационного материала,
- содержательности и логичности представленного доклада,
- ответам на заданные вопросы.

По результатам группового обсуждения всех присутствующих членов ГЭК председатель заполняет оценочный лист (приложение 2).

3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/13931.html

Дополнительная литература

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/

В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)

7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)

Перечень интернет-источников

1. «Национальная электронная библиотека» (http://xn--90ax2c.xn--p1ai/).
2. ЭБС Кантиана (https://elib.kantiana.ru/).
3. ЭБС IPR BOOKS (https://www.iprbookshop.ru/78574.html).
4. ЭБС Znanium (https://znanium.com/catalog/document?id=333215).

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта http://lms-3.kantiana.ru/.
2. Использование электронной образовательной среды БФУ им. И. Канта https://teams.microsoft.com/

4. Фонд оценочных средств для проведения ГИА

Компетенция	Перечень планируемых результатов	Диагностический инструмент	Критерии оценки
ОК-1 Способностью использовать основы философских знаний для формирования мировоззренческой позиции	**Знать**: современные представления о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека, о многообразии форм человеческого знания, соотношении истины и заблуждения, знания и веры, рационального и иррационального в человеческой жизнедеятельности, особенностях функционирования знания в современном обществе, духовных ценностях, их значении в творчестве и повседневной жизни, научиться ориентироваться в них **Уметь**: характеризовать культурно-исторические явления и памятники; формулировать гипотезы о причинах и особенностях развития исторических процессов; систематизировать факты, явления, объекты, изученные в курсе; систематизировать факты, явления, объекты, изученные в курсе; выделять периоды в истории развития региональных и общеисторических процессов; условия формирования личности, ее свободы, ответственности за сохранение жизни, природы, культуры, понимать роль насилия и ненасилия в истории и человеческом поведении нравственных обязанностей человека по отношению к другим и самому себе. рассмотреть представления о сущности сознания, его взаимоотношении с бессознательным, роли сознания и самосознания в поведении, общении и деятельности людей, формировании личности. **Владеть**: навыками критического мышления	1. Актуальность тематики работы и её соответствие профилю ОП 2. Степень полноты обзора состояния вопроса и корректность постановки задачи. 3. Уровень и корректность использования в работе методов исследований, математического моделирования, расчетов. 3. Степень комплексности работы, применение в ней знаний общепрофессиональных и специальных дисциплин. 5. Ясность, четкость, последовательность и обоснованность изложения. 6. Применение современного математического и программного обеспечения, компьютерных технологий в работе. 7. Качество оформления (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов).	Глубокое раскрытие темы, качественное оформление работы, обоснованность сделанных выводов и их аргументированность, оригинальность и новизна полученных результатов.
ОК-2	**Знать**:		

Способностью использовать основы экономических знаний в различных сферах деятельности	содержание основных экономических проблем, происходящих современном обществе и подходы к их решению **Уметь**: принимать самостоятельные эффективные решения на основе анализа и оценки конкретной экономической ситуации **Владеть**: навыками создания простейших эконометрических моделей	8. Объем и качество выполнения графического материала, его соответствие тексту. 9. Обоснованность и доказательность выводов работы. 10. Оригинальность и новизна полученных результатов, научно-исследовательских, технических или методических решений.	
ОК-3 Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России **Уметь**: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера		
ОК-4 Способностью использовать основы правовых знаний в различных сферах деятельности	**Знать**: основные события, явления и процессы отечественной и мировой истории; ключевые методологические, исторические и источниковедческие проблемы отечественной истории; важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России		

	Уметь: выработать собственную позицию в отношении изучаемых исторических проблем; формулировать предположения относительно причин, сущности и значения изучаемых явлений и событий; **Владеть** навыками сопоставлять факты мировой и отечественной истории в контексте других знаний гуманитарного и специально профессионального характера		
ОК-5 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	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования		
ОК-6 Способностью работать в	**Знать**: определения базовых понятий и категорий теории коммуникации;		

коллективе, толерантно воспринимая социальные, культурные и иные различия	формы, уровни и виды коммуникации; структуру коммуникационного процесса; специфику массовой коммуникации; основные положения теорий взаимодействия иаудитории; **Уметь**: дифференцировать, характеризовать и оценивать формы, уровни и виды коммуникации; выстраивать (моделировать) коммуникацию по заданным моделям и видам; отличать массовую коммуникацию от других видов коммуникации по основным параметрам – адресант, адресат, сообщение, каналы, код, эффект; дифференцировать, характеризовать и оценивать отдельные компоненты, составляющие структуру коммуникационного процесса; дифференцировать, характеризовать и оценивать основные положения теорий взаимодействия СМК и аудитории; использовать и при необходимости трансформировать теоретические модели в соответствии с конкретной (реальной) коммуникативной ситуацией; оценивать особенности аудитории, удерживать и активировать ее внимание; **Владеть**: навыками деловой коммуникации; способностью к обобщению, анализу, восприятию информации; базовыми навыками, составляющими коммуникативную компетентность личности, включая навык оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и вотношении собственной личности		
ОК-7 Способностью к	**Знать**: базовую лексику общего языка, лексику представляющую		

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	нейтральный научный стиль, а также основную техническую терминологию; наиболее употребительную (базовую) грамматику и основные грамматические явления, характерные для регистра научной речи лексику и фразеологию, отражающую основные направления технической науки в области радиофизики; основные элементы понимания делового письма; основные приемы аннотирования, реферирования и перевода научно-технической литературы **Уметь**: понимать устную (монологическую и диалогическую) речь на бытовые и специальные темы воспринимать на слух и участвовать в обсуждении тем, связанных со специальностью; читать и понимать со словарем научную литературу по общим и специальным вопросам **Владеть**: навыками разговорно-бытовой речи (владеть нормативным произношением и ритмом речи и применять их для беседы на бытовые и специальные темы) навыками чтения научной литературы с целью извлечения информации; основными навыками (неофициального и делового) письма; основными навыками публичной речи – делать научные сообщения, доклады (с предварительной подготовкой)		
ОК-8 Способностью к самоорганизации и самообразованию	**Знать**: научно-психологические основы выбора, процессуально-структурные компоненты психологического феномена «выбор», основныенаправления современной этики, базовые элементы и приемы, применяемые в подготовленной публичной речи **Уметь**: составлять перспективный план жизни, сучетом возможных препятствий, решать конфликтные ситуации, опираясь на		

	знания о стратегиях поведения, аргументированно излагать свои моральные убеждения и составлять хорошее самостоятельное публичное выступление **Владеть**: приемами самооценки, эффективного общения и слушания, позитивного общения, конгруэнтного поведения, анализа собственных нравственных ценностей и поступков, подготовки, корректировки выступления		
ОК-9 Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	**Знать**: влияние физической культуры на укрепления здоровья, профилактику профессиональных заболеваний и вредных привычек; основные средства и методы физического воспитания; основы здорового образа жизни; методы оценки физического развития, физической подготовленности средствами физической культуры и спорта в студенческом возрасте **Уметь**: использовать средства и методы физической культуры в регулировании своего психофизического состояния; выполнять комплексы упражнений оздоровительной и профессионально прикладной направленности; **Владеть**: навыком самостоятельно применять средства и методы физического воспитания в укреплении здоровья, методами контроля состояния организма при нагрузках; навыками ведения здорового образа жизни, участия в физкультурно-оздоровительной деятельности.		
ОПК-1 Способностью анализировать физические явления и процессы для	**Знать**: основные физические величины и понятия механики; основные физические законы, описывающие динамику материальной точки и систем материальных точек основные физические зако ны, описывающие динамику		

решения профессиональных задач	твердого тела основные физическиепредставления механики колебаний и волн; основные физическиепредставления гидрогазодинамики; основные понятия, законы и модели молекулярной физики основные законы классической электродинамики; основные методы электрическихизмерений фундаментальную базу теоретических знаний по оптике, основные понятия, законы и модели атомной и ядерной физики, методы математического анализа объектов и явлений микромира на основе уравнений квантовой механики; возможные сферы приложения законов и моделей атомной и ядерной физики; негативные факторы техносферы, их воздействие на человека **Уметь**: правильно соотносить содержание конкретных задач с законами физики, эффективно применять общие законы физики для решения конкретных задач в области физики и на междисциплинарных границах физики с другими областями знаний; пользоваться физическими приборами, ставить и решать простейшие экспериментальные задачи, обрабатывать, анализировать иоценивать полученные результаты; строить математические модели простейших физических явлений и использовать для изучения этих моделей доступныйему математический аппарат, включая методы вычислительнойматематики; использовать при работе справочную и учебную литературу, находить другие необходимые источники информации и работать с ними; понимать, излагать и критически анализировать базовую общефизическую информацию применять основные законы и методы электродинамики для решения прикладных задач		

	применять основные законы и методы оптики для решения прикладных задач; студенты должны овладеть приемами и методами решения практических задач оптики, требующих использования разнообразных математических методов **владеть**: навыками использования основных законов механики и молекулярной физики для анализа различных механических и физических систем; навыками оценки на основе физических законов характера механических и физических процессов для различных систем и сред; навыками использованияматематического аппарата для решения физических задач навыками и методиками проведения электрических и магнитных измерений, конструирования контрольно-измерительныхустройств и экспериментальных установок использования технических средств для определения основных параметров техно-логического процесса, изучения свойств физико-технических объектов, изделий и материалов методами обработки данных измерений физических величин, навыками работы с современным экспериментальным оборудованием, методами защиты человека от опасных и вредных факторов; способностью к правильному использованию общенаучной и специальной терминологии в профессиональной области; математическими методами и моделями для описания физических явлений, физического эксперимента, включая методы оценки точности экспериментальных измерений		
ОПК-2 Способностью применять соответствующий математический	**знать**: основные положения теории пределовфункций, основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; основы векторного анализа		

аппарат для решения профессиональных задач	основы аппарата теории обыкновенных дифференциальных уравнений, необходимых для решения теоретических и практических задач **уметь**: ориентироваться в постановках задач; строго доказывать математическое утверждение; определять возможности применения методов математического анализа; пользоваться библиотеками прикладных программ и пакетами программ для решения приклад ных математическихзадач использовать математические методы при решении прикладных задач, приводящих к обыкновенным дифференциальным уравнениям **владеть**: практическими навыками решения основных задач теории пределов функций, дифференцирования, интегрирования навыками решения типовых задач с применением изучаемого теоретического материала; навыками математического исследования динамических проблем из различных областей физики		
ОПК-3 Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	**Знать**: - принципы работы изучаемых электронных устройств и понимать физические процессы, происходящих в них; основные законы и методы расчета электрических цепей; - назначение, принцип работы, основные характеристики и обозначение полупроводниковых элементов, операционных усилителей, интегральных сборок и устройств на их основе; - принципы построения различных вариантов схем электронных устройств с отрицательной и/или положительной обратными связями (ОС), понимать причинывлияния ОС на основные показатели и стабильность параметров изучаемых устройств; понимать		

	причины возникновения неустойчивой работы усилителей с отрицательной ОС; - способы оценки устойчивости электронных устройствс внешними цепями ОС; - принципы и алгоритмы работы устройств формирования и генерирования сигналов; - принципы и алгоритмы работы радиоприемных - - устройств и устройств обработки сигналов; принципиальные схемы и элементную базу устройств, осуществляющих модуляцию и детектирование сигналов. **Уметь**: - объяснять физическое назначение элементов и влияние их параметров на электрические параметры и частотные свойства базовых каскадов аналоговых схем; - применять на практике методы исследования аналоговых электронных устройств, основанных на аналитических и графо-аналитических процедурах анализа; - выполнять расчеты, связанные с выбором режимов работы и определением параметров изучаемых электронных устройств; - формировать цепи ОС с целью улучшения качественных показателей и получения требуемых форм характеристик аналоговых электронных устройств; - проводить компьютерное моделирование и проектирование аналоговых и инфокоммуникационных электронных устройств, а также иметь представление о методах компьютерной оптимизации таких устройств; - пользоваться справочными материалами («Datasheet») на аналоговые и цифровые элементы и ИС при проектировании телекоммуникационных устройств; - определять причины неисправностей инфокоммуникационных устройств и выбраковывать неисправные элементы;		

	составлять, подготавливать и заполнять техническую документацию, требуемую в порядке эксплуатации инфокоммуникационного оборудования **Владеть**: - навыками чтения и изображения электронных схем на основе современной элементной базы; - навыками составления эквивалентных схем на базе принципиальных электрических схем изучаемых устройств; - навыками проектирования и расчета простейших аналоговых и цифровых схем; - навыками работы с контрольно-измерительной аппаратурой; - навыками компьютерного моделирования и проектирования аналоговых и цифровых телекоммуникационных устройств; навыками поиска и устранения простых неисправностей		
ОПК-4 Способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	**Знать**: об объектах информационной безопасности; о направлениях защиты информации; о требованиях к системам защиты информации **Уметь**: использовать основные принципы организации режима защиты информации ориентироваться в вопросах, связанных с технологией защиты информации **Владеть**: навыками извлечения информации из различных источников, представления ее в удобном виде и эффективного использования		
ОПК-5 Способностью использовать нормативные	**Знать**: структуру системы управления информационной безопасность; приемы управлению информационной безопасностью		

правовые акты в профессиональной деятельности	методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз **Уметь**: выделять процессы управления информационной безопасностью защищаемых объектов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью; выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации; обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте. **Владеть**: правилами, процедурами, практические приемы и пр. для управления информационной безопасности системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты методами и средствами минимизации угроз за счет совершенствования процессов управления		
ОПК-6 Способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать	**Знать**: правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности» поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу радиоактивных веществ (РВ) и ХОВ, современных средств поражения анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов методы прогнозирования и оценки ЧС сигналы оповещения ГО и порядок действийнаселения по сигналам		

мероприятия по охране труда и технике безопасности	порядок и содержание работ руководителей предприятий, учреждений, организаций, независимо от их организационно-правовой формы, а также их подразделений по управлению действиями подчиненных в ЧС в соответствии с получаемой специальностью средства и методы повышения безопасности, экологичности и устойчивости технических средств и технологических процессов **Уметь**: проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям эффективно применять средства защиты от негативных воздействий разрабатывать мероприятия по повышению безопасности и экологичности производственнойдеятельности планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных идругих неотложных работ при ликвидации последствий чрезвычайных ситуаций составлять планы мероприятий по повышению собственной адаптивности анализировать, выявлять и конструировать собственные адаптивные стратегии четко действовать по сигналам оповещения, практически выполнять основные мероприятиязащиты от опасностей, возникающих при ведении военных действий или вследствие этих действий, атак же от ЧС природного и техногенного характера **Владеть**: методами прогнозирования чрезвычайных ситуаций и предотвращения их негативных последствий методами повышения безопасности, экологичностии		

	устойчивости технических средств и технологических процессов некоторыми методами повышения стрессоустойчивости. способами управления эмоциями в экстремальных ситуациях		
ОПК-7 Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**Знать**: основные понятия и теоремы теории информации и кодирования; основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования особенности различных подходов к организации информационного обеспечения особенности научного исследования в области информатики и вычислительной техники, важнейшие методологические принципы научного исследования на базовом уровне **Уметь**: вычислять количество информации в сообщениях дискретного источника канала связи; кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач		

	проектировать, оценивать и реализовывать информационное обеспечение информационных систем осуществлять корректную постановку задачи исследования в области информатики и вычислительной техники на базовом уровне **Владеть**: основными методами кодирования и декодирования информации для различных задач средствами визуализации результатов научного исследования, средствами построения информационных ресурсов современными программными пакетами проведения моделирования на базовом уровне		
ПК-1 Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать**: способы классифицирования информационных ресурсов, подлежащих защите, угрозы безопасности информации, способы определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; **Уметь**: классифицировать информационные ресурсы, подлежащие защите, угрозы безопасности информации; определять пути их реализации на основе анализа структуры и содержания		

	информационных процессов и особенностей функционирования объекта защиты; определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения **Владеть**: навыками классифицирования информационных ресурсов, подлежащих защите, методами определения угроз безопасности информации, способами определения путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		
ПК-2 Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать**: основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; **Уметь**: определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий **Владеть**: методикой определения отказоустойчивости автоматизированных систем;		

	методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей		
ПК-3 Способностью администрировать подсистемы информационной безопасности объекта защиты	**Знать**: задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы; методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Уметь**: применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации; обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности **Владеть**: средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков		
ПК-4 Способностью участвовать в работах по	**Знать**: этапы и модели жизненного цикла информационных систем; корпоративные стандарты и методики;		

реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	принципы хранения, защиты, передачи и получения информации в корпоративных сетях **Уметь**: разрабатывать структуру распределенных систем; создавать клиент-серверные приложения для распределенных систем; проектировать хранилища данных; выполнять анализ корпоративных данных **Владеть**: навыками защиты информации в корпоративных сетях связи		
ПК-5 Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**Знать**: правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области компьютерной безопасности **Уметь**: применять действующую законодательную базу в области обеспечения компьютерной безопасности; классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем **Владеть**: навыками работы с нормативными правовыми актами; навыкамиработы с технической документацией на ЭВМ и		

	вычислительных системах; навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках		
ПК-6 Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным		

	требованиям по защите информации		
ПК-7 Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования		
ПК-8 Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических	**Знать**: терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности вкомпьютерной сфере **Уметь**: пользоваться современной научно-технической информацией по исследуемымпроблемам и задачам;		

документов	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации **Владеть**: навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; с технической документацией на компоненты компьютерных систем на русском и иностранном языках		
ПК-9 Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	**Знать**: направления создания правовой базы в области информационной безопасности; области примененияполученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну **Уметь**: разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов **Владеть**: навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; разработки специализированной проектной и технической документации		
ПК-10 Способностью проводить анализ информационной	**Знать**: основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы; понятия и виды		

безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности **Уметь**: определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфики объекта защиты; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач **Владеть**: способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации; навыками установки, настройки и обслуживания программно-аппаратных средств защиты информации; навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов; навыками оценки защищенности объектов информатизации		
ПК-11 Способностью	**Знать**: физические основы образования технических каналов		

проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; основные программные и аппаратные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; **Уметь**: использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; решать типовые задачи в области структурного анализа информационных процессов и систем; проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; проводить классификацию экспериментов; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки погрешностей результатов экспериментов; применять системы компьютерной математики для решения типовых задач **Владеть**: навыками организации охраны на объектах информатизации; навыками применения технических		

	средств защиты информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; умение пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну		
ПК-12 Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать**: основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; методики и стандарты оценки погрешностей измерений; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации **Уметь**: разрабатывать модели угроз и нарушителей информационной безопасности информационных систем;		

	разрабатывать частные политики информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять основные теоретико-числовые методы к решению задачам защиты информации **Владеть**: методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; навыками аналитического и численного решения задач; методами проведения физического эксперимента с последующей обработкой их результатов; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации		
ПК-13 Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной	**Знать**: типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования		

безопасности, управлять процессом их реализации	технических каналов утечки информации; **Уметь**: определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования		
ПК-14 Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать**: назначение, виды и принципы построения организации и управления службы защиты информации **Уметь:** применять современные компьютерные технологии для решения профессиональных задач; ориентироваться в сети научных и образовательных порталов сети Интернет; обрабатывать результаты полученных измерений с помощью математических программных продуктов **Владеть**: навыками работы **с** пакетами прикладных программ компьютерного моделирования; компьютерными технологиями, необходимыми для обмена научной информации		
ПК-15 Способностью	**Знать**: основные принципы организации технического,		

организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии **Уметь**: осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; оценивать эффективность системы защиты информации **Владеть**: навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения		

	возможностей несанкционированного доступа к защищаемой информации		
ПКУ-1 Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики	**Знать**: теоретические основы построения клиент-серверных веб-приложений, общие методы программирования механизмы реализации сетевых угроз по протоколам передачи данных HTTP, FTP, а также известные уязвимости веб-серверов **Уметь**: использовать полученные теоретические знания для решения конкретных прикладных задач, программировать клиент-серверные приложения с применением СУБД для обработки данных, находить и исправлять ошибки в программном коде конфигурировать клиент-серверное программное обеспечение с учетом требуемых параметров сетевой безопасности, анализировать возможные каналы утечки информации **Владеть**: практическими навыками конфигурирования и администрирования веб-серверов, а также навыками настройки систем управления контентом практическими навыками, по оценке защищенности веб-приложений		

4.1. Примерная тематика выпускных квалификационных работ по направлению подготовки 10.01.01 «Информационная безопасность» (профиль подготовки «Организация и технология защиты информации»).

1. Построение виртуальной защищённой сети с учетом требований безопасного хранения ключевой информации в организации
2. Разработка комплекса процедур аудита информационной безопасности Scada систем
3. Разработка методики управления инцидентами и событиями информационной безопасности
4. Модель защиты веб ресурсов на основе CMS
5. Модернизация системы защиты информации на предприятии
6. Автоматическая атака Wi-Fi «Twincy»
7. Исследование ПЭМИН от видеосредств при обработке конфиденциальной информации программно-аппаратным комплексом "Навигатор-П5М"
8. Разработка подсистемы фильтрации электронных почтовых сообщений от спама и вредоносного содержимого с использованием машинного обучения
9. Защита информации при использовании электронной почты
10. Разработка системы защиты информации для систем видеонаблюдения
11. Организация системы контроля и управления доступом с применением биометрических персональных данных
12. Разработка системы защиты обмена электронными почтовыми отправлениями
13. Разработка системы информационной безопасности для лаборатории защиты информации
14. Разработка системы обеспечения информационной безопасности корпоративной сети
15. Разработка системы обеспечения информационной безопасности на примере предприятия
16. Исследование распространения виброакустических колебаний в

инженерных коммуникациях АПК «Смарт»

17. Разработка системы обеспечения информационной безопасности удалённого доступа к внутренним информационным ресурсам для коммерческой организации

18. Разработка средства обнаружения сетевой разведки

19. Совершенствование системы защиты информации в ООО «МечелБизнессервис»

20. Разработка спам-фильтра для сервера корпоративных сетей

21. Разработка проекта системы защиты оконных проемов и решеток специальных помещений

22. Инструментальный аудит удаленного автоматизированного рабочего места

23. Разработка системы защиты конфиденциальной информации от несанкционированного разглашения

24. Разработка системы защищенного документооборота в организации с обработкой персональных данных в автоматизированных системах

25. Организация защиты персональных данных в организации

26. Разработка проекта комплексной защиты информации (обеспечения ИБ) хлебзавод ООО"TURON-NON"

27. Методы защиты автоматизированной системы учета оплаты проезда в муниципальной системе пассажирских перевозок города Калининграда

28. Разработка механизмов защиты диспетчерских компонентов сетей АСУ ТП

29. Разработка проекта системы защиты периметра корпоративный сети коммерческой организации

30. Разработка проекта системы защиты от утечки конфиденциальной информации регионального органа исполнительной власти

31. Разработка программного обеспечения для выявления снифинга в локальных вычислительных сетях

32. Разработка методики измерения экранирующих свойств альтернативных

измерительных площадок программно-аппаратным комплексом «Навигатор 5»

33. Разработка систем обеспечения информационной безопасности промышленного предприятия.

34. Проектирование системы центра реагирования на инциденты информационной безопасности на примере образовательного учреждения

35. Разработка проекта защиты конфиденциальной информации помещения ситуационного центра правительства Калининградской области

36. Разработка программного обеспечения для повышения уровня защищенности конфиденциальной информации

37. Оценка уровня информационной безопасности предприятия и пути совершенствования комплексной системы защиты от информационных угроз

38. Модернизация аппаратного комплекса ситуационного центра правительства Калининградской области

39. Разработка механизмов защиты сетей компьютерных классов общеобразовательной школы

40. Разработка методики измерения затухания альтернативных измерительных площадок программно-аппаратным комплексом «Навигатор 5»

4.2. Примеры формулировки тем и содержания выпускных квалификационных работ

Тема: Разработка механизма защиты диспетчерских компонентов сетей АСУ ТП

Введение

Глава 1. Теоретическая часть.

1.1 Особенности построения и функционирования распределенной многоуровневой АСУ ТП

1.2 Структура многоуровневой АСУ ТП на базе MasterSCADA

1.3 SCADA-система и особенности ее защиты

Глава 2 Повышение защищенности подсистем диспетчерского уровня АСУ ТП.

2.1 Определение архитектуры разрабатываемых механизмов выявления и

блокирования программ.

2.2 Разработка алгоритмов выявления и блокирования вредоносных программ.

2.3 Определение особенностей эксплуатации разработанных механизмов.

Глава 3. Определение эффективности разработанных механизмов защиты.

Заключение.

Список использованных источников

1. ГОСТ Р МЭК 61131-3-2016 Национальный стандарт Российской Федерации. Контроллеры программируемые. Часть 3. Языки программирования" (утв. и введен в действие Приказом Росстандарта от 13.05.2016 N 313-ст) из информационного банка "Отраслевые технические нормы" «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru
2. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 09.08.2018) "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (Зарегистрировано в Минюсте России 30.06.2014 N 32919)
3. Байрс Э. IT-безопасность в промышленности. Глубокий анализ пакетов данных для SCADA-систем // Современные технологии автоматизации. - 2013.-№4. – с.12-16.
4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] – URL:http://window.edu.ru/
5. Антивирусная утилита [Электронный ресурс] – URL:http://z-oleg.com/
6. Втюрин В.А. Автоматизированные системы управления технологическими процессами. Основы АСУ ТП: учебное пособие для студентов высшего учебного заведений // -СПб.: Санкт-Петербургская Государственная Лесотехническая Академия имени С.М. Кирова, 2006. -152
7. «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru

8. Зайцев О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. – СПб.: БХВ-Петербург, 2006. – 304 с.
9. Котенко И. В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. – 2004. – № 1. – с. 56–72.
10. MasterSCADA-система для АСУ ТП [Электронный ресурс] – URL:https://masterscada.insat.ru/
11. Определение эффективности [Электронный ресурс] – URL:https://dsec.ru/
12. Подтопельный В. В. Особенности информационной защиты систем управления на промышленных объектах // III БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2015 г., с. 74-78.
13. Подтопельный В. В. Уязвимости системы информационного сопровождения судов // II БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2014 г., с. 70-74.
14. Фаулер, М. UML. Основы. Учебное пособие [Текст] / М. Фаулер. – Символ-Плюс, 2007. – 192 с.: ил. – 2000 экз. – ISBN: 5-93286-060-5
15. Щербаков А. Сеть CAN: популярные прикладные протоколы // ChipNews,1999, №5.

ПРИЛОЖЕНИЯ

Приложение 1

Оценочный лист сформированности компетенций для руководителя ВКР и членов ГЭК

Коды проверяемых компетенций	Текст ВКР	Этап подготовки к процедуре защиты ВКР
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	+	+
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	+	+
ПКУ-1	+	+

Приложение 2

Оценочный лист членов ГЭК

Оценка уровня сформированности компетенций студента _____ направления подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации защиты информации» в процессе защиты выпускной квалификационной работы, выполненной на тему

_____

_____

Коды проверяемых компетенций	**Показатели оценки результата**	**Показатели уровня сформированности компетенций**			
		2 – низкий	**3 – средний**	**4 – достаточный**	**5 – высокий**
ОК-1	Способностью использовать основы философских знаний для формирования мировоззренческой позиции				
ОК-2	Способностью использовать основы экономических знаний в различных сферах деятельности				
ОК-3	Способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма				
ОК-4	Способностью использовать основы правовых знаний в различных сферах деятельности				
ОК-5	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-6	Способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия				
ОК-7	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-8	Способностью к самоорганизации и самообразованию				
ОК-9	Способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности				
ОПК-1	Способностью анализировать физические явления и процессы для решения профессиональных задач				
ОПК-2	Способностью применять соответствующий математический аппарат для решения профессиональных задач				
ОПК-3	Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач				
ОПК-4	Способностью понимать значение информации в				

	развитии современного общества, применять информационные технологии для поиска и обработки информации				
ОПК-5	Способностью использовать нормативные правовые акты в профессиональной деятельности				
ОПК-6	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-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
ПК-3	Способностью администрировать				

	подсистемы информационной безопасности объекта защиты				
ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
ПК-7	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
ПК-8	Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов				
ПК-9	Способностью осуществлять подбор, изучение и обобщение				

	научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности				
ПК-10	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
ПК-11	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов				
ПК-12	Способностью принимать участие в проведении экспериментальных исследований системы защиты информации				
ПК-13	Способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
ПК-14	Способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности				
ПК-15	Способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими				

	документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
ПКУ-1	Способен самостоятельно приобретать и использовать в практической деятельности новейшие и технологические достижения в области саморазвития и/или построении карьеры и/или педагогики				