МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

Программа адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Составитель:

к.и.н., доцент, заведующий кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДАЮ

Руководитель ОПОП ВО

10.03.01 «Информационная безопасность»

Г.А. Шевцова

26.03.2024

СОГЛАСОВАНО:

Заведующий кафедрой

Информационной безопасности Г.А. Шевцова
26.03.2024

И.о. заведующего кафедрой

Комплексной защиты информации Д.А. Митюшин

26.03.2024

1. Общие положения

1.1. **Целью** государственной итоговой аттестации (ГИА) выпускников является установление соответствия уровня профессиональной подготовки требованиям ФГОС ВО - Бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного и введенного в действие приказом Министерства образования и науки РФ от 17 ноября 2020 г. № 1427

1.2. Формами государственной итоговой аттестации являются:

- Государственный экзамен
- Защита выпускной квалификационной работы (далее – ВКР).

1.3. Виды профессиональной деятельности выпускников и соответствующие им задачи профессиональной деятельности:

- организационно-управленческая деятельность:
  - осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
  - организация работы малых коллективов исполнителей;
  - участие в совершенствовании системы управления информационной безопасностью автоматизированных систем;
  - изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
  - контроль эффективности реализации политики информационной безопасности автоматизированных систем.
- эксплуатационная деятельность:
  - установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учётом установленных требований;
  - администрирование подсистем информационной безопасности автоматизированных систем;
  - участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;
- проектно-технологическая деятельность:
  - сбор и анализ исходных данных для проектирования систем защиты информации автоматизированных систем, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
  - проведение проектных расчётов элементов систем обеспечения информационной безопасности автоматизированных систем;
  - участие в разработке технологической и эксплуатационной документации;
  - проведение предварительного технико-экономического обоснования проектных расчётов;
- экспериментально-исследовательская деятельность:
  - подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов
  - составление обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

- работа с программным обеспечением с соблюдением действующих требований по защите информации

1.4. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы высшего образования

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
Универсальные компетенции (УК)			
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Применяет знание основных теоретико-методологических положений философии, концептуальных подходов к пониманию природы информации как научной и философской категории, методологических основ системного подхода;		V
	УК-1.2 Формирует и аргументировано отстаивает собственную позицию по различным философским проблемам, обосновывает и адекватно оценивает современные явления и процессы в общественной жизни на основе системного подхода.		V
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач		V
	УК-2.2 Способность использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.		V
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 Понимает эффективность использования стратегии сотрудничества для достижения поставленной цели; определяет роль каждого участника в команде;		V
	УК-3.2 Эффективно взаимодействует с членами команды; участвует в обмене информацией, знаниями и опытом;		V

	содействует презентации результатов работы команды; соблюдает этические нормы взаимодействия		
УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1 Владеет системой норм русского литературного языка и нормами иностранного (-ых) языка (-ов); способен логически и грамматически верно строить коммуникацию, используя вербальные и невербальные средства взаимодействия		V
	УК-4.2 Свободно воспринимает, анализирует и критически оценивает устную и письменную общепрофессиональную информацию на русском и иностранном (-ых) языке (-ах); демонстрирует навыки перевода с иностранного (-ых) на государственный язык, а также с государственного на иностранный (-ые) язык (-и)		V
	УК-4.3 Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач для достижения профессиональных целей на государственном и иностранном (-ых) языках		V
УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1 Демонстрирует толерантное восприятие социальных и культурных различий, уважительное и бережное отношению к историческому наследию и культурным традициям;		V
	УК-5.2 Проявляет в своём поведении уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте мировой истории и культурных традиций мира		V
	УК-5.3 Понимает межкультурное разнообразия общества в его различных контекстах: философском, социально-		V

	историческом, этическом.		
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 Определяет цели собственной деятельности, оценивая пути их достижения с учётом ресурсов, условий, средств, временной перспективы развития деятельности и планируемых результатов;		V
	УК-6.2 Формулирует цели собственной деятельности, определяя пути их достижения с учётом ресурсов, условий, средств, временной перспективы развития деятельности и планируемых результатов.		V
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1 Выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учётом физиологических особенностей организма;		V
	УК-7.2 Планирует своё рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности;		V
	УК-7.3 Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности		V
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1 Понимает цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.	V	V
	УК-8.2 Использует знания системы гражданской обороны, структуры РСЧС и их основные задачи, как часть системы общегосударственных мероприятий.	V	V
	УК-8.3 Оказывает первую помощь в очаге поражения, используя средства индивидуальной и коллективной защиты.	V	V

УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знает основные законы и закономерности функционирования экономики; основы экономической теории, необходимые для решения профессиональных и социальных задач	V	V
	УК-9.2 Умеет применять экономические знания при выполнении практических задач; принимать обоснованные экономические решения в различных областях жизнедеятельности	V	V
	УК-9.3 Владеет методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач	V	V
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями		V
	УК-10.2 Умеет анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению		V
	УК-10.3 Владеет навыками работы с законодательными и другими нормативными правовыми актами		V
Общепрофессиональные компетенции (ОПК)			
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации	V	
	ОПК-1.2 Умеет классифицировать и оценивать угрозы информационной безопасности	V	
	ОПК-1.3 Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире	V	

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1 Знает классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных	V	
	ОПК-2.2 Умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	V	
	ОПК-2.3 Владеет навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности	V	
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1 Знает основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации	V	
	ОПК-3.2 Умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач	V	
	ОПК-3.3 Владеет навыками использования справочных материалов по математическому анализу, использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач	V	
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1 Знает основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики	V	
	ОПК-4.2 Умеет делать выводы и формулировать их в виде отчёта о проделанной	V	

	исследовательской работе		
	ОПК-4.3 Владеет методами расчёта	V	
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации	V	V
	ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	V	V
	ОПК-5.3 Владеет навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации	V	V
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	V	V
	ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации	V	V
	ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации	V	V
ОПК-7 Способен использовать языки программирования и	ОПК-7.1 Знает основные принципы построения компьютера, формы и способы представления данных; области и	V	

технологии разработки программных средств для решения задач профессиональной деятельности	особенности применения языков программирования высокого уровня		
	ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач	V	
	ОПК-7.3 Владеть навыками разработки, документирования, тестирования и отладки программ; разработки алгоритмов решения типовых профессиональных задач	V	
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 Знает принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией		V
	ОПК-8.2 Уметь обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами		V
	ОПК-8.3 Владеет навыком составления и оформления отчётных документов по результатам обзора научно-технической литературы, нормативных и методических документов		V
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	V	
	ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	V	

	ОПК-9.3 Владеет методами и средствами криптографической и технической защиты информации	V	
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1 Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	V	
	ОПК-10.2 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	V	
	ОПК-10.3 Владеет принципами формирования политики информационной безопасности объекта информатизации	V	
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1 Знает стандартные вероятностно-статистические методы анализа экспериментальных данных	V	
	ОПК-11.2 Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных	V	
	ОПК-11.3 Владеет навыками по проведению эксперимента по заданной методике с составлением итогового документа	V	
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта	V	
	ОПК-12.2 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	V	
	ОПК-12.3 Владеет навыками по разработке	V	

	основных показателей технико-экономического обоснования соответствующих проектных решений		
ОПК-13 Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-13.1 Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире	V	
	ОПК-13.2 Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории	V	
	ОПК-13.3 Владеет навыками по соотнесению общих исторических процессов и отдельных фактов, выявлению существенных черт исторических процессов, явлений и событий	V	
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1 Знает принципы построения систем защиты информации; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя		V
	ОПК-2.1.2 Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей		V
	ОПК-2.1.3 Владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации		V
ОПК-2.2 Способен формировать предложения по оптимизации	ОПК-2.2.1 Знает организационные меры по защите информации, основные методы управления защитой информации		V

структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации		V
	ОПК-2.2.3 Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации		V
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации		V
	ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям		V
	ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям		V
ОПК-2.4 Способен проводить аудит защищенности объекта	ОПК-2.4.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер		V

информатизации в соответствии с нормативными документами	защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации		
	ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации		V
	ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств		V
Профессиональные компетенции по видам деятельности (ПК)			
Тип задач проф. деятельности: Эксплуатационный			
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1 Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации	V	
	ПК-1.2 Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации	V	
	ПК-1.3 Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	V	
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы	ПК-2.1 Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования	V	
	ПК-2.2 Умеет противодействовать угрозам	V	

программирования для решения профессиональных задач	безопасности информации с использованием встроенных средств защиты информации		
	ПК-2.3 Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах	V	
ПК-3 Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1. Знает требования к встроенным средствам защиты информации программного обеспечения	V	
	ПК-3.2. Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила	V	
	ПК.3.3. Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	V	
ПК-4 Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4.1. Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о		
	ПК-4.2. Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищенности и доверия		
	ПК-4.3. Владеет навыками разработки руководящих документов по защите информации в организации		
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	V	
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить	V	

	аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации		
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации	V	
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	V	
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	V	
	ПК-6.3 Владеет навыками определения уровня защищённости и доверия средств защиты информации	V	
Тип задач проф. деятельности: Проектно-технологический			
ПК-7 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.1 Знает разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении	V	
	ПК-7.2 Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении	V	
	ПК-7.3 Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении	V	
ПК-8 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на	V	

	соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД		
	ПК-8.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении	V	
	ПК-8.3 Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении	V	
Тип задач проф. деятельности: экспериментально-исследовательский			
ПК-9 Способен 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-9.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	V	
	ПК-9.2 Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации	V	
	ПК-9.3 Владеет организационными мерами по защите информации	V	
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	V	
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах	V	

	информатизации, и характере обрабатываемой на них информации		
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	V	
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем	V	
	ПК-11.2 Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта	V	
	ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости	V	
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации	V	V
	ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации	V	V
	ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчётных и исследовательских задач	V	V
Тип задач проф. деятельности: Организационно-управленческий			
ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями	V	V

безопасности, управлении процессом их реализации	по эксплуатации		
	ПК-13.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	V	V
	ПК-13.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	V	V
ПК-14 Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ПК-14.1 Знает организацию проведения инструктажа руководящего состава и обучения персонала по вопросам защиты информации	V	V
	ПК-14.2 Умеет организовать работу персонала по использованию технических, программных (программно-технических) средств защиты	V	V
	ПК-14.3 Владеет навыками по осуществлению планирования и организации работы персонала с учетом требований по защите информации	V	V
ПК-15 Способен 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	ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков	V	V
	ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке	V	V
	ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты	V	V

	информации		

2. Программа государственного экзамена

2.1. Содержание экзамена

В билет государственного экзамена входят два вопроса. Первый вопрос – из разделов 1-2 программы. Второй вопрос – из раздела 3 или из разделов 4-6. Ниже приводятся примерный перечень вопросов, включаемых в билеты.

Раздел 1. Теория информационной безопасности и методология защиты информации – ***проверка сформированности компетенций - УК-1; УК-2; УК-3; УК-4; УК-5; УК-8; УК-9; ОПК-4; ОПК-6, ПК-5;***

1.1. Понятие и сущность информационной безопасности современного общества. Доктрина информационной безопасности Российской Федерации. – У***К-1; УК-2, УК-5, ОПК-4,***

1.2. Понятия «информация», «сообщение», «сведения», «документированная информация», «информационные технологии», информационные системы». Способы и средства документирования информации, возникающие угрозы. - У***К-1; ОПК-4***

1.3. Информация как предмет защиты. Понятие и сущность информационной безопасности объекта. - У***К-2, ОПК-4***

1.4. Понятие уязвимости информации. Формы и виды проявления уязвимости информации. - ***УК-1, ОПК-4***

1.5. Принципы, критерии и условия отнесения информации к защищаемой. - У***К-8***

1.6. Формы и методики отнесения информации к защищаемой. - У***К-2***

1.7. Классификация конфиденциальной информации по видам тайн. - У***К-4***

1.8. Понятие и структура угроз информации. - ***ОПК-6***

1.9. Источники, виды и способы дестабилизирующего воздействия на информацию. – У***К-7, ПК-5***

1.10. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию. - ***ОПК-6, ПК-5***

1.11. Каналы несанкционированного доступа к конфиденциальной информации. - У***К-7, ПК-5,***

1.12. Соотношение между каналами несанкционированного доступа и каналами утечки информации. - ***УК-2***

1.13. Методы несанкционированного доступа к информации, применяемые при использовании различных каналов доступа. - ***ПК-5***

1.14. Понятие, сущность и значение защиты информации. - ***УК-3, ОК-8***

1.15. Классификация носителей информации и особенности защиты зафиксированной на них информации. ***УК-1; ОПК-4***

1.16. Объекты защиты информации, их классификация и особенности. - ***УК-8***

1.17. Виды и способы дестабилизирующего воздействия на объекты защиты. - ***ОПК-6***

1.19. Принципы, цели и теоретические основы защиты информации. - ***УК-8***

1.20. Классификация видов защиты информации. - ***УК-8***

1.21. Классификация методов и средств защиты информации. - ***УК-8***

1.22. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к информации. - ***ПК-5***

1.23. Государственная система защиты информации. Основные функции межведомственной комиссии по защите государственной тайны. - ***УК-4, ОПК-7***

1.24. Сущность моделирования информационных процессов и систем. Разработка модели комплексной системы защиты информации. - ***УК-7, ПК-5***

Раздел 2. Комплексная система защиты информации (КСЗИ) на предприятии – ***проверка сформированности компетенций - УК-6; УК-9; ОПК-3; ПК-4; ПК-7; ПК-8; ПК-13; ПК-14***

2.1. Сущность, задачи и принципы функционирования комплексной системы защиты информации. ***ОПК-3, ПК-4, ПК-13***

2.2. Сущность и основные этапы организационного проектирования комплексной системы защиты информации. ***- УК-6, ПК-4, ПК-7, ПК-8***

2.3. Понятие и сущность управления комплексной системой защиты информации.- ***ПК-4, ПК-8***

2.4. Сущность и содержание контроля эффективности комплексной системы защиты информации. - ***ОПК-3, ПК-4, ПК-13***

2.5. Методы принятия управленческих решений в комплексной системе защиты информации. ***- УК-6,***

2.6. Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации.

2.7. Кадровое и ресурсное обеспечение защиты информации. ***- УК-6, УК-9, ПК-8, ПК-14***

Раздел 3. Правовая защита информации ***– проверка сформированности компетенций - УК-4; ПК-9, ПК-15***

3.1. Особенности правовой защиты государственной тайны. Определение понятия государственной тайны. Правовые основы защиты государственной тайны. Понятие о перечнях сведений, составляющих государственно тайну. Принципы и порядок отнесения сведений к государственной тайне. Степени секретности сведений. Порядок распоряжения сведениями, составляющими государственную тайну. Особенности передачи сведений, составляющих государственную тайну, другим государствам. Ограничение прав обладателя информации, в связи с ее засекречиванием. Органы по защите государственной тайны и их полномочия. Контроль и надзор за обеспечением защиты государственной тайны. Уголовно-правовая защита информации, составляющей государственную тайну. - ***УК-4, ПК-9***

3.2. Особенности правовой защиты служебной тайны. Определение понятия служебной тайны. Правовые основы защиты служебной тайны. Виды информации, относящейся к служебной тайне. Меры по охране конфиденциальности информации ограниченного доступа, переданной в государственные органы юридическими и физическими лицами. Полномочия руководителя федерального органа в отношении использования собственной служебной тайны. - ***УК-4, ПК-9, ПК-15***

3.3. Особенности правовой защиты коммерческой тайны. Определение понятия коммерческой тайны. Правовые основы защиты коммерческой тайны. Установление режима коммерческой тайны. Охрана коммерческой тайны в трудовых отношениях. Практические аспекты использования законодательства о коммерческой тайне. Особенности правовой охраны секретов производства (ноу-хау) в режиме коммерческой тайны. Ответственность за правонарушения, связанные с незаконным сбором, разглашением или использованием информации, составляющей коммерческую тайну. - ***УК-4, ПК-9***

3.4. Особенности правовой защиты персональных данных. Определение понятия персональные данные. Правовые основы защиты персональных данных. Разница между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права. Общедоступные источники персональных данных. Специальные категории персональных данных. Биометрические персональные данные. Право субъекта персональных данных на доступ к своим персональным данным. Обязанности оператора персональных данных. Классификация информационных систем персональных данных. - ***УК-4, ПК-9, ПК-15***

3.5. Правовое регулирование отношений в сфере авторского права. Определение авторских прав, как интеллектуальных прав на произведения литературы, науки и искусства.

Действие исключительных прав на эти произведения. Возникновение авторского права. Соавторство. Объекты авторских прав и объекты, на которые не распространяются авторские права. Личные неимущественные права. Исключительные имущественные права. Знак охраны авторского права. Срок действия исключительного права на произведение. Переход произведения в общественное достояние и переход исключительного права на произведение по наследству. Принцип исчерпания исключительных авторских прав на оригинал или экземпляр опубликованного произведения. Законодательно установленные случаи и порядок свободного воспроизведения и использования произведения. Порядок распоряжения автора своим исключительным правом. Договор об отчуждении исключительного права на произведение. Лицензионный договор о предоставлении права использования произведения. Права автора служебного произведения. - ***УК-4, ПК-9***

3.6. Правовое регулирование отношений в сфере прав, смежных с авторскими (смежные права) Определение прав, смежных с авторскими, как интеллектуальных прав на результаты исполнительской деятельности (исполнения), на фонограммы, на сообщение в эфир или по кабелю радио- и телепередач (вещание организаций эфирного и кабельного вещания), на содержание баз данных, а также на произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние. Знак правовой охраны смежных прав. Организации, осуществляющие коллективное управление авторскими и смежными правами и правовые основы деятельности. - ***УК-4, ПК-9***

3.7. Правовое регулирование отношений в сфере патентного права Определение патентных прав, как интеллектуальных прав на изобретения, полезные модели и промышленные образцы. Понятие автора и соавтора объекта патентного права. Понятие патента. Условия патентоспособности. Право авторства. Право на получение патента. Исключительное право на изобретение, полезную модель и промышленный образец, сроки действия исключительных прав, порядок распоряжения исключительным правом. Порядок получения патента. Государственная регистрация объектов патентных прав. Приоритет изобретения, полезной модели и промышленного образца. Особенности правовой охраны и использования секретных изобретений. Защита прав авторов изобретений, полезных моделей и промышленных образцов и патентообладателей. - ***УК-4, ПК-9***

3.8. Права на средства индивидуализации юридических лиц и индивидуальных предпринимателей, а также на средства индивидуализации производимых ими товаров, выполняемых работ или оказываемых услуг. Право на товарный знак, как средство обозначения, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей, а также для индивидуализации выполняемых ими работ или оказываемых ими услуг. Обладатель исключительного права на товарный знак. Виды товарных знаков. Свидетельство на товарный знак. Государственная регистрация товарного знака, основания для отказа в регистрации. Использование товарного знака и распоряжение исключительным правом на товарный знак. Последствия неиспользования товарного знака. Понятие общеизвестного товарного знака и особенности правовой охраны и использования такого знака. Защита права на товарный знак. Ответственность за незаконное использование товарного знака. - ***УК-4, ПК-9***

Раздел 4. Организационная защита информации. Защита и обработка конфиденциальных документов. **– *проверка сформированности компетенций - УК-4; ПК-8; ПК-9, ПК-10***

4.1. Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации. Установление и изменение степени ограничения доступа сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение и изменение грифа секретности работам, документам и изделиям. Понятие «рассекречивание сведений». Основания для рассекречивания сведений, документов и изделий. **- *УК-4; ПК-10***

4.2. Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих государственную тайну. Основные цели, задачи, функции уполномоченных органов по ведению лицензионной деятельности. Порядок лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Организация и проведение специальных экспертиз предприятий. Порядок рассмотрения заявлений предприятий о выдаче лицензии. Основания для выдачи (отказе) в выдаче лицензии, приостановлении действия или о ее аннулировании. Порядок проведения государственной аттестации руководителей предприятий. ***- УК-4; ПК-10***

4.3. Порядок сертификации средств защиты информации. Участники сертификации и их функции. Виды средств защиты информации, подлежащих сертификации. Порядок проведения сертификации средств защиты информации. Понятие о сертификате соответствия и знаках соответствия СЗИ-ГТ. Инспекционный контроль. ***- ПК-8; ПК-9, ПК-10***

4.4. Порядок допуска и доступа персонала и иных лиц к конфиденциальной информации. Допуск должностных лиц и граждан к государственной тайне. Основания для отказа или прекращения допуска. Ограничение прав. Переоформление допуска. Назначение и формы допусков к государственной тайне, порядок оформления и учета. Особенности доступа к конфиденциальной информации. Назначение, принципы и задачи разрешительной системы доступа к информации ограниченного доступа. Порядок оформления разрешения на доступ. Особенности доступа к информации лиц, командированных из других предприятий. ***- ПК-9, ПК-10***

4.5. Организация внутриобъектового и пропускного режимов. Виды охраняемых объектов. Виды, назначение и задачи охраны объектов, состав функций охраны. Построение системы охраны объекта, многорубежная охрана. Регламентация деятельности, обязанностей и ответственности персонала охраны. Взаимодействие персонала с техническими средствами сигнализирования, информирования и идентификации. Понятие, задачи и структура внутриобъектового режима. Назначение и задачи пропускного режима. Порядок организации доступа персонала в помещения различных категорий. Функционирование контрольно-пропускных пунктов. Виды пропусков и идентификаторов, их учет и порядок выдачи. Классификация посетителей. Правила работы с посетителями различных классификационных групп. Методы контроля за посетителями. Требования к помещениям для приема посетителей. ***- ПК-9, ПК-10***

4.6. Организационные требования к режимным помещениям. Требования, предъявляемые к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями. Порядок назначения комиссии для аттестации помещений на пригодность для ведения работ. Документальное оформление после обследования помещений на пригодность. Назначение ответственных лиц, имеющих право вскрывать и опечатывать режимные помещения. Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения секретных изделий и документов. Порядок приема-сдачи под охрану режимные помещения. ***- УК-1; ПК-9, ПК-10***

4.7. Организационная защита информации в процессе проведения совещаний и переговоров по конфиденциальным вопросам. Угрозы безопасности информации, задачи и направления ее защиты в процессе проведения совещаний и переговоров, приеме посетителей. Общие требования к отбору информации для оглашения. Правила подготовки и проведения совещаний и переговоров. Документирование информации, оформление протоколов и итоговых документов. Порядок осуществления аудио и видео записи. Требования к помещениям и их охране. ***- УК-2; ПК-9, ПК-10, ПК-13***

4.8. Организационная защита информации в процессе издательской, рекламной и выставочной деятельности. Угрозы безопасности информации, задачи и направления ее защиты в процессе издательской, рекламной и выставочной деятельности. Общие требования к отбору информации для оглашения. Порядок оформления разрешения на подготовку

материалов к открытому опубликованию. Применяемые методы защиты информации. Порядок работы со средствами массовой информации. Виды рекламной деятельности, порядок отражения информации в рекламных изданиях. Особенности и виды выставочной деятельности. Оформление разрешения на демонстрацию изделий, особенности защиты информации. - ***УК-1; ПК-9, ПК-10***

4.9. Организационная защита конфиденциальной продукции в процессе ее изготовления, хранения и транспортировки. Разработка и проведение мероприятий по обеспечению режима конфиденциальности. Учет продукции. Основания для снятия ее с учета. Особенности и порядок хранения. Основные требования при получении и транспортировке продукции. Документирование хода и результатов уничтожения продукции. - ***УК-2; ПК-8; ПК-9, ПК-10, ПК-14.***

4.10. Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности. Цели и задачи внутреннего расследования. Основания для проведения внутреннего расследования. Процедура проведения расследования. Состав комиссии (комиссий). Права и обязанности членов комиссии по проведению расследования. Документирование хода и результатов внутреннего расследования. 15 Обеспечение прав работника, в отношении которого проводится расследование. Меры, принимаемые по результатам расследования. Взаимодействие с правоохранительными органами. - ***УК-1; ПК-8; ПК-9, ПК-10***

4.11. Особенности учета носителей информации и проектов конфиденциальных документов. Угрозы информации в процессе составления и изготовления документов, задачи ее защиты. Виды учитываемых бумажных и технических носителей для составления документов. Назначение и задачи учета носителей. Состав основных процедур и особенности учета носителей конфиденциальной информации. Назначение и задачи учета изготавливаемых проектов конфиденциальных документов. Связь с другими видами учета. Состав основных процедур. Особенности изготовления и учета конфиденциальных документов. Состав учетных операций при издании документов. - ***ПК-8; ПК-9***

4.12. Назначение и особенности учета конфиденциальных документов. Цели, задачи и виды учета конфиденциальных документов, его место в технологической системе обработки и хранения документов. Угрозы документам в процессе учета, способы защиты информации. Назначение справочно-информационного банка данных по документам. Традиционный и автоматизированный учет. Назначение учета поступивших конфиденциальных документов. Процедура учета пакетов. Состав основных процедур учета поступивших документов. Назначение и особенности учета изданных конфиденциальных документов. Связь с другими видами учета. Состав основных процедур. Назначение учета конфиденциальных документов выделенного хранения. Связь с другими видами учета. Состав основных процедур. - ***ПК-8; ПК-9***

4.13. Классификация, формирование и хранение дел, содержащих конфиденциальные документы. Назначение номенклатуры дел, ее место в технологической системе обработки и хранения конфиденциальных документов. Содержание процедур составления, ведения и закрытия номенклатуры дел. Угрозы документам в процессе их формирования в дела и хранении. Процедура оформления дела при его заведении и формировании. Порядок формирования дел, правила их хранения. Задачи защиты информации, решаемые при формировании дел. Процедура 16 оформления дела при его закрытии. Назначение и задачи учета законченных производством дел, картотек и журналов. - ***ПК-8; ПК-9***

4.14. Передача документов в архив, уничтожение документов. Назначение экспертизы ценности документов, задачи экспертной комиссии. Процедура составления описи дел, передаваемых в ведомственный архив. Процедура подготовки документов различных категорий к уничтожению. Процедура составления акта на уничтожение. Состав документов и носителей, уничтожаемых без акта. Процедура уничтожения документов и ее документирование. - ***ПК-8; ПК-9***

4.15. Порядок работы с конфиденциальными документами. Угрозы документам в процессе работы с ними сотрудников предприятия, задачи защиты документов. Реализация разрешительной системы доступа к документам. Процедура рассмотрения документов руководителем. Процедуры ознакомления исполнителей с документами и передачи документов на исполнение. Процедуры получения документов от исполнителей. Организация внутреннего документооборота. Правила работы сотрудников с документами на бумажных и технических носителях, с электронными документами. Порядок хранения документов на рабочем месте. Хранение документов во внерабочее время. Учет документов, находящихся у исполнителей. ***- ПК-8; ПК-9***

4.16. Проверка наличия документов, дел и носителей информации. Назначение, задачи и типы проверок наличия документов, дел и носителей информации. Процедура ежедневной проверки наличия. Состав, объем и процедура квартальной проверки наличия. Состав, объем и процедура годовой проверки наличия. Основания и процедура внеплановой проверки наличия документов, дел и носителей информации. ***- ПК-8; ПК-9, ПК-14***

4.17. Экспедиционная обработка отправляемых конфиденциальных документов. Угрозы документам в процессе их экспедиционной обработки и доставки адресатам, задачи защиты. Назначение экспедиционной обработки документов. Состав процедур, сопровождающихся отправку конфиденциальных документов адресатам. Особенности обработки отправляемых и получаемых конфиденциальных документов. ***- ПК-8; ПК-9***

4.18. Работа с персоналом, допускаемым к конфиденциальной информации. Задачи и стадии работы с персоналом. Критерии и процедуры подбора персонала. Документирование приема. Соглашение о неразглашении тайны. Направления и методы текущей работы с персоналом. Задачи, принципы и способы обучение персонала. Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией. Виды морального и материального стимулирования. Процедуры увольнения работников и их документирование. ***- ПК-8; ПК-9, ПК-10***

4.19. Угрозы информации при документировании и задачи ее защиты. Способы и средства документирования конфиденциальной информации. Способы аудио и видео документирования. Средства документирования информации. Способы документирования с помощью технических средств. Средства копирования документов. Средства передачи информации. Классификация угроз информации при использовании средств документирования информации и задачи защиты информации. ***- УК-1; ПК-8; ПК-9, ПК-10***

Раздел 5. Инженерно-техническая защита информации. ***– проверка сформированности компетенций - ОПК-1; ПК-3, ПК-11; ПК-12***

5.1. Классификация демаскирующих признаков по характеристикам объектов и информативности. Мера информативности признака. Понятие об эталонной и текущей признаковых структурах. ***- ОПК-1***

5.2. Средства скрытного наблюдения за объектами. Принципы работы приборов ночного видения. Принципы работы локаторов бокового обзора, способы повышения разрешающей способности. ***- ОПК-1; ПК-11; ПК-12***

5.3. Способы и средства подслушивания с использованием технических средств. Особенности остронаправленных микрофонов. Особенности лазерного и СВЧ подслушивания. ***- ОПК-1; ПК-12***

5.4. Виды побочных электромагнитных излучений и наводок. Отличия пассивных и активных акустоэлектрических преобразователей. Условие возникновения паразитной генерации в усилителях. ***- ОПК-1; ПК-3, ПК-12***

5.5. Принципы инженерно-технической защиты информации и построения ее системы. Назначение и типы контролируемых зон. ***- ОПК-1; ПК-3, ПК-11; ПК-12***

5.6. Классификация и сущность методов инженерно-технической защиты информации. Основные показатели эффективности инженерно-технической защиты информации. ***- ОПК-1; ПК-3, ПК-11; ПК-12***

5.7. Назначение и виды физической защиты источников информации. Принципы работы системы контроля управления доступом. Достоинства и недостатки атрибутных и биометрических идентификаторов. - ***ОПК-1; ПК-3, ПК-11; ПК-12***

5.8. Способы и средства защиты информации от подслушивания. Условия эффективной защиты путем акустического зашумления помещения. - ***ОПК-1; ПК-12***

5.9. Способы и средства, используемые для защиты информации от наблюдения в оптическом и радиодиапазонах. - ***ОПК-1; ПК-12***

5.10. Способы скрытия сигналов в стандартных телефонных каналах. Достоинства и недостатки скремблеров. Принципы работы и особенности вокодеров. - ***ОПК-1; ПК-11; ПК-12***

5.11. Виды закладных устройств и способы их поиска. Состав и возможности автоматизированного комплекса радиомониторинга. Типы и принципы работы нелинейных локаторов. - ***ОПК-1; ПК-12***

5.12. Требования к экранам электромагнитных полей на низких и высоких частотах. Способы снижения излучений симметричных и несимметричных кабелей. Эффективность экранирования. - ***ОПК-1; ПК-3, ПК-12***

5.13. Средства, применяемые для видеонаблюдения в системах физической защиты. Принципы работы детектора движения. Способы увеличения видеозаписи изображений от телевизионных камер наблюдения. - ***ОПК-1; ПК-11; ПК-12***

5.14. Виды охранных и пожарных извещателей. Способы повышения помехоустойчивости акустических, оптико-электронных и радиоволновых извещателей. - ***ОПК-1; ПК-11; ПК-12***

5.15. Способы и средства нейтрализации угроз. Принципы нейтрализации угроз в автономных и централизованных системах охраны. Состав автоматизированного комплекса газового пожаротушения. - ***ОПК-1; ПК-11; ПК-12***

5.16. Факторы, вызывающие утечку информации по цепям электропитания и заземления. Меры по предотвращению этой утечки. - ***ОПК-1; ПК-11; ПК-12***

5.17. Основные этапы и показатели проектирования системы инженерно-технической защиты информации. Принципы оценки показателей. - ***ОПК-1; ПК-3, ПК-11; ПК-12***

5.18. Мероприятия по выявлению каналов утечки информации. Специальные проверки. Цель и способы проведения. - ***ОПК-1; ПК-3, ПК-11; ПК-12***

5.19. Мероприятия по выявлению каналов утечки информации. Специальные исследования в области защиты речевой информации, акустоэлектрических преобразований и ПЭМИН. - ***ОПК-1; ПК-3, ПК-11; ПК-12***

Раздел 6. Программно-аппаратная и криптографическая защита информации в компьютерных сетях – ***проверка сформированности компетенций - ОПК-3; ОПК-7; ПК-1; ПК-2; ПК-6; ПК-8***

6.1. Простейшие шифры. Шифры с симметричным и асимметричным ключом. Понятие стойкости криптографического алгоритма. - ***ОПК-3; ОПК-7; ПК-1***

6.2. Алгоритмы гаммирования, блочные шифры, ГОСТ 28147-89, DES. - ***ПК-1***

6.3. Стандарты электронной цифровой подписи 3410, 3411. - ***ПК-2; ПК-6***

6.4. Системы с открытым ключом. Алгоритм RSA. Инфраструктура систем с открытым ключом PKI. - ***ПК-1; ПК-2; ПК-6; ПК-8***

6.5. Разграничение доступа в операционных системах. - ***ОПК-3; ПК-1; ПК-2; ПК-6; ПК-8***

6.6. Штатные средства идентификации/ аутентификации в операционных системах. - ***ПК-1; ПК-2; ПК-6; ПК-8***

6.7. Межсетевые экраны. - ***ПК-1; ПК-2***

6.8. Требования руководящих документов ФСТЭК и ФСБ России - ***ПК-1; ПК-2; ПК-6; ПК-8***

2.2. Оценочные материалы для проведения государственного экзамена

2.2.1. Описание показателей, критериев и шкалы оценивания

Оценка	**Критерии оценки**
отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это в ходе государственного экзамена. Обучающийся исчерпывающе и логически стройно излагает материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Компетенции сформированы на уровне – «высокий».
хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его в ходе государственного экзамена, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Компетенции сформированы на уровне – «хороший».
удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении в ходе государственного экзамена. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Компетенции сформированы на уровне – «достаточный».
неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении в ходе государственного экзамена. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по

	дисциплине. Компетенции на уровне «достаточный» не сформированы.

2.2.2. Типовые контрольные задания или иные материалы

Перечень контрольных вопросов, необходимых для комплексного контроля сформированности компетенций приведён в подразделе 2.1. раздела 2 Программы государственного экзамена

2.2.3. Методические материалы, определяющие процедуры оценивания

Экзамен проводится в аудитории, которая заранее определяется графиком ГИА и готовится сотрудниками кафедры. В ней оборудуются места для членов государственной экзаменационной комиссии, секретаря комиссии и индивидуальные места для студентов.

Обеспечение ГЭК

В государственную экзаменационную комиссию по приёму государственного экзамена представляются следующие документы:

- приказ о составе комиссии,
- приказ о допуске студентов к ИГА,
- программа государственного экзамена,
- экзаменационные билеты,
- оформленные зачётные книжки студентов,
- чистая бумага со штампом для письменных ответов,
- ведомость сдачи государственного экзамена,
- бланки протоколов заседаний комиссии по приёму государственных экзаменов.

Общие положения по проведению экзамена

Экзамен проводится в устной форме. Для подготовки ответа студенту выделяется не менее 45 минут.

В случае обнаружения у выпускника после получения им экзаменационного билета учебных пособий, методических материалов, учебной и иной литературы (за исключением разрешённых для использования на государственном экзамене), конспектов, шпаргалок, независимо от типа носителя информации, а также любых технических средств и средств передачи информации, либо использования им подсказки, вне зависимости от того, были ли использованы указанные материалы и (или) средства в подготовке к ответу на государственном экзамене, комиссия изымает до окончания государственного экзамена указанные материалы и (или) средства с указанием соответствующих сведений в протоколе заседания ГЭК и принимает решение об оценке знаний такого выпускника «неудовлетворительно» либо о продолжении государственного экзамена (заслушивании ответа на экзаменационный билет).

При подготовке студентам рекомендуется делать краткие записи ответов на проштампованных листах. Письменные пометки делаются в произвольной форме. Это может быть развёрнутый план ответов, статистические данные, точные формулировки нормативных актов, схемы, позволяющие иллюстрировать ответ, и т.п. Записи, сделанные при подготовке к ответу, позволят студенту составить план ответа на вопросы, и, следовательно, полно, логично раскрыть их содержание. В то же время записи не должны быть слишком подробные. В них трудно ориентироваться при ответах, есть опасность упустить главные положения, излишней детализации несущественных аспектов вопроса, затянуть его. В итоге это может привести к снижению уровня ответа и повлиять на его оценку.

Последовательность проведения экзамена

Последовательность проведения экзамена можно представить в виде трёх этапов:

1. Начало экзамена.
2. Заслушивание ответов.

3. Подведение итогов экзамена.

1. Начало экзамена.

В день работы государственной экзаменационной комиссии по приёму государственного экзамена перед началом экзамена студенты - выпускники приглашаются в аудиторию, где Председатель комиссии:

− знакомит присутствующих и экзаменующихся с приказом о создании экзаменационной комиссии по приёму государственного экзамена, зачитывает его и представляет экзаменующимся состав комиссии;

− вскрывает конверт с экзаменационными билетами, проверяет их количество и раскладывает на специально выделенном для этого столе;

− даёт общие рекомендации экзаменующимся при подготовке ответов и устном изложении вопросов билета, а также при ответах на дополнительные вопросы;

− студенты учебной группы покидают аудиторию, а оставшиеся студенты в соответствии со списком очерёдности сдачи экзамена (как правило, первые пять человек) выбирают билеты, называют их номера и занимают свободные индивидуальные места за столами для подготовки ответов.

2. Заслушивание ответов.

Студенты, подготовившись к ответу, поочерёдно занимают место перед комиссией для сдачи экзамена. Для ответа каждому студенту отводится примерно 15 минут.

Возможны следующие варианты заслушивания ответов:

I вариант. Студент раскрывает содержание одного вопроса билета, и сразу ему предлагают ответить на уточняющие вопросы, затем по второму вопросу и так далее по всему билету.

II вариант. Студент отвечает на все вопросы билета, а затем дает ответы членам комиссии на уточняющие, поясняющие и дополняющие вопросы.

Как правило, дополнительные вопросы должны быть тесно связаны с основными вопросами билета.

Право выбора порядка ответа предоставляется экзаменующемуся студенту.

В обоих из этих вариантов комиссия, внимательно слушая экзаменующегося, предоставляет ему возможность дать полный ответ по всем вопросам.

В некоторых случаях, по инициативе председателя, его заместителей или членов комиссии (или в результате их согласованного решения), ответ студента может быть тактично приостановлен. При этом даётся краткое, но убедительное пояснение причины приостановки ответа: ответ явно не по существу вопроса, ответ слишком детализирован, экзаменующийся допускает ошибку в изложении и т.д. Другая причина - когда студент грамотно и полно изложит основное содержание вопроса, но продолжает его развивать. Если ответ остановлен по первой причине, то экзаменующемуся предлагают перестроить содержание излагаемой информации сразу же или после ответа на другие вопросы билета.

Ответивший студент сдаёт свои записи по билету, а билет секретарю комиссии.

По окончании ответов студентов под руководством Председателя ГЭК проводится закрытое заседание комиссии по обсуждению ответов и выставлению оценок. Одновременно формулируется общая оценка уровня теоретических и практических знаний экзаменующихся, выделяются наиболее грамотные компетентные ответы.

Оценки по каждому студенту заносятся в ведомость, протоколы и зачётные книжки, комиссия подписывает эти документы.

3. Подведение итогов сдачи экзамена.

Все студенты, сдававшие государственный экзамен, приглашаются в аудиторию, где Председатель комиссии подводит итоги сдачи государственного итогового экзамена: оглашает оценки, отмечает лучших студентов, высказывает общие замечания.

2.3. Учебно-методическое и информационное обеспечение государственного экзамена

Источники

основные

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/
2. Гражданский кодекс Российской Федерации. Часть первая, от 30.11.1994 N 51-ФЗ Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/
3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/
5. Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/
6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/
7. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/
8. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/
9. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/
10. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/
11. Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/
12. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/
13. Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/
14. Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/
15. Федеральный закон от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_36945/
16. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/
17. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время.

– Загл. с экрана.
18. Приказ ФСТЭК России от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экрана.
19. ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст), Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=447600#013921417480764586
20. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст), Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=418509#08480021357350149
21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М.: Стандартинформ, 2007. — 11 с. - Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9034#008124909983936601
22. Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации 05.12.2016 № 646) http://ivo.garant.ru/#/document/71556224/paragraph/1:1
23. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». Режим доступа : https://fstec.ru/component/attachments/download/148 свободный. – Загл. с экрана.
24. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утв. Решением Коллегии Гостехкомиссии России № 7.2/02.03.2001 г. Режим доступа : http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm свободный. – Загл. с экрана.
25. Типовое положение о подразделении по защите информации от иностранных технических разведок и от её утечки по техническим каналам на предприятии (в учреждении, организации), одоб. решением Гостехкомиссии России от 14 марта 1995 года № 32. Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?base=EXP&dst=100259&n=376976&req=doc#08515518016040791. – Загл. с экрана.
26. Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте (одобрено решением от 03.10.95 г. № 42 Гостехкомиссии России). Режим доступа : http http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=381868&dst=100536#08270169448516825. (Приложение № 12) – Загл. с экрана.
27. ПУЭ-76 «Правила устройства электроустановок» (утв. Минэнерго СССР) (6-ое издание) Режим доступа : https://base.garant.ru/3923095/. – Загл. с экрана.
28. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.
29. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный

ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

30. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
31. Руководящий документ. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.
32. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
33. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.

Литература

Основная

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2024. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/2131865
2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/2052391
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/
4. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578
5. Торокин А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. – М. :

6. Белов В.М., Новиков С.Н., Солонская О.И. Теория информации. Курс лекций. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012. – 143 с. URL: http://znanium.com/bookread2.php?book=364790.
7. Ореховская Н.А. Социальные коммуникации. М.: Альфа-М: ИНФРА-М, 2014. 224 с. - Режим доступа: http://znanium.com/bookread2.php?book=448967
8. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: http://znanium.com/catalog/product/1013794
9. Душин, В. К. Теоретические основы информационных процессов и систем [Электронный ресурс]: Учебник / В. К. Душин. - 5-е изд. - М.: Издательско-торговая корпорация «Дашков и К°», 2014. (Режим доступа: http://znanium.com/catalog.php?bookinfo=450784).
10. Ананьева Т.Н., Новикова Н.Г., Исаев Г.Н. Стандартизация, сертификация и управление качеством программного обеспечения: учеб. пособие [Электронный ресурс]: — М. : ИНФРА-М, 2017. — 232 с. (Режим доступа: http://znanium.com/catalog.php?bookinfo=792682).
11. Исаев Г.Н. Управление качеством информационных систем[Электронный ресурс]: - М.:НИЦ ИНФРА-М, 2016. - 248 с. (Режим доступа: http://znanium.com/catalog.php?bookinfo=543677).
12. Исаев Г.Н. Информационные технологии: учеб. Пособие - 2-е изд., стер. - Москва: Омега-Л, 2013. - 464 с.
13. Исаев Г.Н. Проектирование информационных систем: учеб. Пособие - Москва: Омега-Л, 2013. - 424 с.
14. Алгоритмизация и программирование**:** Учебное пособие / С.А. Канцедал. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с. (Режим доступа: http://znanium.com/catalog.php?bookinfo=429576).
15. Разработка и эксплуатация автоматизированных информационных систем: Учебное пособие / Л.Г. Гагарина. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 384 с.: (Режим доступа: http://www.znanium.com).
16. Илюшечкин, В. М. Операционные системы [Электронный ресурс]: учебное пособие / В. М. Илюшечкин. - 2-е изд. (эл.). -М.:: БИНОМ. Лаборатория знаний, 2012. - 111 с. (Режим доступа: http://www.znanium.com).
17. Основы компьютерных сетей: Учебное пособие / Б.Д.Виснадул, С.А.Лупин, С.В. Сидоров.; Под ред. Л.Г.Гагариной - М.: ИД ФОРУМ: НИЦ Инфра-М, 2012. - 272 с. (Режим доступа: http://www.znanium.com).

Дополнительная

1. Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль).
2. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578
3. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность).
4. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ.

безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность).

5. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. – Москва :Гор. линия-Телеком, 2015. – 586 с.: 60х90 1/16 (Обложка) ISBN 978-5-9912-0424-8 - Текст : электронный. - URL: https://new.znanium.com/catalog/product/895240
6. Техническая защита информации : лабораторный практикум : для студентов, обучающихся по направлению подготовки 090900.62 "Информационная безопасность" (программа подготовки бакалавра) / Гришина Наталия Васильевна, Гудов Геннадий Николаевич, Халяпин Дмитрий Борисович; Гришина Н. В., Гудов Г. Н., Халяпин Д. Б. ; Аккредитов. образоват. частное учреждение высш. образования "Моск. финансово-юрид. ун-т МФЮА", Каф. защиты информ. - Москва : МФЮА, 2015. - 113, [1] с. : рис., табл.
7. Баринов, В. А. Организационное проектирование: Учебник / Баринов В. А. - Москва : НИЦ ИНФРА-М, 2015. - 384 с. (Учебники для программы МВА) ISBN 978-5-16-010992-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/492911. – Режим доступа: по подписке..
8. Проектирование информационных систем [Электронный ресурс] : учебное пособие для бакалавриата по направлению подготовки 230700 - Прикладная информатика по профилям: Прикладная информатика в информационной сфере ; Прикладная информатика в экономике / Минобрнауки России, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информатики, Каф. информ. технологий ; [авт.: В. А. Лекае]. - Электрон. дан. - М. : РГГУ, 2013. - 360 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000008060. - ISBN 978-5-7281-1517-5. -С. 89-123.
9. Гусева Т.Ф. Практическое использование сервисов социальных сетей в учебном процессе // Инновационное развитие. - 2016. - № 5 (5). - С. 15-16.- Режим доступа: URL: https://elibrary.ru/download/elibrary_27722742_91152932.pdf
10. Сергеев А.Н., Пономарева Ю.С. Социальные сервисы и обучение: разработка учебных проектов в сети Интернет // Научный руководитель. - 2014. № 5 (6). - С. 43-52. - Режим доступа: URL: http: // https://elibrary.ru/download/elibrary_24328537_95444466.pdf
11. Галатенко В. А. Основы информационной безопасности : учеб. пособие : для студентов вузов, обучающихся по специальности 351400 "Прикладная информатика" / В. А. Галатенко; [под ред. В. Б. Бетелина]. - 4-е изд. - М. : Интернет-Ун-т информ. технологий : БИНОМ, Лаб. знаний, 2008. - 205 с. : рис., табл. - (Серия "Основы информационных технологий"). - Библиогр.: с. 200-205. - ISBN 978-5-94774-821-5
12. Кузнецов, И. Н. Диссертационные работы: методика подготовки и оформления : учебно-методическое пособие / И. Н. Кузнецов. — 4-е изд. — Москва : Издательско-торговая корпорация «Дашков и К°», 2014. — 488 с. - ISBN 978-5-394-01697-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093025 – Режим доступа: по подписке..
13. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие. - 2 ; доп. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2017. - 239 с. - ISBN 978-5-00091-007-8. -Режим доступа: https://new.znanium.com/catalog/document?id=343811.
14. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для студентов вузов, обучающихся по специальности 075400 - "Комплексная защита объектов информ." / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : рис.,табл. - Библиогр.: с.276-278 (51 назв.). - ISBN 5-935171-97.
15. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. — (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156– Режим доступа: по

подписке..
16. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 – Режим доступа: по подписке.
17. Тоискин, В. С. Системы документальной электросвязи : учебное пособие / В.С. Тоискин, А.П. Жук. — Москва : РИОР : ИНФРА-М, 2021. — 352 с. — (Высшее образование: Бакалавриат). — DOI: https://dx.doi.org/10.12737/5864. - ISBN 978-5-369-00609-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1072265
18. Гадзиковский, В. И. Цифровая обработка сигналов : учебное пособие / В. И. Гадзиковский. - Москва : СОЛОН-ПРЕСС, 2020. - 766 с. - ISBN 978-5-91359-117-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1858810 - Режим доступа: по подписке.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Журнал “Проблемы передачи информации” http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&wshow=contents&option_lang=rus
2. Журнал “Прикладная дискретная математика” http://journals.tsu.ru/pdm/&journal_page=archive.
3. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru
4. Система "Академик". - Режим доступа: URL: https://dic.academic.ru/dic.nsf/ruwiki/1334827
5. Государственная публичная научно-техническая библиотека России. - Режим доступа: URL: http://www.gpntb.ru
6. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru
7. Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru
8. Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru
9. Методологические проблемы наук об информации: http://inion.ru/seminars.mpni/.
10. Статьи по информатике и информационным технологиям из научных библиотек: http://www.scholar.ru/catalog.php?topic_id=14
11. Научная электронная библиотека: http://elibrary.ru/.
12. Сайт института проблем информатики РАН: http://www.ipiran.ru/.
13. Национальная электронная библиотека (НЭБ) www.rusneb.ru
14. ELibrary.ru Научная электронная библиотека www.elibrary.ru
15. Электронная библиотека Grebennikon.ru www.grebennikon.ru

3. Рекомендации по подготовке и оформлению ВКР

3.1. Общие требования к содержанию и оформлению ВКР

Итоговая государственная аттестация выпускников РГГУ по направлению 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр») включает в себя защиту выпускной квалификационной работы (ВКР) бакалавра. Защита выпускной квалификационной работы (ВКР) является обязательной формой государственной итоговой аттестации студентов, обучающихся по программе бакалавриата направления подготовки «Информационная безопасность».

Цель выполнения и защиты ВКР бакалавра – установление соответствия уровня профессиональной подготовки студентов требованиям ФГОС ВО.

Задачами выполнения и защиты ВКР бакалавров являются:

– систематизация, закрепление и расширение теоретических знаний по направлению «Информационная безопасность» и приобретение навыков практического применения этих

знаний при решении конкретных инженерных, научных и производственных задач;

– развитие умений студентов работать с литературой и интернет-источниками, находить необходимые источники информации, анализировать и систематизировать результаты информационного поиска;

– развитие навыков проведения самостоятельной работы, овладение методиками теоретических, экспериментальных и научно-практических исследований;

– приобретение опыта систематизации результатов исследований, анализа и оптимизации проектных решений, формулировки выводов и положений выполненной работы и приобретение опыта их публичной защиты.

В соответствии с ФГОС, объектами профессиональной деятельности бакалавров направления «Информационная безопасность», и, соответственно, объектами ВКР должны являться:

- объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
- процессы управления информационной безопасностью защищаемых объектов.

Тематическая направленность, основная цель ВКР, и решаемые в ней задачи также должны соответствовать требованиям стандарта, то есть перечисленным в нем областям и видам профессиональной деятельности и продемонстрировать степень овладения выпускником по этим видам деятельности соответствующих профессиональных компетенций, содержащихся как во ФГОС, так и в разработанной вузом основной образовательной программе (ООП). Представленная к защите ВКР, а также сам процесс ее защиты должны продемонстрировать членам ГЭК знания, умения и навыки, полученные бакалавром за весь период обучения в процессе реализации ООП. Ниже приведён обобщённый список знаний, умений и навыков, которым следует руководствоваться при оценке качества защиты и выполнения ВКР и уровня усвоения бакалавром содержания дисциплин рабочего учебного плана.

Бакалавр по направлению «Информационная безопасность» должен **знать:**

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;
- современные средства разработки и анализа программного обеспечения на языках высокого уровня;
- аппаратные средства вычислительной техники;
- операционные системы персональных ЭВМ;
- основы администрирования вычислительных сетей;
- системы управления базами данных;
- принципы построения информационных систем;
- структуру систем документационного обеспечения;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы 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;

- принципы и методы организационной защиты информации;
- 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;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;
- сигналы электросвязи, принципы построения систем и средств связи;
- методы анализа электрических цепей;
- принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;
- основы схемотехники;

Бакалавр по направлению «Информационная безопасность» должен **уметь:**

- выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;
- составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;
- формулировать и настраивать политику безопасности распространённых операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищённости компьютерных систем;
- пользоваться нормативными документами по защите информации;
- применять на практике методы анализа электрических цепей;

Бакалавр по направлению «Информационная безопасность» должен **владеть:**

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- навыками выявления и уничтожения компьютерных вирусов;
- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- навыками организации и обеспечения режима секретности;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- навыками чтения электронных схем;
- методами анализа и формализации информационных процессов объекта и связей между ними;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методиками проверки защищённости объектов информатизации на соответствие требованиям нормативных документов;
- профессиональной терминологией;

- навыками безопасного использования технических средств в профессиональной деятельности.

Общие требования к содержанию и оформлению ВКР

Темы выпускных работ бакалавров разрабатываются кафедрой «Информационной безопасности» ежегодно обновляются с учётом заявок представителей предприятий (организаций, учреждений), на базе которых студенты работают и (или) проходят производственную практику, а также с учётом практических и (или) научных интересов обучающихся, включая их участие в научно-исследовательских работах.

Время, отводимое на подготовку квалификационной работы в соответствии с рабочим учебным планом, составляет 6 недель. С целью повышения качества ВКР студент должен определиться с ее тематикой на четвёртом курсе в рамках дисциплины «Основы научных исследований».

Выпускная квалификационная работа должна иметь внутреннее единство и завершённость, отражать ход и результаты разработки выбранной темы, соответствовать современному уровню развития науки и техники, а ее тема должна быть актуальной.

Выпускная работа бакалавра может быть связана с разработкой конкретных теоретических вопросов, являющихся частью научно-исследовательских работ, выполняемых кафедрой, с экспериментальными исследованиями или с решением прикладных задач (проектированием машин и оборудования, разработкой технологических процессов и т.д.), актуальных для кафедры или конкретных предприятий или организаций.

Выпускная работа бакалавра выполняется каждым студентом самостоятельно единолично или в составе коллектива научной лаборатории, отдела, группы, тематика работы которого включает в себя тему выпускной работы студента. В последнем случае в выпускной работе обязательно должен быть отражён личный вклад автора в результаты коллективной работы.

Не обязательно, чтобы ВКР включала в себя сразу все объекты и виды профессиональной деятельности.

В качестве основы выпускных работ могут браться курсовые работы и проекты, выполненные в соответствии с учебным планом, базирующиеся на материале основных дисциплин общепрофессионального цикла и специальных дисциплин образовательного стандарта направления, дополненные специальными разделами, расширяющими круг вопросов, рассматриваемых в работе.

По решению кафедры в качестве выпускной работы в порядке исключения могут быть приняты статьи, опубликованные или подготовленные только студентом, а также научные доклады, представленные на студенческих конференциях, конференциях молодых учёных и т.д.

Также как исключение в качестве выпускных работ могут рассматриваться работы, имеющие реферативный характер, однако, содержание такой работы должно включать обобщения и новые выводы, разработанные непосредственно автором.

Руководство выпускными работами осуществляется либо преподавателями и научными сотрудниками кафедры, имеющими учёную степень или занимаемую должность не ниже старшего преподавателя, либо специалистами-работодателями в области информационной безопасности. В случае необходимости, кафедре предоставляется право приглашать в качестве руководителей сотрудников других кафедр университета, ведущих специалистов и высококвалифицированных работников предприятий, научно-исследовательских и проектных институтов и других организаций, давших предварительное согласие на руководство. Для обеспечения возможности прохождения педагогической практики магистрантами и аспирантами допускается их привлечение в качестве соруководителей ВКР, если ее тематика близка или совпадает с тематикой будущей магистерской или кандидатской диссертации аспиранта (магистранта). Вопрос о назначении руководителей выпускных работ и утверждении их тем обсуждается на кафедре и контролируется руководством ВУЗа по

представлению кафедры и деканата. При этом, тема ВКР и руководитель закрепляется за студентом приказом ректора.

Выполнение ВКР является заключительным этапом обучения студентов в ВУЗе и имеет своими целями:

– систематизацию и расширение теоретических и практических знаний по направлению подготовки, применение этих знаний при решении конкретных научных, технических, организационных или правовых задач и вопросов;

– закрепление навыков ведения самостоятельной проектной работы, овладение методиками научных исследований и экспериментов при решении разрабатываемых в выпускной квалификационной работе проблем и вопросов;

– выявление степени подготовленности студента к практической работе по направлению подготовки.

Выпускная квалификационная работа должна свидетельствовать об умении студента:

– чётко формулировать тему исследования, определять степень актуальности и разработанности поставленной темы на современном этапе;

– собирать и анализировать исходные факты и материалы;

– разрабатывать (выбирать) методику исследования и проводить на ее основе самостоятельное исследование;

– делать обоснованные выводы, формулировать научные результаты и практические рекомендации по проделанной работе;

– грамотно и доказательно излагать свои мысли и результаты исследования;

– правильно оформлять пояснительную записку.

Перечень тем ВКР обучающихся ежегодно обновляется и утверждается Советом ИИНТБ не позднее 1 сентября.

Студенту предоставляется право выбора темы выпускной квалификационной работы. Студент может предложить для выпускной квалификационной работы тему, не вошедшую в рекомендуемую тематику, с обоснованием целесообразности ее разработки.

Выбор темы выпускной квалификационной работы осуществляется путём подачи студентом письменного заявления на выпускающую кафедру.

В заявлении указываются предполагаемая тема выпускной квалификационной работы и предполагаемый научный руководитель.

Заявления студентов рассматриваются на заседании кафедры. Студенту предоставляется право присутствия на заседании кафедры при рассмотрении его заявления. По каждому заявлению кафедра утверждает тему выпускной квалификационной работы и назначает научного руководителя из числа профессоров, доцентов или старших преподавателей кафедры.

При утверждении темы выпускной квалификационной работы учитываются:
актуальность проблемы, степень ее разработанности, наличие у студента опыта работы по направлению подготовки, участие в научно-исследовательской работе и его успеваемость.

В течение одной недели после утверждения темы выпускной квалификационной работы, студент совместно с научным руководителем составляет календарный план выполнения и задание на выполнение выпускной квалификационной работы.

В зависимости от характера темы, наименования и количество этапов в календарном плане могут быть изменены. Календарный план и задание утверждается научным руководителем до начала подготовки выпускной квалификационной работы. По окончании выполнения каждого этапа студент предоставляет научному руководителю указанные в графике письменные отчётные материалы. Научный руководитель отчитывается на заседаниях кафедры о ходе подготовки и написания студентом выпускной квалификационной работы.

По каждой ВКР кафедрой назначается рецензент из числа профессорско-преподавательского состава кафедры.

Закрепление за обучающимися тем ВКР, назначение руководителей и рецензентов осуществляется приказом ректора.

ВКР выпускника по направлению подготовки «Прикладная информатика» может представлять собой:

– научно-практическую разработку в прикладной области (в информационной сфере, экономике) на примере конкретных объектов или бизнес-процессов конкретного учреждения;

– проектную разработку части конкретной информационной системы.

В ВКР, представляющей собой научно-практическую разработку, должны быть подробно изложены аналитическая и практическая части. Каждое проектное предложение должно содержать научное обоснование необходимости и эффективности его внедрения и методику внедрения. Технико-экономическое обоснование принятых решений с количественной оценкой результатов включается в состав ВКР в том случае, если имеется апробированная методика таких расчётов.

ВКР как разработка проекта части конкретной информационной системы должна содержать подробную проектную документацию (техническое задание на ИС, документацию и спецификацию выбранных аппаратно-программных средств, технико-экономическое обоснование проектных решений), выполненную в соответствии с ГОСТ на проектную документацию.

За все сведения, изложенные в ВКР, порядок их использования при составлении фактического материала и другой информации, обоснованность и достоверность выводов и защищаемых положений, профессиональную, нравственную и юридическую ответственность несёт непосредственно автор выпускной работы, в соответствии с действующими в Российской Федерации и в РГГУ правовыми и/или локальными нормативными актами.

Основные задачи выпускной квалификационной работы:

– развитие навыков самостоятельной работы при решении проблем профессионального характера;

– развитие умения критически оценивать и обобщать теоретические положения;

– презентация навыков публичного доклада и защиты результатов работы, предложений и рекомендаций;

– выявление соответствия подготовленности выпускника к выполнению требований, предъявляемых ФГОС.

Выпускная квалификационная работа выполняется в форме бакалаврской работы, включающей текстовые документы, представляемые в бумажном и электронном виде и презентацию в электронном виде.

К текстовым документам относятся: задание на ВКР, пояснительная записка, отзыв руководителя, отчёт о поверке на наличие заимствований, документы, подтверждающие использование разработок студента на предприятии (при наличии).

В презентацию включаются тема, цель и задачи ВКР, графические материалы в виде чертежей, схем, диаграмм, таблиц, формул, фотографий и других форм иллюстрационных материалов, заключение.

Бакалаврская работа включает следующие разделы:

- титульный лист,
- реферат,
- содержание (оглавление),
- список использованных сокращений,
- введение,
- основные разделы,
- заключение,
- список используемой литературы,
- приложения.

Общий объем выпускной квалификационной работы – 45…60 страниц.

3.2. Оценочные материалы для ВКР

3.2.1. Описание показателей, критериев и шкалы оценивания

Оценка	**Критерии оценки**
отлично	Оценка «отлично» выставляется, если тема ВКР раскрыта, цель и задачи чётко сформулированы и реализованы. Автор использует современные аналитические и методологические инструментарии. Работа содержит фрагменты научного исследования и характеризуется высоким качеством и глубиной теоретико-методологического анализа, критического обзора литературных источников, наличием научной проблематики. Обобщения и выводы базируются на качественно обработанной статистической информационной базе. Авторская позиция аргументирована, представленные рекомендации имеют практическую ценность. Отзыв и рецензия положительны. Доклад содержателен, проиллюстрирован наглядными материалами, отражает результаты исследования и высокий уровень теоретической и профессиональной подготовки выпускника. Ответы на вопросы членов ГЭК полные и правильные.
хорошо	Оценка «хорошо» выставляется, если тема в ВКР раскрыта, теоретические обобщения и выводы в основном правильные, но присутствуют отдельные недостатки непринципиального характера: поверхностно сделан анализ литературных источников, недостаточно использованы материалы субъекта исследования, использование современного аналитического инструментария ограничено, представленные в работе предложения автора не содержат аналитического обоснования экономической целесообразности их реализации. Отзыв и рецензия положительны, но имеют отдельные замечания. Доклад логичен, проиллюстрирован наглядными материалами, в целом отражает результаты исследования и достаточный уровень теоретической и профессиональной подготовки выпускника. Ответы на вопросы членов ГЭК правильные, но не всегда полные или корректные.
удовлетворительно	Оценка «удовлетворительно» выставляется, если тема работы в основном раскрыта, но имеются недостатки содержательного характера: нечётко сформулирована цель и задачи, теоретический раздел носит компилятивный характер, отсутствует научная полемика, предложения недостаточно обоснованы, есть замечания к логике и последовательности изложения материала, который носит преимущественно описательный характер. Работа оформлена небрежно. Отзыв и рецензия положительны, но имеют замечания. Доклад отражает основные результаты работы и достаточный уровень теоретической и профессиональной подготовки выпускника. Не все ответы на вопросы членов ГЭК полные или правильные
неудовлетворительно	Оценка «неудовлетворительно» выставляется, если в работе отсутствует понимание цели, задач и предмета исследования. Разделы не связаны между собой, названия отдельных разделов не отвечает их содержанию. Теоретический анализ и оценка состояния объекта исследования носят описательный характер.

	Предложения и рекомендации непоследовательны, их экономическое обоснование неполное или отсутствует. Представленный статистический материал устарел. Оформление работы имеет существенные недостатки. Доклад не отражает содержания выполненной работы. Наглядные материалы носят случайный характер или отсутствуют. Большинство ответов на вопросы не правильные, студент не владеет предметом исследования.

3.2.2. Примерная тематика ВКР

1. Разработка организационно-технических рекомендаций по повышению эффективности защиты конфиденциальной информации предприятия (на конкретном примере).

2. Разработка организационно-технических мер по защите информации, составляющей служебную тайну, предприятия (на конкретном примере).

3. Разработка предложений по созданию системы защиты информации предприятия централизованной структуры.

4. Разработка предложений по созданию защищенной информационной системы предприятия децентрализованной структуры.

5. Обоснование решений по определению способов оценки угроз информационной безопасности предприятия (на конкретном примере).

6. Разработка организационно-технических мер защиты выделенного помещения предприятия (на конкретном примере).

7. Разработка рекомендаций руководителю предприятия по оборудованию помещения для проведения служебных совещаний (на конкретном примере).

8. Разработка рекомендаций руководителю предприятия по оборудованию помещения для обработки персональных данных (на конкретном примере).

9. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия (на конкретном примере).

10. Разработка модели комплексной системы защиты информации предприятия (на конкретном примере).

11. Оценка рисков и управление информационной безопасностью предприятия (на конкретном примере).

12. Разработка автоматизированной системы оценки информационных рисков предприятия (на конкретном примере).

13. Организация комплексной системы защиты конфиденциальной информации предприятия (на конкретном примере).

14. Разработка политики информационной безопасности на основе анализа информационных рисков предприятия (на конкретном примере).

15. Совершенствование нормативно-методической базы защиты конфиденциальной информации предприятия (на конкретном примере).

16. Разработка организационно-технических мер противодействия утечке информации по техническим каналам предприятия (на конкретном примере).

17. Разработка рекомендаций по совершенствованию защиты коммерческой тайны предприятия (на конкретном примере).

18. Разработка рекомендаций по совершенствованию защиты ресурсов автоматизированной системы предприятия (на конкретном примере).

19. Оценка эффективности системы защиты информации предприятия (на конкретном примере).

20. Разработка рекомендаций по проведению аудита информационной безопасности предприятия (на конкретном примере).

21. Разработка рекомендаций по использованию зарубежного опыта (на примере конкретной страны или ряда стран) при организации защиты конфиденциальной информации.

22. Организация информационно-аналитической деятельности по обеспечению информационной безопасности предприятия (на конкретном примере).

23. Формирование информационно-аналитического обеспечения для работы руководителя подразделения защиты информации предприятия (на конкретном примере).

24. Разработка направлений совершенствования и регламентации доступа персонала к конфиденциальной информации, документам и продукции предприятия (на конкретном примере).

25. Разработка нормативно-методических документов по регламентации организационной защиты информации, обрабатываемой средствами вычислительной и организационной техники предприятия (на конкретном примере).

26. Разработка направлений и способов контроля надежности и эффективности организационной зашиты информации предприятия (на конкретном примере).

27. Разработка направлений, методов и нормативно-методических документов по защите информации в рекламной, выставочной и издательской деятельности предприятия (на конкретном примере).

28. Разработка направлений, методов и нормативно-методических документов по организационной защите продукции при ее производстве, транспортировки и хранении предприятия (на конкретном примере).

29. Разработка направлений, методов и нормативно-методических документов по организационной защите персональных данных предприятия (на конкретном примере).

30. Разработка предложений по реализации на предприятии комплекса мер противодействия утечки информации по скрытым информационным каналам.

32. Разработка направлений, методов и нормативно-методического обеспечения работы с персоналом, обладающих конфиденциальной информацией.

33. Разработка и регламентация технологии хранения и использования конфиденциальных документов в архивах (на конкретном примере).

34. Разработка и регламентация организационной защиты информации при проведении научно-исследовательских и опытно-конструкторских работ (на конкретном примере).

35. Организация защиты конфиденциальной информации при разработке инновационных проектов (на конкретном примере).

36. Организация защиты конфиденциальной информации корпоративными пользователями систем интернет-банкинга (на конкретном примере).

37. Организация защиты конфиденциальной информации корпоративными пользователями систем удаленного доступа (на конкретном примере).

38. Разработка системы защиты персональных данных предприятия (на конкретном примере).

39. Организация системы защиты электронного документооборота предприятия (на конкретном примере).

40. Организация защищенного документооборота предприятия (на конкретном примере).

41. «Разработка рекомендаций по совершенствованию организации и управления службой защиты информации предприятия (на конкретном примере)».

41. Разработка организационно-технических рекомендаций по совершенствованию защиты конфиденциальной информации предприятия (на конкретном примере).

42. Разработка предложений по совершенствованию управления системой защиты информации предприятия (на конкретном примере).

3.2.3. Методические материалы, определяющие процедуры оценивания

1) Результат работы. Представляет собой овеществлённую реализацию какого-либо проекта или его части, например, работающую программу, программно-аппаратный комплекс или устройство, дидактические материалы, методики или технологии, результаты исследований, технические или рабочие проекты, оформленные соответствующими документами (например, в виде инструкций, чертежей или собственно проектов), отдельные из которых (например, чертежи и схемы) могут составлять графическую часть ВКР.

Приветствуется, если ВКР включает в себя элементы научных исследований. Результатом таких исследований могут быть разработанные алгоритмы, модели, данные анализа, разработанная методика расчёта, данные экспериментальных исследований и выявленные в них закономерности и др. Полученные алгоритмы и модели могут быть апробированы как в программной системе собственной разработки, так и в программных инструментальных системах сторонних разработчиков. При этом крайне важно экспериментально подтвердить полученные результаты.

Если правообладателем результата ВКР или его заказчиком является не вуз, а сторонняя организация или предприятие, причём этот результат не может быть по каким-либо причинам транспортирован в вуз для его демонстрации, выпускник может либо пригласить представителей кафедры на место нахождения результата, либо предоставить в вуз иные доказательства его наличия. Например, это могут быть справки о внедрении, акты внедрения и испытания, видеозаписи и фотографии. В любом случае, результаты ВКР всегда должны быть ориентированы под конкретного заказчика, а ещё лучше, если они будут к моменту защиты уже реально внедрены и использоваться в производственной деятельности у этого заказчика.

2) Пояснительная записка (ПЗ). Общий объем пояснительной записки рекомендуется в пределах 40 - 60 страниц формата А4 (Шрифт Times New Roman, 14, через полтора интервала). При определении объёма записки не учитывается объем приложений. В ПЗ на основании обзора существующих аналогов проводится анализ состояния дел в предметной области для выбранного объекта, формулируются задачи и цель ВКР, и далее, в зависимости от типа ВКР, описывается процесс решения поставленных задач, и достигнутые результаты. Оформление ПЗ выполняется в соответствии с требованиями и рекомендаций по выполнению выпускных квалификационных работ бакалавров по направлению 10.03.01 «Информационная безопасность», размещённых на сайте ИИНТБ РГГУ.

3) Демонстрационные материалы, используемые при выступлении с докладом при защите ВКР на ГЭК.

4) Электронная версия ПЗ, презентации и иных демонстрационных материалов при их наличии и возможности представления в электронном виде (фильмы, отдельные фотографии, чертежи, схемы и т.п. Прилагается к ПЗ на CD – диске. Если ВКР посвящена разработке программного обеспечения (ПО), электронная версия должна содержать полный набор компонентов ПО, необходимый для воспроизведения программы, включая исходный текст, исполняемые модули и библиотеки, набор драйверов, утилит, библиотек API и фреймворков,

инструментальных сред разработки. Исключение составляют проприетарные среды, являющиеся собственностью заказчика ВКР, а также универсальные среды широкого применения, лицензия на которые имеется в вузе.

Все листы пояснительной записки должны быть сброшюрованы в папку формата А4 или потребительского формата, близкого к формату А4. На папке должна быть наклеена этикетка (60х100 мм) с указанием аббревиатуры университета (РГГУ), вида документа (выпускная работа бакалавра), кода учебной группы и направления подготовки, автора работы и года окончания выполнения. Этикетка выполняется машинописным способом.

Защита выпускных работ бакалавров

Решение о допуске ВКР к защите принимается комиссией во время предварительной защиты. Цель предзащиты – оценка завершённости ВКР, качества ее выполнения и оформления, соответствия требованиям ФГОС и выпускающей кафедры, наличия реально полученных результатов, а также оценки готовности самого студента к защите.

Предзащиту ВКР выпускающая кафедра проводит во второй половине июня, но не позднее, чем за 10 дней до защиты. Для этого составляется график заседания комиссий по проведению предзащит. При разработке графика для установления очерёдности может учитываться степень готовых к защите работ на основании сведений, поступающих от руководителей. На каждом заседании комиссии по предзащите должно присутствовать не менее двух членов комиссии из числа ведущих преподавателей выпускающей кафедры. Желательно (но не обязательно), чтобы на предзащите присутствовал и руководитель ВКР. Предзащита состоит из двух этапов: демонстрации реально полученных бакалавром результатов (работающий программный продукт, устройство или программно-технический комплекс, разработанный проект или результаты моделирования, экспериментальных или теоретических исследований) и оценки степени готовности к защите ПЗ, презентации, иных материалов и самого выпускника.

Для предварительной защиты студент должен подготовить:

- результаты своей деятельности для демонстрации их комиссии;
- полностью оформленную пояснительную записку в несброшюрованном виде;
- согласованные с руководителем доклад и презентацию.

Конкретный вид предоставляемых для демонстрации практической реализации сведений и материалов зависит от тематической направленности ВКР и характера полученного в ходе ее выполнения результата.

На основании просмотренной записки, сделанного студентом доклада, презентации, качества ответов на заданные вопросы, и оценки продемонстрированных результатов, полученных в ходе проведения ВКР, комиссия принимает решение о допуске к защите или необходимости повторения процедуры предзащиты, если устранить замечания в срок представляется возможным.

Защита выпускных работ выполняется после завершения 6 недель, отведённых на их выполнение, написание пояснительной записки и предзащиты. Конкретные сроки работы ГЭК устанавливаются в соответствии с учебным планом. Расписание работы каждой комиссии составляется из расчёта не более 12 защит в один день, утверждается на уровне вуза по представлению кафедры и доводится до общего сведения не позднее, чем за неделю до начала защиты выпускных работ.

К защите допускаются студенты, успешно завершившие полный курс обучения по направлению подготовки и представившие выпускную работу с отзывом руководителя в установленный срок. Допуск к защите выпускных работ оформляется распоряжением по факультету не позднее, чем за неделю до защиты.

Руководитель ВКР представляет письменный отзыв, который должен содержать оценку:

– соответствия результатов ВКР поставленным целям и задачам;

–правильности и самостоятельности принимаемых студентом решений;

– умения автора работать с научной, методической, справочной литературой и электронными информационными ресурсами;

– степени сформированности профессиональных компетенций у студента;

– личных качеств студента, проявившихся в процессе работы над ВКР.

Заканчивается письменный отзыв руководителя формулировкой рекомендации к защите.

Защита выпускных работ проводится на открытых заседаниях государственной экзаменационной комиссии с участием не менее 2/3 ее состава и не менее трёх человек. Присутствие на заседании председателя или его заместителя является обязательным. Заседания ГЭК протекают в следующем порядке.

В начале заседания председатель ГЭК объявляет о начале защит и предоставляет слово секретарю. Секретарь оглашает название, автора и руководителя ВКР, место ее выполнения, после чего предоставляет слово выпускнику для доклада. По окончании доклада председатель предлагает сначала членам ГЭК, а затем и всем присутствующим задать вопросы студенту. После окончания ответов на вопросы секретарь ГЭК зачитывает перечень дополнительных документов, представленных на защиту (например, акты о внедрении, дипломы, грамоты, свидетельства об участии в выставках и конкурсах, и т.п.) и отзыв руководителя. Далее председатель даёт возможность докладчику ответить на замечания при их наличии, предоставляя ему заключительное слово. После заключительного слова высказать своё мнение о работе могут все присутствующие на защите. Если у присутствующих не появилось вопросов, и нет желающих высказать своё мнение о работе, председатель объявляет окончание защиты, и начинается процедура защиты очередной работы. По итогам каждой защиты каждый член ГЭК проставляет оценку ВКР в баллах и заносит ее в оценочный лист. После последней защиты объявляется закрытое совещание ГЭК, на котором членами ГЭК обсуждаются результаты защит, подводятся общие итоги работы комиссии. По каждой работе выводится ее средний рейтинг, даётся итоговая оценка и принимается решение о присвоении выпускнику квалификации «бакалавр» по соответствующему направлению и выдаче ему документа установленного образца о базовом высшем образовании. Выпускникам, защитившим ВКР на «отлично» и получившим за время обучения в университете оценки только «отлично» и «хорошо», причём количество оценок «хорошо» не должно быть больше 25%, выдаются дипломы с отличием. По окончании закрытого заседания выпускники приглашаются в аудиторию, и председатель ГЭК объявляет результаты защиты.

По итогам заседаний для каждой защиты оформляется специальный протокол, в котором отмечаются вопросы, заданные выпускнику, даётся оценка выполнения работы и ее защиты, отмечается практическая и научная ценность работы и фиксируются принятые по итогам защиты дополнительные решения и рекомендации о необходимости продолжении образования, направления работы на конкурсы, доведения сведений о ней заинтересованным организациям, использовании в учебном процессе или ином внедрении. Здесь же регистрируется запись о присуждении квалификации и определение степени диплома (например, с отличием). рекомендации по продолжению выполнения и необходимости ее внедрения.

Студенты, не защитившие выпускную работу, нарушившие сроки представления выпускных работ на защиту, а также не явившиеся на защиту без уважительной причины или получившие оценку "неудовлетворительно" отчисляются из университета за неуспеваемость, получают академическую справку установленного образца и отчисляются из университета с правом повторной защиты выпускной работы в течение трёх лет. Вопрос о теме и задании повторно защищаемых работ решает профилирующая кафедра.

Студентам, не явившимся на заседание ГЭК по уважительной причине, ректором университета может быть предоставлена возможность защиты работы в дополнительные сроки работы комиссии. Студентам, не завершившим выпускную работу в установленный срок по уважительной причине, ректором может быть продлён срок обучения на выпускном

(четвёртом) курсе до следующего периода работы экзаменационной комиссии, но не более, чем на один год.

Выпускные работы хранятся на кафедре в течение 5 лет. Ответственность за хранение ВКР и порядок их использования в учебном процессе возлагается на заведующего кафедрой.

По истечении нормативного срока хранения ВКР подлежат уничтожению в установленном порядке.

4. Материально-техническое обеспечение государственной итоговой аттестации

Для материально-технического обеспечения государственной итоговой аттестации используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

5. Особенности проведения государственной итоговой аттестации для обучающихся из числа лиц с ограниченными возможностями здоровья

Процедуры проведения ГИА для обучающихся с ограниченными возможностями здоровья регламентируются действующим Положением о проведении государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры.