ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Направление подготовки (специальность): 10.05.03 - Информационная безопасность автоматизированных систем

Профиль подготовки (специализация): Информационная **б**езопасность автоматизированных систем критически важных объектов

Квалификация (степень) выпускника специалист

СОДЕРЖАНИЕ

1. Перечень компетенций, которыми должен овладеть обучающийся в результате освоения образовательной программы.

В соответствии с целями и видами профессиональной деятельности основной профессиональной образовательной программы в результате освоения выпускниками должны овладеть следующими компетенциями:

Таблица 1.

Код компетенции	Содержание компетенции	Виды профессиональной деятельности
ОК-1	способностью использовать основы философских знаний для формирования мировоззренческой позиции	научно-исследовательская; проектно-производственная;
ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности	научно-исследовательская; проектно-производственная
ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	научно-исследовательская; проектно-производственная
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	научно-исследовательская; проектно-производственная
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	научно-исследовательская; проектно-производственная
ОК-6	способностью работать в коллективе ,толерантно воспринимая социальные, культурные и иные различия	научно-исследовательская; проектно-производственная
ОК-7	способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	научно-исследовательская; проектно-производственная
ОК-8	способностью к самоорганизации и самообразованию	научно-исследовательская; проектно-производственная
ОК-9	способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности	научно-исследовательская; проектно-производственная
ОПК-1	способностью анализировать физические явления и процессы, применять	научно-исследовательская;

	соответствующий математический аппарат для формализации и решения профессиональных задач	проектно-производственная
ОПК-2	способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	научно-исследовательская; проектно-производственная
ОПК-3	способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	научно-исследовательская; проектно-производственная
ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	научно-исследовательская; проектно-производственная
ОПК-5	способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	научно-исследовательская; проектно-производственная
ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности	научно-исследовательская; проектно-производственная
ОПК-7	способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	научно-исследовательская; проектно-производственная
ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий	научно-исследовательская; проектно-производственная
ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	научно-исследовательская; проектно-производственная
ПК-2	способностью создавать и исследовать модели автоматизированных систем	научно-исследовательская; проектно-производственная
ПК-3	способностью проводить анализ защищенности автоматизированных систем	научно-исследовательская; проектно-производственная
ПК-4	способностью разрабатывать модели угроз и модели нарушителя	научно-исследовательская;

	информационной безопасности автоматизированной системы	проектно-производственная
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	научно-исследовательская; проектно-производственная
ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	научно-исследовательская; проектно-производственная
ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	научно-исследовательская; проектно-производственная
ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	научно-исследовательская; проектно-производственная
ПК-10	способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	научно-исследовательская; проектно-производственная
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	научно-исследовательская; проектно-производственная
ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	научно-исследовательская; проектно-производственная
ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом	научно-исследовательская; проектно-производственная

	нормативных документов по защите информации	
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	научно-исследовательская; проектно-производственная
ПК-18	способностью организовать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	научно-исследовательская; проектно-производственная
ПК-19	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	научно-исследовательская; проектно-производственная
ПК-2	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	научно-исследовательская; проектно-производственная
ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	научно-исследовательская; проектно-производственная
ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	научно-исследовательская; проектно-производственная
ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	научно-исследовательская; проектно-производственная
ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	научно-исследовательская; проектно-производственная
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	научно-исследовательская; проектно-производственная
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит	научно-исследовательская; проектно-производственная

	безопасности автоматизированной системы	
ПК-28	способностью управлять информационной безопасностью автоматизированной системы	научно-исследовательская; проектно-производственная
ПСК-3.1	способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	научно-исследовательская; проектно-производственная
ПСК-3.2	способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	научно-исследовательская; проектно-производственная
ПСК-3.3	способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	научно-исследовательская; проектно-производственная
ПСК-3.4	способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	научно-исследовательская; проектно-производственная
ПСК-3.5	способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	научно-исследовательская; проектно-производственная

2. Показатели и критерии оценивания компетенций.

В ходе государственной итоговой аттестации оценивается сформированность компетенций, которыми должны овладеть обучающиеся в результате освоения основной профессиональной образовательной программы.

Таблица 2.

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ОК-1	способность использовать основы философских знаний для формирования мировоззренческой позиции	**Знать:** 1 этап: основные исторические периоды развития философии, представителей, особенности их взглядов, 2 этап - теоретические основы философии. **Уметь:** 1 этап – на основе опыта философских исследований прошлого уметь исследовать основные проблемы человека, общества, мира 2 этап – философски исследовать и анализировать проблемы, связанные, с областью будущей жизни и профессиональной деятельностью **Владеть:** 1 этап - владеть базовыми принципами философского познания 2 этап – владеть основными приёмами, методами и формами философского познания	*ответы на билет государственного экзамена и выполнение выпускной квалификационной работы*
ОК-2	Способность использовать основы экономических знаний в различных сферах деятельности	**Знать:** 1 этап: основы экономики; 2 этап: основные принципы и направления применения экономических знаний **Уметь:** 1 этап: применять экономические знания в различных сферах	

		деятельности; 2 этап: работать в различных сферах деятельности, используя экономические знания **Владеть:** 1 этап: навыками использования полученных экономических знаний; 2 этап: навыками использования основ экономических знаний в различных сферах деятельности	
ОК-3	способность анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	**Знать:** Этап 1: знать основные исторические события России и мира с древних времен до конца XIX в. Этап 2: знать узловые проблемы истории России и мира в XX в. **Уметь:** Этап 1: уметь собирать информацию из различных источников Этап 2: уметь критически оценивать и анализировать собранную информацию **Владеть:** Этап 1: навыки обобщения, анализа, восприятия информации, постановки цели и выбора путей её достижения Этап 2: навыки понимания и свободного воспроизведения основных исторических событий	
ОК-4	способностью использовать основы	**Знать:** Этап 1. Знать источники получения	

	правовых знаний в различных сферах деятельности	информации о нормативно-правовых документах Этап 2. Знать содержания нормативно-правовых актов. **Уметь:** Этап 1. Ориентироваться в системе законодательства и нормативных правовых актов Этап 2. Использовать правовые нормы в различных сферах деятельности **Владеть:** Этап 1. Владеть навыками подготовки публичной речи. Этап 2. Владеть навыками произнесения публичной речи, аргументации и ведения дискуссии	
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества/ государства, соблюдать нормы профессиональной этики	**Знать:** Этап 1: - основные этапы развития этической мысли; Этап 2: - принципы и правила профессиональных отношений и профессионального поведения. **Уметь:** Этап 1: - использовать полученные знания в конкретных ситуациях морального выбора в профессиональной (служебной) практике; Этап 2: - применять принципы теоретического анализа общечеловеческих норм этики к практике	

		деловых отношений. **Владеть:** Этап 1: - выявлять проблемы этики и этикета; Этап 2: - разрабатывать модели этичного поведения с точки зрения принципов доверия, честности и ответственности	
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать:** Этап 1: основы современной концепции социального государства, основные закономерности формирования политической сферы общества Этап 2: современные политологические проблемы, понятия, принципы и методы исследования **Уметь:** Этап 1: анализировать социально-политические процессы развития современного общества Этап 2: применять методы и средства познания в профессиональной деятельности, используя политологическую информацию **Владеть:** Этап 1: взаимодействия в поликультурной и полиэтнической среде на основе толерантного восприятия социальных и культурных различий	

		Этап 2: использования основных положений и методов социально-гуманитарных наук при решении социальных и профессиональных задач	
ОК-7	способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	**Знать:** 1 этап: основные значения лексических единиц, грамматических явлений и структур иностранного языка; знание норм социального поведения и речевого этикета своей страны и страны изучаемого языка. 2 этап: основные значения терминов, грамматических явлений и структур языка, используемых в устном и письменном профессиональном общении. **Уметь:** 1этап: читать иноязычную литературу; получать и сообщать информацию на иностранном языке в устной и письменной форме. 2 этап: самостоятельно читать иноязычную литературу по специальности; сообщать информацию на иностранном языке в устной и письменной форме; использовать иностранный язык в межличностном общении и профессиональной	

		деятельности. **Владеть:** 1 этап: навыки монологической и диалогической речи, чтения и письма неспециализированной тематики, а также страноведческого и культурологического характера. 2 этап: навыки чтения, письма, устной речи в ситуациях иноязычного общения в профессиональной сфере деятельности, предусмотренной направлениями специальности.	
ОК-8	способностью к самоорганизации и самообразованию	**Знать:** Этап 1: базовые понятия самоорганизации Этап 2: базовые понятия самообразования **Уметь:** Этап 1: использовать методы и средства самоорганизации Этап 2: использовать методы и средства самообразования **Владеть:** Этап 1: практические навыки использования методов самоорганизации Этап 2: практические навыки использования методов самообразования	
ОК-9	способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной	**Знать:** Этап 1 -знать основные положения о физической культуре в общекультурной и профессиональной подготовки студентов, о социально – биологических	

	деятельности.	основах физической культуры, об основах здорового образа и стиля жизни. Этап 2- знать об оздоровительных системах, о профессионально-прикладной физической подготовке студентов, об общедоступном и профессиональном спорте. **Уметь:** Этап 1- уметь применять систему знаний практических умений и навыков, обеспечивающих сохранение и укрепление здоровья, воспитание и совершенствование психофизических способностей и качеств. Этап 2-уметь применять различные виды физической культуры и спорта в оздоровительных, профессиональных и рекреационных целях. **Владеть:** Этап 1 – владеть практическими навыками основ физической культуры. Этап 2 -владеть практическими методами основ физической культуры.	
ОПК-1	способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения	**Знать:** Этап 1- знание основных законов механики и термодинамики; Этап 2- знание основных явлений и законов физики в области электричества	

	профессиональных задач	и магнетизма; **Уметь:** Этап 1 - применять знания из области механики и термодинамики для решения профессиональных задач; Этап 2 - применять знания в области электричества и магнетизма для решения профессиональных задач. **Владеть:** Этап 1 – навыки применения международной системы единиц измерения Си; - навыки владения физической терминологией Этап 2 - навыки решения задач из области электричества и магнетизма; - навыки проведения физического эксперимента и обработки его результатов.	
ОПК-2	способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории	**Знать:** 1 этап знать -основные понятия, положения и концепции алгебры и геометрии, алгебраические структуры; 2 этап знать -соответствующий математический аппарат алгебры и геометрии, применяемый при решении профессиональных задач. **Уметь:** 1 этап уметь	

	информации, в том числе с использованием вычислительной техники.	-формулировать основные понятия, положения и концепции алгебры и геометрии, алгебраические структуры; 2 этап уметь -корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры и геометрии. **Владеть:** 1 этап владеть -основными понятиями, положениями и концепциями алгебры и геометрии, алгебраическими структурами; 2 этап владеть -соответствующим математическим аппаратом алгебры и геометрии, применяемым при решении профессиональных задач.	
ОПК-3	способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности	**Знать:** Этап 1: методы программирования и методы разработки эффективных алгоритмов решения прикладных задач. Этап 2: современные средства разработки и анализа программного обеспечения на языках высокого уровня. **Уметь:** Этап 1: выбирать необходимые инструментальные средства для разработки программ в	

		различных операционных системах и средах. Этап 2: составлять, тестировать, проводить отладку и оформлять программы на языках высокого уровня, включая объектно-ориентированные **Владеть:** Этап 1: владеть современными средствами разработки программного обеспечения на процедурных языках программирования. Этап 2: владеть современными средствами разработки программного обеспечения на объектно-ориентированных языках программирования.	
ОПК-4	способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах.	**Знать:** Этап 1: - основные понятия и методы информации математической логики и теории алгоритмов, теории информации и кодирования; - основные нормативные правовые акты в области информационной безопасности, принципы и методы организационной защиты информации; Этап 2: - принципы и методы организационной защиты информации. **Уметь:** Этап 1: - использовать	

		математические методы и модели для решения прикладных задач; - использовать программные и аппаратные средства персонального компьютера; Этап 2: - осуществлять поиск информации по профилю деятельности в различных источниках, в том числе в глобальных компьютерных системах; - анализировать и оценивать угрозы информационной безопасности объекта. **Владеть:** Этап 1: -методами количественного анализа процессов обработки, поиска и передачи информации; - навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); Этап 2: - навыками работы с нормативными правовыми актами, методами и средствами выявления угроз безопасности автоматизированным	

		системам; - методами технической защиты информации; - навыками организации и обеспечения информационной безопасности.	
ОПК-5	способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	**Знать:** Этап 1: основные методы научных исследований Этап 2: основные методы проведения экспериментальных исследований **Уметь:** Этап 1: применять методы научных исследований. Этап 2: применять методы экспериментальных исследований **Владеть:** Этап 1: применения методов научных исследований. Этап 2: применения методов экспериментальных исследований	
ОПК-6	Способность применять нормативные правовые акты в профессиональной деятельности	**Знать:** Этап 1 Основные нормативные правовые акты в области обеспечения информационной безопасности и защиты информации, Этап 2 Нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области и на их	

		основе разрабатывать политику безопасности организации **Уметь:** Этап 1 Пользоваться нормативными правовые акты в области обеспечения информационной безопасности и защиты информации в профессиональной деятельности Этап 2 Умения внедрять нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области **Владеть:** Этап 1 Навыки работы с нормативными правовыми актами Этап 2 Навыки составления внутренних документов организации по информационной безопасности на основе работы с нормативными правовыми актами РФ	
ОПК-7	способность применять приёмы первой помощи, методы защиты производственного персонала и населения в условиях ЧС	**Знать:** Этап 1: базовые теоретические, правовые, организационные основы безопасности жизнедеятельности Этап 2: общие принципы,	

		последовательность и содержание мероприятий по оказанию первой помощи пострадавшему; методы защиты от негативных производственных и поражающих факторов ЧС **Уметь:** Этап 1: идентифицировать основные опасности среды обитания человека, оценивать риск их реализации и последствия. Этап 2: выбирать приемы оказания первой помощи, методы защиты от негативных производственных и поражающих факторов ЧС **Владеть:** Этап 1: владение знаниями теоретических, законодательных и правовых основ в области БЖД; Этап 2: владение приемами оказания первой помощи при несчастных случаях и в ЧС, навыками рационализации профессиональной деятельности с целью обеспечения безопасности и основными методами защиты в условиях ЧС	
ОПК-8	способность к освоению новых образцов программных, технических средств и информационных	**Знать:** Этап 1: основные программные, технические и информационные средства	

	технологий	Этап 2: принципы применения программных, технических и информационных средств. **Уметь:** Этап 1: использовать программные, технические и информационные средства Этап 2: освоить новые программные, технические и информационные средства **Владеть:** Этап 1: использования программных, технических и информационных средств Этап 2: освоения новых программных, технических и информационных средств	
ПК-1	способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	**Знать:** Этап 1: основные методы поиска научно – технической и нормативной литературы Этап 2: основные методические материалы по вопросам информационной безопасности **Уметь:** Этап 1: осуществлять подбор литературы по информационной безопасности Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности **Владеть:** Этап 1: осуществления	

		подбора литературы по информационной безопасности Этап 2: умения обобщения и составления обзора литературы по информационной безопасности	
ПК-2	способность создавать и исследовать модели автоматизированных систем	**Знать:** Этап 1: базовые понятия основ моделирования Этап 2: модели автоматизированных систем **Уметь:** Этап 1: использовать методы моделирования для создания моделей Этап 2: использовать структурные модели **Владеть:** Этап 1: использования методов моделирования для создания моделей 2: использования структурных моделей	
ПК-3	способность проводить анализ защищенности автоматизированных систем	**Знать:** Этап 1: методику анализа защищенности автоматизированных систем Этап 2: современные стандарты в области информационной безопасности **Уметь:** Этап 1: разрабатывать методику анализа защищенности автоматизированных систем Этап 2: использовать стандарты в области информационной безопасности **Владеть:** Этап 1: разработки анализа защищенности автоматизированных	

		систем Этап 2: использования стандартов в области информационной безопасности	
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**Знать:** Этап 1 основные модели угроз информационной безопасности Этап 2: модели нарушителей информационной безопасности **Уметь:** Этап 1: разрабатывать модели угроз информационной безопасности Этап 2: разрабатывать модели нарушителей информационной безопасности **Владеть:** Этап 1: разработки модели угроз информационной безопасности Этап 2: разработки модели нарушителей информационной безопасности	
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	**Знать:** Этап 1: основные риски информационной безопасности Этап 2: основные этапы анализа рисков информационной безопасности **Уметь:** Этап 1: рассчитывать риски информационной безопасности Этап 2: разрабатывать методику анализа рисков информационной безопасности **Владеть:** Этап 1: рассчета	

		рисков информационной безопасности Этап 2 разработки методики анализа рисков информационной безопасности	
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Знать:** Этап 1:- современные аппаратные средства вычислительной техники; Этап 2: современные инструментальные средства и технологии программирования **Уметь:** Этап 1: выполнять работы по настройке аппаратно - программных комплексов Этап 2: выполнять работы по настройке технических средств защиты информации **Владеть:** Этап 1: настройки и обслуживания аппаратно - программных комплексов Этап 2: настройки технических средств защиты информации	
ПК-7	способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**Знать:** Этап 1: основные методы поиска научно – технической и нормативной литературы Этап 2: основные методические материалы по вопросам информационной безопасности **Уметь:** Этап 1: осуществлять подбор литературы по информационной безопасности	

		Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности **Владеть:** Этап 1: осуществления подбора литературы по информационной безопасности Этап 2: умения обобщения и составления обзора литературы по информационной безопасности	
ПК-8	способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений	
ПК-9	способностью участвовать в разработке защищенных	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной	

	автоматизированных систем в сфере профессиональной деятельности	безопасности Этап 2: основные методы технико – экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений	
ПК-10	способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** Этап 1: знать физические структуры и основные типы полупроводниковых приборов, их свойства и характеристики; Этап 2: знать принципы выбора элементной базы для функциональных узлов электронной аппаратуры с учетом требований эксплуатации и экономической эффективности **Уметь:** Этап 1: уметь работать с современной элементной базой электронной аппаратуры; Этап 2: уметь осуществлять обоснованный выбор структурных и	

		принципиальных схем электронных устройств **Владеть:** Этап 1: владеть навыками чтения и составления принципиальных схем базовых функциональных узлов электронной аппаратуры; Этап 2: владеть навыками оценки параметров электронных приборов и устройств по комплекту документации	
ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	**Знать:** Этап 1 основные составляющие политики безопасности Этап 2: принципы разработки политики безопасности **Уметь:** Этап 1: разрабатывать политику безопасности Этап 2: применять комплексный подход к обеспечению информационной безопасности **Владеть:** Этап 1: навыки разработки политики безопасности Этап 2применения комплексного подхода к обеспечению информационной безопасности	
ПК-12	способность участвовать в проектировании системы управления информационной безопасностью автоматизированной	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико –	

	системы	экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений	
ПК-13	способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования	

		проектных решений	
ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** Этап 1: основные этапы контрольных проверок технических средств защиты информации Этап 2: основные принципы работы технических средств защиты информаци **Уметь:** Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации **Владеть:** Этап 1: навыки применения контрольных проверок Этап 2: навыки оценки эффективности применении аппаратно - программных комплексов	
ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	**Знать:** Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов **Уметь:** Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки и оценки результатов эксперимента **Владеть:** Этап 1: разработки методики проведения экспериментов	

		Этап 2: разработки методики обработки и оценки результатов эксперимента	
ПК-16	способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	**Знать:** Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов **Уметь:** Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки и оценки результатов эксперимента **Владеть:** Этап 1: разработки методики проведения экспериментов Этап 2: разработки методики обработки и оценки результатов эксперимента	
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	**Знать:** Этап 1: методику анализа информационной безопасности Этап 2: современные стандарты в области информационной безопасности **Уметь:** Этап 1: разрабатывать методику анализа информационной безопасности Этап 2: использовать стандарты в области информационной безопасности **Владеть:** Этап 1: разработки анализа информационной безопасности Этап 2: использования стандартов в области	

		информационной безопасности	
ПК-18	способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**Знать:** Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности **Уметь:** Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности **Владеть:** Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности	
ПК-19	способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**Знать:** Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности **Уметь:** Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной	

		безопасности **Владеть:** Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности	
ПК-20	способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать:** Этап 1: принципы разработки и внедрения информационных систем; Этап 2: принципы эффективного применения автоматизированных информационных систем с учетом требований информационной безопасности **Уметь:** Этап 1: использовать методы разработки и внедрения информационных систем Этап 2: реализовать разработку автоматизированной информационной системы с учетом требований информационной безопасности **Владеть:** Этап 1: методами разработки, внедрения, эксплуатации информационных систем Этап 2: методами сопровождения информационных систем	
ПК-21	способностью разрабатывать проекты документов,	**Знать:** Этап 1: основные этапы оформления	

	регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	рабочей документации Этап 2: основные нормативные и методические документы **Уметь:** Этап 1: разрабатывать основные рабочие документы Этап 2: применять нормативные документы в рабочей документации **Владеть:** Этап 1: навыки разработки рабочих документов Этап 2: навыки применения нормативных документов	
ПК-22	способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знать:** Этап 1 основные составляющие политики безопасности Этап 2: принципы разработки политики безопасности **Уметь:** Этап 1: разрабатывать политику безопасности Этап 2: применять комплексный подход к обеспечению информационной безопасности **Владеть:** Этап 1: навыки разработки политики безопасности Этап 2применения комплексного подхода к обеспечению информационной безопасности	
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации	**Знать:** Этап 1: основные принципы администрирования Этап 2: современные инструментальные	

	ограниченного доступа	средства администрирования **Уметь:** Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь использовать инструментальные средства администрирования подсистемы безопасности **Владеть:** Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности	
ПК-24	способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**Знать:** Этап 1: принципы эффективного применения информационно-технологических ресурсов; Этап 2: принципы информационной безопасности **Уметь:** Этап 1: использовать методы эффективного применения информационно-технологических ресурсов Этап 2: реализовать политику информационной безопасности **Владеть:** Этап 1: методами разработки, внедрения, эксплуатации	

		информационно-технологических ресурсов Этап 2: методами сопровождения информационно-технологических ресурсов	
ПК-25	способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	**Знать:** Этап 1: принципы эффективной реализации резервного копирования данных; Этап 2: принципы информационной безопасности в процессах резервного копирования данных **Уметь:** Этап 1: использовать методы резервного копирования данных Этап 2: реализовать политики информационной безопасности для процессов резервного копирования данных **Владеть:** Этап 1: методами разработки, внедрения, эксплуатации резервного копирования данных Этап 2: методами сопровождения резервного копирования данных	
ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	**Знать:** Этап 1: основные принципы администрирования Этап 2: современные инструментальные средства администрирования **Уметь:** Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь	

		использовать инструментальные средства администрирования подсистемы безопасности **Владеть:** Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности	
ПК-27	способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Знать:** Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности **Уметь:** Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности **Владеть:** Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности	
ПК-28	способность управлять информационной безопасностью	**Знать:** Этап 1: основные меры по выполнения обеспечения	

	автоматизированной системы	информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности **Уметь:** Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности **Владеть:** Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности	
ПСК-3.1	способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	**Знать:** Этап 1: основные информационные технологии Этап 2: автоматизированные системы, применяемые при организации защиты информации **Уметь:** Этап 1: разрабатывать и использовать особенности информационных технологий Этап 2: использовать особенности автоматизированных систем при организации системы защиты **Владеть:** Этап 1: использования информационных технологий при	

		организации системы защиты Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты	
ПСК-3.2	способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	**Знать:** Этап 1: основные операционные системы, системы управления базами данных Этап 2: комплекс задач при администрировании подсистем информационной безопасности **Уметь:** Этап 1: выполнять комплекс задач администрирования подсистемы безопасности Этап 2: выполнять комплекс задач по безопасности операционных систем и баз данных **Владеть:** Этап 1:выполения комплекса задач администрирования подсистем безопасности Этап 2: выполнения администрирования компьютерных сетей по безопасности	
ПСК-3.3	способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности	**Знать:** Этап 1: основные показатели надежности систем обеспечения информационной безопасности Этап 2: комплекс мер по обеспечению надежности систем	

	критически важных объектов и автоматизированных систем критически важных объектов	обеспечения информационной безопасности **Уметь:** Этап 1: планировать комплекс мер по обеспечению надежности систем безопасности Этап 2:организовывать комплекс мер по обеспечению надежности подсистемы безопасности информации **Владеть:** Этап 1: планирования комплекса мер по обеспечению надежности систем безопасности Этап 2: организации комплекса мер по обеспечению надежности подсистемы безопасности информации	
ПСК-3.4	способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем	

		информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений	
ПСК-3.5	способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	**Знать:** Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений **Уметь:** Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений **Владеть:** Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений	

3. Государственный экзамен

3. 1 Шкала оценивания.

Университет использует традиционную шкалу оценивания, представленную в таблице ниже.

Таблица 3.

Оценка	Характеристика оценки
«Отлично»	Обучающийся показывает высокий уровень компетентности, знания программного материала, раскрывает не только основные понятия, но и анализирует их со своей точки зрения. Показывает высокий уровень теоретических знаний экзаменационного билета. Профессионально, грамотно, последовательно и четко излагает материал, аргументировано формулирует выводы. В рамках

	требований к специальности знает законодательно-нормативную базу. Глубоко и полно раскрывает дополнительные вопросы.
«Хорошо»	Обучающийся показывает достаточно уровень компетентности, знаний и практику их применения. Уверенно и профессионально излагает состояние вопросов экзаменационного билета. Показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений. Ответ построен логично, материал излагается хорошим языком. При этом в ответе обучающийся допускает несущественные ошибки или у него возникают сложности при ответе на дополнительные вопросы.
«Удовлетворительно»	Обучающийся показывает достаточные знания учебного и лекционного материала, при этом в ответе не всегда присутствует логика, отсутствуют связь между анализом, аргументацией и выводами. На дополнительные вопросы членов государственной экзаменационной комиссии затрудняется с ответами, показывает недостаточно глубокие знания.
«Неудовлетворительно»	Выставляется обучающемуся в случае, если материал излагается непоследовательно, не аргументировано, ответы на вопросы выявили несоответствие уровня знаний выпускника требованиям ФГОС ВО в части формируемых компетенций, а также дополнительных компетенций, установленными вузом. Неправильно отвечает на поставленные вопросы членами государственной экзаменационной комиссией или затрудняется с ответами.

3.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы.

Вопросы по дисциплине «Основы аттестации объектов информатизации»

1. Конституция Российской Федерации от 12 декабря 1993 г.
2. Закон Российской Федерации от 28.12.2010 № 390 "О безопасности".
3. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9.09.2000 г. № Пр-1895.
4. Закон Российской Федерации от 28.12.2010 № 390"О безопасности
5. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17.12.1997 г. № 1300.
6. Федеральный Закон Российской Федерации от 27.12.2002 г. (действующая редакция от 23.06.2014) № 184-ФЗ "О техническом регулировании".
7. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30.03.1992 г.
8. Федеральный Закон Российской Федерации от 27.12.2002 г. (действующая редакция от 23.06.2014) № 184-ФЗ "О техническом регулировании". Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
9. Указ Президента Российской Федерации 17 марта 2008 года (ред. от 25.07.2014) № 351 “О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена”.
10. Указ Президента Российской Федерации “Вопросы Федеральной службы по техническому и экспортному контролю”; “Вопросы Межведомственной комиссии по

защите государственной тайны" и "О некоторых мерах государственного регулирования размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации и иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации

11. Указ Президента Российской Федерации от 16.08.2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю".
12. Указ Президента Российской Федерации от 6.10.2004 г. № 1286. "Вопросы Межведомственной комиссии по защите государственной тайны".
13. Указ Президента Российской Федерации от 23.04.2001 г. №458. "О некоторых мерах государственного регулирования размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации и иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации".

Вопросы по дисциплине «Инженерно-техническая защита информации и технические средства на критически важных объектах»

1. Режим защиты информации не устанавливается в отношении сведений, относящихся к …
государственной тайне
деятельности государственных деятелей
конфиденциальной информации
персональным данным
2. В регистрации средства массовой информации не может быть отказано…
когда заявление подано не соответствующим лицом
по мотивам нецелесообразности
даже если сведения в заявлении не соответствуют действительности
если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения
3. Засекречиванию подлежат сведения о …
состоянии демографии
состоянии преступности
фактах нарушения прав и свобод человека и гражданина
силах и средствах гражданской обороны
4. Проверить электронно-цифровую подпись под документом может…
только эксперт, преобразуя электронный образец документа и открытый ключ отправителя
любое заинтересованное лицо, преобразуя электронный образец документа, открытый ключ отправителя и собственно значение электронно-цифровой подписи
только эксперт с помощью преобразований электронного образца документа, открытого ключа отправителя и собственно значения электронно-цифровой подписи
только отправитель электронного документа
5. Режим документированной информации – это …
выделенная информация по определенной цели
электронный документ с электронно-цифровой подписью
выделенная информация в любой знаковой форме
электронная информация, позволяющая ее идентифицировать
6. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется …
для доставки почтовых отправлений
в целях профессиональной деятельности журналиста

в целях профессиональной деятельности оператора
для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно
7. Режим общественного достояния устанавливается для …
любой общедоступной информации
сведений, которые являются уникальными, незаменимыми по своей природе
любой общественной организации
для государственных органов и муниципальных образований
8. Учредителями средства массовой информации могут выступать…
граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории российской Федерации
только юридические лица
граждане, достигшие 16 лет и юридические лица
граждане другого государства, постоянно не проживающие в Российской Федерации, юридические лица и органы государственной власти
граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти
9. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи.
1 месяца, 1 года
7 месяцев, полгода
1 года, 3 лет
10. С точки зрения информационного права информация – это …
сведения о законодательстве, правовых явлениях, правоприменительной деятельности
данные о развитии конкретной правовой науки и ее практическом применении
сведения независимо от формы их представления
форма выражения объективных знаний
11. Не являются объектами информационного правоотношения …
неправовая информация
обладатели информации
информационные системы
элементы информационной системы
информационные продукты
недокументированная информация
12. Общее управление информационной сферой не вправе осуществлять …
экспертные советы
министерство информационных технологий
федеральное агентство по науке и инновациям
федеральные службы

Вопросы по дисциплине «Обеспечение информационной безопасности на критически важных объектах»

1. Общие вопросы информационной безопасности.
2. Государственная система информационной безопасности.
3. Понятие угрозы. Виды противников или «нарушителей».
4. Организация защиты информации при приеме на предприятии иностранных представителей
5. Основные цели планирования мероприятий по организационной защите.
6. Информационная безопасность и ее обеспечение.

7. Причины нарушения целостности информации

Основные направления работы с персоналом и методы работы с персоналом, допущенным к конфиденциальным документам

Организация защиты информации при проведении совещаний

8. Аппаратные и программные средства для защиты компьютерных систем от НСД.
9. Хеширование. Имитовставки. Криптографические генераторы случайных чисел.
10. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов.
11. Организация защиты информации при приеме на предприятии иностранных представителей

Основные цели планирования мероприятий по организационной защите

Вопросы по дисциплине «Защита электронного документооборота критически важных объектов»

1. Задачи, функции и структура информационной системы электронного документооборота.
2. Электронный регламент управления организацией.
3. Проблема стандартизации метаданных и форматов в контексте реализации проекта «Электронного правительства».
4. Юридическая сила электронного документа.
5. Проблема защиты информации и информационной безопасности в системах электронного документооборота.
6. Защита персональных данных в информационных системах
7. Признаки классификации систем электронного документооборота критически важных объектов.
8. Степень интегрированности программного обеспечения в рамках организации, многофункциональность, масштабирование, мультиформатность, открытость формата, отношение к поддержке безбумажного документооборота, отечественным стандартам делопроизводства.
9. Различие технологий workflow и docflow.
10. Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ.
11. Общегосударственные информационные системы. Федеральные целевые программы в области внедрения электронного документооборота.
12. Критерии выбора программного обеспечения для системы электронного документооборота критически важных объектов и фирмы-разработчика.

Вопросы по дисциплине «Методы и средства противодействия террористической деятельности в системах управления критически важных объектов»

1. Почему количественный анализ рисков в чистом виде не достижим?

A. Он достижим и используется

B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.

C. Это связано с точностью количественных элементов

+D. Количественные измерения должны применяться к качественным элементам

2. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

+A. Много информации нужно собрать и ввести в программу

B. Руководство должно одобрить создание группы

C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки

D. Множество людей должно одобрить данные

3. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
A. Стандарты
B. Должный процесс (Due process)
+C. Должная забота (Due care)
D. Снижение обязательств
4. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
+D. Открытый стандарт, определяющий цели контроля

5. Из каких четырех доменов состоит CobiT?
+A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
6. Что представляет собой стандарт ISO/IEC 27799?
+A. Стандарт по защите персональных данных о здоровье
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60
7. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
+B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости
8. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
A. NIST и OCTAVE являются корпоративными
+B. NIST и OCTAVE ориентирован на ИТ
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными

9. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
A. Анализ связующего дерева
B. AS/NZS
C. NIST
+D. Анализ сбоев и дефектов
10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
+A. Сотрудники
B. Хакеры

C. Атакующие
D. Контрагенты (лица, работающие по договору)
11. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
+C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации
12. Что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
+B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные
13. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных
B. Пользователи
C. Администраторы
+D. Руководство
14. Что такое процедура?
A. Правила использования программного и аппаратного обеспечения в компании
+B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

Вопросы по дисциплине «Защита информации в телекоммуникационных системах» основные понятия построения систем и сетей электросвязи и особенности их эксплуатации:

1. тактико-технические характеристики основных телекоммуникационных систем, сигналов и протоколов, применяемых для передачи различных видов сообщений;
2. перспективы развития систем и сетей связи
3. творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем;
4. отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи;
5. разрабатывать структурные схемы систем связи с заданными характеристиками;
6. владеть навыками анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений;
7. анализа сетевых протоколов;
8. навыками работы с научно-технической литературой по изучению перспективных систем и сетей связи с целью повышения эффективности использования защищенных телекоммуникационных систем;
9. структуры построения узлов ЗТКС;
10. организацию технической эксплуатации на узлах;
11. принципы работы автоматизированных систем технической эксплуатации;
12. оценивать показатели надежности;
13. выбирать основные контролируемые параметры технического состояния ТКС.
14. тестировать оборудование ЗТКС;•
15. выявления технических каналов утечки информации;

16. организационного и правового обеспечения информационной безопасности
17. телекоммуникационных систем в рамках должностных обязанностей техника по защите информации
18. организации защиты в различных операционных системах и средах
19. основные положения системного подхода к технической защите информации;
20. основные технические каналы утечки защищаемой информации в автоматизированных и телекоммуникационных системах, физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности;

3.3 Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

Члены государственной экзаменационной комиссии самостоятельно оценивают уровень подготовки выпускника. Оценка за сдачу экзамена составляет среднее арифметическое от его оценок за каждый ответ из билета государственного экзамена (табл.4). Если среднее арифметическое составляет не целое число, то решение об оценке принимается «в пользу экзаменуемого». Оценивая ответы экзаменуемого, члены государственной экзаменационной комиссии должны учитывать насколько он свободно владеет и излагает материал.

Оценка государственной экзаменационной комиссии определяется на закрытом заседании большинством голосов ее членов. При равенстве голосов голос председателя государственной экзаменационной комиссии является решающим.

Таблица 4 - Структура формирования оценки государственного экзамена

Показатели оценивания	Учебная дисциплина (оценка)					
	Основы аттестации объектов	Инженерно-техническая защита	Обеспечение информационной	Защита электронного документ	Методы и средства противодействия	Защита информации в телекоммун
Умение оперировать профессиональными понятиями и терминами	4	5	4	4	4	4
Глубина раскрытия вопроса	4	5	4	4	4	4
Способность анализировать ситуацию и вырабатывать	4	5	4	4	4	4
Дополнительный вопрос	4	5	4	4	4	4
Средняя оценка по дисциплине	4	5	4	4	4	4
Итоговая оценка по государственному экзамену	16	20	16	16	16	16

4 Выпускная квалификационная работа

4.1 Шкала оценивания.

Университет использует традиционную шкалу оценивания, представленную в таблице ниже.

Таблица 5

Оценка	Характеристика оценки
«Отлично»	выставляется, если: - при выполнении ВКР выпускник продемонстрировал полное соответствие уровня своей подготовки требованиям ФГОС ВО, показал глубокие знания и умения; - представленная к защите работа выполнена в полном соответствии с заданием, отличается глубиной профессиональной проработки всех разделов ее содержательной части, выполнена и оформлена качественно и в соответствии с установленными правилами; - в докладе исчерпывающе, последовательно, четко, логически стройно и кратко изложена суть работы и ее основные результаты; - на все вопросы членов государственной экзаменационной комиссии даны обстоятельные и правильные ответы; - критические замечания научного руководителя выпускником проанализированы, и в процессе защиты приведены аргументированные доказательства правильности решений, принятых в работе.
«Хорошо»	выставляется, если: - при выполнении ВКР выпускник продемонстрировал соответствие уровня своей подготовки требованиям федерального государственного образовательного стандарта, показал достаточно хорошие знания и умения; - представленная к защите работа выполнена в полном соответствии с заданием, отличается глубиной профессиональной проработки всех разделов ее содержательной части, выполнена и оформлена качественно и в соответствии с установленными правилами; - в докладе правильно изложена суть работы и ее основные результаты, однако при изложении допущены отдельные неточности; - на большинство вопросов членов комиссии даны правильные ответы; - критические замечания научного руководителя выпускником проанализированы, и в процессе защиты приведены аргументированные доказательства правильности решений, принятых в работе.
«Удовлетворительно»	выставляется, если: - при выполнении ВКР выпускник продемонстрировал соответствие уровня своей подготовки требованиям ФГОС ВО, показал удовлетворительные знания и умения; - представленная к защите работа выполнена в соответствии с заданием, но без достаточно глубокой проработки некоторых разделов, имеют место несущественные ошибки

	и нарушения установленных правил оформления работы; - в докладе изложена суть работы и ее результаты; - на вопросы членов комиссии выпускник отвечает, но неуверенно; - не все критические замечания научного руководителя проанализированы правильно.
«Неудовлетворительно»	выставляется тогда, когда: - в ВКР обнаружены значительные ошибки, свидетельствующие о том, что уровень подготовки выпускника не соответствует требованиям федерального государственного образовательного стандарта; - при решении задач, сформулированных в задании, выпускник не показывает необходимых знаний и умений; - доклад затянут по времени и (или) читался с листа; - на большинство вопросов членов комиссии ответы даны неправильные или не даны вообще.

4.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы.

Представляется тематика выпускных квалификационных работ.

1. «Исследование принципов построения биометрических систем контроля доступа на основе анализа рукописного почерка»;
2. «Исследование характеристик систем стеганографии звуковых данных с использованием дискретного вейвлет-преобразования»;
3. «Анализ стойкости криптосистемы, использующей для открытого обмена ключами нейронные сети»;
4. «Корреляционный анализ предупреждений системы обнаружения атак на основе нечёткой логики»;
5. «Разработка методов и алгоритмов защиты исходного кода программ от несанкционированного доступа»;
6. «Разработка методики оценки эффективности средств защиты информации».
7. «Система защиты данных в корпоративных сетях на основе криптографических методов»;
8. «Система защиты объекта от несанкционированного проникновения с использованием пассивных технических средств охраны»;
9. «Система обнаружения атак на основе искусственной нейронной сети»;
10. «Система контроля движения на охраняемом объекте с помощью активных радиоволновых технических средств»;
11. «Подсистемы контроля управления доступом и охраны территории на базе интегрированной системы «Орион».

4.3 Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы.

Оценка за выпускную квалификационную работу составляет среднее арифметическое от его оценок за каждый из критериев. Если среднее арифметическое составляет не целое число, то решение об оценке принимается «в пользу экзаменуемого».

Оценка результата защиты выпускной квалификационной работы производится на закрытом заседании государственной экзаменационной комиссии. При равенстве голосов голос председателя государственной экзаменационной комиссии является решающим. За

основу принимаются следующие критерии:

Таблица 6 – Структура формирования оценки защиты ВКР

Код компетенции	Показатели оценивания										
	Оформление	Список используемой литературы	Обзорная	Теоретическая часть	Проектная часть	Охрана труда и окружающей среды	Экономическая часть	Заключение	Доклад	Графическая часть	Средняя оценка
ПК-1;		1		1			1	1		1	5
ПК-2;	1		1			1			1		4
ПК-3;		1			1			1	1	1	5
ПК-4;	1			1			1				3
ПК-5;		1			1	1		1	1		5
ПК-6;	1				1				1		3
ПК-7;		1		1		1	1				4
ПК-8;								1		1	2
ПК-9;	1	1		1	1		1		1		6
ПК-10;			1		1	1	1	1	1		6
ПК-11;	1		1		1					1	4
ПК-12;		1	1					1			3
ПК-13;	1					1	1			1	4
ПК-14;		1	1		1				1		4
ПК-15;	1			1			1	1		1	5
ПК-16;		1	1				1				3
ПК-17;				1					1	1	3
ПК-18;	1	1			1			1			4
ПК-19;			1			1				1	3
ПК-20;	1	1					1		1		4
ПК-21;				1	1			1		1	4
ПК-22;				1							1
ПК-23;	1		1			1				1	4
ПК-24;				1	1		1				3
ПК-25;									1		1
ПК-26;			1			1		1			3
ПК-27;				1		1					2
ПК-28;			1			1					2
Итоговая оценка защиты ВКР											100