Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ

Заведующий кафедрой ИЗИ
_____ М.Ю. Монахов
"28" 12 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ МАГИСТРАНТОВ

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки _____

Уровень высшего образования магистратура

Форма обучения очная

Владимир 2016

1. Общие положения

Государственная итоговая аттестация (ГИА) направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВО по направлению 10.04.01 "Информационная безопасность".

Целью ГИА является оценка сформированности компетенций и определение соответствия результатов освоения обучающимися ОПОП соответствующим требованиям ФГОС. ГИА по направлению 10.04.01 "Информационная безопасность" включает защиту выпускной квалификационной работы магистрантов (ВКР).

Нормативно-правовое обеспечение ФОС для государственной итоговой аттестации магистрантов.

ФОС для государственной итоговой аттестации магистрантов разработан на основании следующих документов:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры, утвержденного Приказом Минобрнауки РФ от 19.12.2013г. № 1367;
- Письма Минобразования РФ от 16.05.2002 г. № 14-55-353 ин/15 «О методике создания оценочных средств для итоговой государственной аттестации выпускников вузов»;
- Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры, утвержденного Приказом Минобрнауки РФ от 29. 06. 2015 г. № 636;
- Федерального государственного образовательного стандарта по направлению подготовки 10.03.01 Информационная безопасность;
- Положение о разработке фонда оценочных средств (ФОС) государственной итоговой аттестации (ГИА), (решение НМС ВлГУ, протокол №9 от 19.05.2016) и утвержденное приказом ВлГУ от 08.06.2016 №260/1;
- Устава ВлГУ и других нормативных локальных актов ВлГУ.

2. Перечень компетенции, которыми должен овладеть обучающийся в результате освоения образовательной программы в соответствии с ФГОС ВО

В соответствии с требованиями ФГОС ВО государственная итоговая аттестация обеспечивает контроль полноты формирования следующих общекультурных и профессиональных компетенций, которыми должен обладать выпускник по направлению 10.04.01 "Информационная безопасность".

Выпускник по направлению 10.04.01 "Информационная безопасность" с квалификацией «магистр» в соответствие с целями основной образовательной программы (ОПОП) и задачами профессиональной деятельности в результате освоения данной ОПОП должен обладать следующими компетенциями:

Состав компетенций и планируемые результаты

Коды компетенций по ФГОС	Компетенции	Планируемые результаты
ОК-1	способность к абстрактному мышлению, анализу, синтезу	**знать:** основные теории и методы макро- и микроэкономики; экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности); основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; - содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук; основные этапы развития философской мысли, основную проблематику и структуру философского знания. **уметь:** анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; - использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; анализировать мировоззренческие, социально и личностно значимые философские проблемы; анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности. **владеть:** - приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; - основными методами научного познания; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники.
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	**знать:** основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **уметь:** самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **владеть:** навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.

ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	**Знать:** основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **Уметь:** - строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть:** методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима секретности навыками управления информационной безопасностью простых объектов.
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**Знать:** цели, задачи и принципы построения системы защиты информации; - требования, предъявляемые к системе защиты информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности**.** **Уметь:** определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять системы компьютерной математики для решения типовых задач; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.

		Владеть: информацией о факторах, определяющие необходимость защиты территории и здания предприятия;- информацией о взаимодействии между субъектами, защищающими и использующими информацию ограниченного доступа; информацией о структуре технического задания на создание комплексной системы защиты информации на предприятии; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; -методикой определения возможностей несанкционированного доступа к защищаемой информации; методикой разработке модели комплексной системы защиты информации; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	**Знать:** основные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей КС-субъектов доступа к данным; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; основные теоретико-числовые методы применительно к задачам защиты информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. **Уметь:** квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты; применять средства ВТ, средства программирования для эффективной реализации аппаратно-программных комплексов заданного качества и в заданные сроки; проводить испытания объектов профессиональной деятельности; производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть:** навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками сопровождения программно-аппаратных средств защиты информации; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов.
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	**Знать:** понятийно-категориальный аппарат информационной безопасности; возможности, состояние и перспективы развития информационных технологий; основной инструментарий в виде программного обеспечения для деловых применений при анализе, проектировании и прогнозировании; назначение, принципы работы средств новых информационных технологий; сетевые информационные технологии; качественные и количественные методы описания информационных технологий; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **Уметь:** ставить и решать типовые задачи с помощью современных информационных технологий; применять на

		пользовательском уровне основные средства новых информационных технологий в профессиональной деятельности; использовать информационно-поисковые средства локальных и глобальных вычислительных и информационных сетей; применять системы компьютерной математики для решения типовых задач; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть:** навыками применения современных информационных технологий к текущим реальным ситуациям, основными классификациями информационных систем, навыками развертывания основных программных комплексов и программ, реализующих ту или иную информационную технологию; навыками аналитического и численного решения задач математической статистики.
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок	**Знать:** основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; методы подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; методы концептуального проектирования технологий обеспечения информационной безопасности. **Уметь:** использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть:** Основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.

ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	**знать:** основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **уметь:** проводить классификацию экспериментов; выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **владеть:** методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов; навыками аналитического и численного решения задач; методами проведения физического эксперимента при выявлении технических каналов утечки информации.
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	**знать:** основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования;

		использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **владеть:** основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно- процессуальном и финансовом законодательстве; навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.
ПК-9	способность проводить аудит информационной безопасности информационных систем и объектов информатизации	**Знать**: суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности. **Уметь:** ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть**: методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов.
ПК-10	способность проводить аттестацию объектов информатизации по требованиям безопасности информации	**знать:** -основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России. Знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности. **уметь:** - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и

		информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно- технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме. **владеть:** навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; - типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования; :- навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну
ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности	**знать:** - основные теории и методы макро- и микроэкономики;- методы концептуального проектирования технологий обеспечения информационной безопасности; - основы психологии личности и социальную среду общества; **уметь:** анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; - Прогнозировать информационные риски, анализировать результаты их возможной реализации, разрабатывать защитные механизмы для предотвращения типовых угроз; находить психологические контакты с обучаемыми; - учебно-методическую нормативную базу; основы документооборота и документоведения **владеть:** приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям; навыками управления информационной безопасностью простых объектов; навыками обеспечения социально-психологической безопасности личности; навыками мотивации сотрудников небольших коллективов; - навыками составления нормативно-распорядительных документов
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	**Знать:** основные принципы управления и системной организации; – разновидности и свойства систем управления. **Уметь:** - строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; - обосновывать принципы организации

		технического, программного и информационного обеспечения информационной безопасности **Владеть:** – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микро-ЭВМ в системах управления; - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками управления информационной безопасностью простых объектов
ПК-13	способность организовать управление информационной безопасностью	**Знать:** – разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 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 организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; - основные документы, регламентирующую организационную безопасность на объекте; - 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; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем **Уметь:** – программно реализовывать алгоритмы управления в цифровых системах;: - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности **Владеть:** - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех.документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микро-ЭВМ в системах управления

ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	**Знать:** – разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 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 организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; - основные документы, регламентирующую организационную безопасность на объекте; - 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; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. **Уметь:** – программно реализовывать алгоритмы управления в цифровых системах;: - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. **Владеть:** - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех.документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микро-ЭВМ в системах управления.
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	**знать:** основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии. **уметь:** осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;

		организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; синтезировать структуру комплексной системы защиты информации; оценивать эффективность системы защиты информации. **владеть:** навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации.
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	**знать:** основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений; **уметь: -** осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности; **владеть:** навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы

3. Описание показателей и критериев оценивания компетенций, а также шкал оценивания

Характеристика работы		Баллы	
1. Оценка работы по формальным критериям			
1.1.	Использование литературы (достаточное количество актуальных источников, достаточность цитирования, использование нормативных документов, научной и справочной литературы	0-5	
1.2.	Соответствие ВКР «Регламенту оформления ВКР по основным профессиональным образовательным стандартам высшего образования ВлГУ» и методическим указаниям кафедры	0-5	
	ВСЕГО БАЛЛОВ	0-10	
2. Оценка работы по содержанию			
2.1.	Введение содержит следующие обязательные элементы: - актуальность темы и практическая значимость работы; - цель ВКР, соответствующая заявленной теме; - круг взаимосвязанных задач, определенных поставленной целью; - объект исследования; - предмет исследования.	0-5	
2.2.	Содержательность и глубина проведенного теоретического исследования поставленной проблемы	0-10	
2.3.	Содержательность экономико-организационной характеристики объекта исследования и глубина проведённого анализа проблемы	0-20	
2.4.	Содержательность рекомендаций автора, по совершенствованию технологических процессов или устранению проблем в деятельности объекта исследования, выявленных по результатам проведенного анализа.	0-15	
2.5.	Оригинальность и практическая значимость предложений и рекомендаций	0-5	
	ВСЕГО БАЛЛОВ	0-55	
3. Оценка защиты выпускной квалификационной работы			
3.1.	Качество доклада (структурированность, полнота раскрытия решенных задач для достижения поставленной цели, аргументированность выводов, включая чертежную документацию)	0-5	
3.2.	Качество и использование презентационного материала (информативность, соответствие содержанию доклада, наглядность, достаточность).	0-5	
3.3.	Ответы на вопросы комиссии (полнота, глубина, оригинальность мышления).	0-25	
	ВСЕГО БАЛЛОВ	0-35	
	СУММА БАЛЛОВ	**100**	

Шкала соотнесения баллов и оценок

Оценка	**Количество баллов**
«2» неудовлетворительно	0-60
«3» удовлетворительно	61-73
«4» хорошо	74-90
«5» отлично	91-100

Члены ГЭК оценивают ВКР, исходя из степени раскрытия темы, самостоятельности и глубины изучения проблемы, обоснованности выводов и предложений, а также исходя из уровня сформированности компетенций выпускника, который оценивают руководитель, рецензент и сами члены ГЭК. Результаты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценки:

«Отлично»:

- доклад структурирован, раскрывает причины выбора темы и ее актуальность, цель, задачи, предмет, объект исследования, логику получения каждого вывода; в заключительной части доклада показаны перспективы и задачи дальнейшего исследования данной темы, освещены вопросы практического применения и внедрения результатов исследования в практику;
- ВКР выполнена в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом;
- представленный демонстрационный материал высокого качества в части оформления и полностью соответствует содержанию ВКР и доклада;
- ответы на вопросы членов ГЭК показывают глубокое знание исследуемой проблемы, подкрепляются ссылками на соответствующие литературные источники, выводами и расчетами из ВКР, демонстрируют самостоятельность и глубину изучения проблемы студентом;
- выводы в отзыве руководителя и в рецензии на ВКР не содержат замечаний;
- результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет от 4,75 до 5 баллов.

«Хорошо»:

Доклад структурирован, допускаются одна-две неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, но эти неточности устраняются при ответах на дополнительные уточняющие вопросы.

- ВКР выполнена в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом.
- представленный демонстрационный материал хорошего качества в части оформления и полностью соответствует содержанию ВКР и доклада;
- ответы на вопросы членов ГЭК показывают хорошее владение материалом, подкрепляются выводами и расчетами из ВКР, показывают самостоятельность и глубину изучения проблемы студентом;
- выводы в отзыве руководителя и в рецензии на ВКР без замечаний или содержат незначительные замечания, которые не влияют на полноту раскрытия темы;
- результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет от 3,75 до 4,75 баллов.

«Удовлетворительно»:

- доклад структурирован, допускаются неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, но эти неточности устраняются в ответах на дополнительные вопросы;

- ВКР выполнена в соответствии с целевой установкой, но не в полной мере отвечает предъявляемым требованиям;
- представленный демонстрационный материал удовлетворительного качества в части оформления и в целом соответствует содержанию ВКР и доклада;
- ответы на вопросы членов ГЭК носят не достаточно полный и аргументированный характер, не раскрывают до конца сущности вопроса, слабо подкрепляются выводами и расчетами из ВКР, показывают недостаточную самостоятельность и глубину изучения проблемы студентом.
- выводы в отзыве руководителя и в рецензии на ВКР содержат замечания, указывают на недостатки, которые не позволили студенту в полной мере раскрыть тему;
- результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет от 2,75 до 3,75 баллов.

«Неудовлетворительно»:
- доклад недостаточно структурирован, допускаются существенные неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, эти неточности не устраняются в ответах на дополнительные вопросы;
- ВКР не отвечает предъявляемым требованиям;
- представленный демонстрационный материал низкого качества в части оформления и не соответствует содержанию ВКР и доклада;
- ответы на вопросы членов ГЭК носят неполный характер, не раскрывают сущности вопроса, не подкрепляются выводами и расчетами из ВКР, показывают недостаточную самостоятельность и глубину изучения проблемы студентом.
- выводы в отзыве руководителя и в рецензии на ВКР содержат существенные замечания, указывают на недостатки, которые не позволили студенту раскрыть тему;
- результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет от 2 до 2,75 баллов.

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

Примерные темы ВКР могут быть представлены следующими направлениями:
- разработка и обоснование системы мер, обеспечивающих организацию и технологию защиты информации конкретного объекта, на основе использования различных защитных средств: организационных, инженерно-технических, правовых, криптографических, программно-аппаратных;
- нахождение и обоснование решения научно-исследовательской задачи одной из актуальных проблем в области защиты информации, обеспечивающей информационную безопасность выбранного объекта, путем разработки требуемых выводов и заключений, а так же построении математических и информационных моделей;

Структура ВКР:

Введение. Раскрывается актуальность выбора темы, формулируются компоненты методологического аппарата: проблема, объект, предмет, цель, задачи.

Глава 1. Аналитический обзор. Производится предпроектное описание выбранного объекта; производится анализ и моделирование информационных процессов протекающих в объекте; конкретизируются и анализируются решаемые в работе задачи, рассматриваются основные виды угроз информационной безопасности объекта; описываются возможные средства и инструменты решения поставленной перед работой задачи. Разрабатывается план мероприятий по решению обозначенной задачи.

Глава 2. Решение поставленной задачи. Производится выбор и обоснование выбора методов и средств для решения поставленных перед работой задач (методы и средства проектирования, аппаратные и программные средства защиты информации, а так же среды программирования). Осуществляется реализация проектных решений в

соответствии с поставленными задачами. Описываются результаты тестирования разработанных мер по обеспечению информационной безопасности объекта.

Глава 3. Краткая характеристика программных средств.

Описываются все программные средства, направленные на достижение поставленной перед работой цели и полученные в результате работы над ВКР. Приводятся подробные руководства программисту и пользователю.

Заключение.

Приводятся выводы в соответствии с поставленными и выполненными задачами.

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

Итоговая оценка за выполнение и защиту ВКР складывается из оценок: текста пояснительной записки ВКР; демонстрационных материалов (презентации результатов работы); доклада на защите; - ответов на вопросы членов комиссии.

Лица, оценивающие сформированность компетенций	**Элементы оценивания**			
	Текст пояснительной записки	**Презентация**	**Доклад**	**Ответы на вопросы членов ГЭК**
Руководитель	ОК-1; ПК-1-ПК16	ОК-1; ПК-1-ПК-16	ОК-1; ПК-1-ПК16	ОК-1; ПК1-ПК-16
Рецензент	ОК-1; ПК-1-ПК3; ПК-5-ПК-6; ПК-8-ПК-9; ПК-13-ПК16	ОК-1; ПК-1-ПК3; ПК-5-ПК-6; ПК-8-ПК-9; ПК-13-ПК16	ОК-1; ПК-1-ПК3; ПК-5-ПК-6; ПК-8-ПК-9; ПК-13-ПК16	ОК-1; ПК-1-ПК3; ПК-5-ПК-6; ПК-8-ПК-9; ПК-13-ПК16
Члены ГЭК	ОК-1; ПК-1; 2; 3; 4; ПК-6; ПК-8; ПК14; 15; 16			

Таблица закрепленных для оценивания компетенций за руководителем ВКР, рецензентом и членами ГЭК.

Коды	**Руководитель ВКР**	**Рецензент**	**Члены ГЭК**
ОК-1	+	+	+
ПК-1	+	+	+
ПК-2	+	+	+
ПК-3	+	+	+
ПК-4	+		
ПК-5	+	+	
ПК-6	+	+	+
ПК-7	+		
ПК-8	+	+	+
ПК-9	+	+	
ПК-10	+		
ПК-11	+		
ПК-12	+		
ПК-13	+	+	
ПК-14	+	+	+
ПК-15	+	+	+
ПК-16	+	+	+

На основании указанных выше критериев формируется итоговая оценка по ВКР (форма оценочного листа приведена в приложении 1).

Приложение №1

Оценочный лист результатов защиты выпускной квалификационной работы бакалавра

Критерии оценки	Баллы	Общекультурные компетенции: ОК1	Профессиональные компетенции					Итого
			Проектная деятельность: ПК1 - ПК4	Научно-исследовательская деятельность: ПК5 – ПК8	Контрольно-аналитическая деятельность: ПК9 – ПК10	Педагогическая деятельность: ПК11	Организационно-управленческая деятельность: ПК12 – ПК16	
Работа с литературными источниками	0-5							
Качество оформления ВКР	0-5							
Обоснованность цели ВКР во введении	0-5							
Содержательность и аргументация проведенного теоретического исследования (1 глава)	0-10							
Качество аналитической части (2 глава)	0-20							
Проработанность рекомендаций и мероприятий (3 глава)	0-15							
Оригинальность и практическая значимость предложений и рекомендаций в ВКР	0-5							
Качество доклада	0-5							
Содержание и оформление презентации	0-5							
Ответы на вопросы	0-25							
Сумма	100							
Дополнительные критерии								
Оценка руководителя ВКР								
Оценка рецензента								
Наличие публикаций и актов (справок) о внедрении								

Приложение №2

Оценочный лист руководителя ВКР
Оценка уровня сформированности компетенций
студента _____группы_____

Код компетенции	Компетенция	Показатели уровня сформированности компетенций			
		2-низкий	3-достаточный	4 выше ожидаемого	5 высокий
ОК-1	способность к абстрактному мышлению, анализу, синтезу				
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности				
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов				
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности				
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества				
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно- технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок				
ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента				
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи				
ПК-9	способность проводить аудит информационной безопасности информационных систем и объектов информатизации				
ПК-10	способность проводить аттестацию объектов информатизации по требованиям безопасности информации				

ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности				
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения				
ПК-13	способность организовать управление информационной безопасностью				
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России				
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности				
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности				

Руководитель _____

Подпись_____ «____»_____201__г.

Приложение №3

Оценочный лист рецензента ВКР
Оценка уровня сформированности компетенций
студента _____ _____группы_____

Код компетенции	Компетенция	Показатели уровня сформированности компетенций			
		2-низкий	3-достаточный	4 выше ожидаемого	5 высокий
ОК-1	способность к абстрактному мышлению, анализу, синтезу				
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности				
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов				
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества				
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно- технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок				
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи				
ПК-9	способность проводить аудит информационной безопасности информационных систем и объектов информатизации				
ПК-13	способность организовать управление информационной безопасностью				
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России				
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности				
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности				

Рецензент _____

(Ф.И.О., ученая степень, ученое звание, место работы, должность)

Подпись_____ «____»_____201__г.

Приложение №4

Оценочный лист членов ГЭК
Оценка уровня сформированности компетенций
студента _____ _____ группы_____

Код компетенции	Компетенция	Показатели уровня сформированности компетенций			
		2-низкий	3-достаточный	4 выше ожидаемого	5 высокий
ОК-1	способность к абстрактному мышлению, анализу, синтезу				
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты				
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности				
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов				
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно- технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок				
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи				
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России				
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности				
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности				

Член ГЭК_____

(Ф.И.О., ученая степень, ученое звание, место работы, должность)

Подпись_____ «____»_____201__г.

Фонд оценочных средств составлен в соответствии с требованиями ФГОС ВО по направлению 10.04.01 «Информационная безопасность»

Фонд оценочных средств составил доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры ИЗИ

Протокол № 7 от 28.12.2016 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)