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
Директор ИИТР
_____ А.А.Галкин
«_28__» _декабря____ 2016 г.

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки _Комплексная защита объектов информатизации__

Уровень высшего образования _____бакалавриат_____

Форма обучения _____очная_____

Владимир 2016

1. Цели и задачи государственной итоговой аттестации

Цель и задачи государственной итоговой аттестации (ГИА) студентов формулируются с учетом объектов и видов профессиональной деятельности, на которые ориентирована основная профессиональная образовательная программа (ОПОП) подготовки бакалавров направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации».

Государственная итоговая аттестация предназначена для определения практической и теоретической подготовленности бакалавров к выполнению профессиональных задач, установленных государственным образовательным стандартом, и продолжению образования в магистратуре.

Аттестационные испытания, входящие в состав государственной итоговой аттестации выпускника, должны полностью соответствовать основной образовательной программе высшего образования, которую он освоил за время обучения. Государственная итоговая аттестация выявляет степень усвоения студентом всех профессиональных компетенций, отнесенных к тем видам деятельности, на которые ориентирована программа бакалавриата, и его подготовленность к самостоятельной профессиональной деятельности.

Подготовка и проведение государственной итоговой аттестации базируется на закреплении полученных знаний в процессе выполнения выпускной квалификационной работы. При этом акцент делается на практическое применение полученных навыков в самостоятельной работе.

2. Виды и задачи профессиональной деятельности выпускников

Область профессиональной деятельности выпускников, освоивших программу бакалавриата, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Объектами профессиональной деятельности выпускников, освоивших программу бакалавриата, являются:

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

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу бакалавриата:

эксплуатационная;
проектно-технологическая;
экспериментально-исследовательская;
организационно-управленческая.

Выпускник, освоивший программу бакалавриата, готов решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности: **эксплуатационная деятельность:**

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

- администрирование подсистем информационной безопасности объекта; участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

проектно-технологическая деятельность:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации; проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

3. Компетенции обучающегося, формируемые в результате государственной итоговой аттестации

В соответствии с требованиями ФГОС ВО государственная итоговая аттестация обеспечивает контроль полноты формирования следующих общекультурных и профессиональных компетенций, которыми должен обладать выпускник по программе бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность».

Выпускник по направлению подготовки 10.03.01 «Информационная безопасность» с квалификацией (степенью) бакалавр в соответствие с целями основной профессиональной образовательной программы (ОПОП) и задачами профессиональной деятельности в результате освоения данной ОПОП бакалавриата должен обладать следующими компетенциями:

Состав компетенций и планируемые результаты

Коды компетенций по ФГОС*	Компетенции	Планируемые результаты
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	**знать:** основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а так же нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны основные принципы и сертификации средств защиты информации. **уметь:** использовать в практической деятельности правовые знания, анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав. **владеть:** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
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 и государства, соблюдать нормы профессиональной этики	**знать:** место и роль информационных воздействий как факторов угроз национальной безопасности, характер и содержание угроз информационного воздействия на личность, общество, государство, роль информационного противоборства в обеспечении информационной безопасности Российской Федерации, основные международные правовые акты, регулирующие уровень интенсивности информационных воздействий и их снижение в интересах информационной безопасности личности, общества и государства, методы аналитической работы в интересах оценки информационной обстановки; место и роль информационной безопасности в системе национальной безопасности Российской Федерации. **уметь:** осмысливать процессы, события и явления в России и мировом сообществе, выделять теоретические, прикладные, ценностные аспекты культурологического знания, применять их для обоснования практических решений, касающихся как повседневной жизни, так и профессиональной области **владеть:** методикой организации информационного противоборства.
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного	**знать:** иноязычную лексику, грамматику и понятия, характерные для профессиональной коммуникации: лексический минимум в объеме 4000 учебных лексических единиц общего и терминологического характера (для иностранного языка).

	взаимодействия, в том числе в сфере профессиональной деятельности	**уметь:** понимать (в процессе чтения, аудирования, перевода) и передавать (в процессе говорения, письма) иноязычную информацию в рамках профессиональной культуры: использовать знание иностранного языка в профессиональной деятельности и межличностном общении **владеть:** иностранным языком в объеме. необходимом для возможности получения информации по профессиональной тематике, и навыками устной речи: опытом применения иностранного языка в ситуациях межкультурного общения в академическом и обшепрофесснональном контексте.
ОК-8	способностью к самоорганизации и самообразованию	**знать:** различные формы и методы научно-исследовательской работы. **уметь:** анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результата этого анализа. **владеть:** навыками освоения и внедрения новых систем защиты, сопровождения систем защиты; осуществлять поиск наиболее эффективных путей обработки информации, принципами и методами защиты информации.
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	**знать:** - суть научного метода, его основные характеристики, современную естественнонаучную картину мира; - основные законы и принципы, которым подчиняется поведение разнообразных физических моделей, а также, вытекающие из этих законов следствия и возможность их применения на практике; - теоретические методы построения решения разнообразных задач по физике; -методы и принципы постановки экспериментов в физике; - основные методы компьютерной физики; - основные принципы связи физики с другими науками; **уметь:** - проводить физический анализ практических задач; - приобретать новые научные и практические знания, опираясь на методы физики; - решать разнообразные задачи по физике; - широко использовать научную, справочную литературу, интернет-информацию в области физики в проектно-конструкторской, производственно-технологической, научно-исследовательской деятельности; - формировать системный подход к принятию управленческих решений; - анализировать и формализовать задачи своей профессиональной деятельности (научно-исследовательские, экспертно-аналитические, организационно-управленческие и др.) и выбирать адекватные пути и методы для их решения; квалифицированно применять имеющийся математический аппарат; использовать математические методы и модели для решения прикладных задач; применять основные законы физики при решении прикладных задач; **владеть:** - теоретическими методами курса общей физики; - -математическим аппаратом

		соответствующим теоретическим методам курса общей физики; - -методами анализа и решения задач по физике; - -методами использования компьютера, интернет-технологий при решении задач по физике;- методикой постановки и проведения физического эксперимента; - методикой анализа и обработки результатов физического эксперимента; - методами математического описания физических явлений и процессов, методами обработки информации, представленной в различном виде; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы.
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	**знать:** - суть научного метода, его основные характеристики, современную естественнонаучную картину мира, - основные понятия математики, в том числе математического анализа, линейной алгебры, интегрального и дифференциального исчисления, рядов, теории вероятности и математической статистики, дискретной математики; - математические методы обработки экспериментальных данных. **уметь:** формировать системный подход к принятию управленческих решений, анализировать альтернативные варианты; - использовать математические методы и модели для решения прикладных задач **владеть:** методами математического описания физических явлений и процессов, методами обработки информации, представленной в различном виде; - математическим аппаратом, навыками алгоритмизации и решения основных задач в профессиональной области; - математической символикой, для выражения количественных и качественных соотношений объектов.
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	**Знать:** - основные понятия и принципы построения электронных схем и цепей; - физические явления в электронных цепях и схемах и основы теории их функционирования; - элементную базу, характеристики элементов электрических и электронных цепей и схем; - структурные и упрощенные принципиальные схемы основных типов электронных цепей и схем; методы анализа цепей постоянного и переменного токов; - принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; - принципы работы электромагнитных устройств, трансформаторов, электрических машин **Уметь:** - проводить расчеты цепей постоянного и переменного тока с применением законов электротехники; - выполнять измерения электрических параметров цепей и схем; - собирать электронные схемы различного назначения; - выбирать необходимые электрические устройства и машины применительно к конкретной задаче; проводить

		электрические измерения **Владеть:** - навыками чтения электронных схем; - методами расчета основных параметров и характеристик электрических и электронных цепей и схем; - способностью формировать законченное представление полученных при расчётах и испытаниях результатов в виде протоколов и технических отчётов с его публичной защитой; - методами проведения электрических измерений.
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	**знать:** историю возникновения направления "Информационная безопасность", развитие направления "Информационная безопасность". ОСНОВНУЮ терминологию. Основы законодательства в области информационной безопасности, основные разделы направления "Информационная безопасность", типы угроз информационной безопасности и способы их упреждения, источники угроз информационной безопасности; - теоретические основы оценки рисков и угроз, предпосылки для управления информационными рисками и угрозами, основные требования по управлению информационными рисками и угрозами, порядок оценки рисков и угроз информационной безопасности, порядок обработки рисков и угроз. **уметь:** анализировать механизмы реализации методов зашиты конкретных объектов и процессов для решения профессиональных задач, применять штатные средства зашиты и специализированные продукты для решения типовых задач, квалифицированно оценивать область применения конкретных механизмов зашиты, грамотно использовать аппаратные средства зашиты при решении практических задач; - определять источники угрозы информационной безопасности; - применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки эффективности подсистем охраны **владеть:** методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией, навыками внедрение и эксплуатации современных средств охраны, методами и средствами выявления угроз безопасности, методиками проверки защищенности с требованиями нормативных документов.
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	**знать:** основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а так же нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в

		области обеспечения защиты государственной тайны основные принципы и сертификации средств защиты информации. **уметь:** использовать в практической деятельности правовые знания, анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав. **владеть:** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
ОПК-6	способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	**знать:** опасные и вредные факторы «человек - среда обитания», методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий. **уметь:** проводить контроль параметров и уровня негативных воздействий на человека, эффективно применять средства охраны от негативных воздействий, организовывать защиту объекта активными и пассивными способами и техническими средствами, применять известные методы и средства технической охраны объектов информатизации, проводить их сравнительный анализ, обеспечивать выбор оптимальных по условиям эксплуатации и экономичности технических средств охраны объектов информатизации; анализировать и оценивать степень риска проявления факторов опасности системы «человек - среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности. **владеть:** навыками безопасного использования технических средств в профессиональной деятельности.
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**знать:** теоретические основы оценки рисков и угроз, предпосылки для управления информационными рисками и угрозами, основные требования по управлению информационными рисками и угрозами, порядок оценки рисков и угроз информационной безопасности, порядок обработки рисков и угроз. **уметь:** определять источники угрозы информационной безопасности, организовывать предпроектное обследование, разрабатывать меры защиты от выявленных угроз, выбирать и устанавливать технические средства охраны, оценивать эффективность и надежность технической охраны, применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки эффективности подсистемы технической охраны. **владеть:** профессиональной терминологией, навыками внедрение и эксплуатации современных средств технической охраны, методами и средствами выявления угроз безопасности, методиками проверки

		защищенности с требованиями нормативных документов.
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать:** методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; современные средства разработки и анализа программного обеспечения на языках высокого уровня; аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; сигналы электросвязи, принципы построения систем и средств связи; принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы схемотехники; **Уметь:** выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; **Владеть:** методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; методами расчета и инструментального контроля показателей технической защиты информации; навыками чтения электронных схем; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; профессиональной терминологией.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать:** основные понятия и методы администрирования Unix (Linux) в объеме, необходимом для практического использования операционной системы как серверной платформы основных сетевых служб (tftp, ftp, samba, http), платформы для создания АРМ разработки программного обеспечения на популярных языках высокого уровня, платформы для создания типового АРМ офисного сотрудника; - стандартные и пользовательские типы данных и методы их обработки; - принципы структурного и модульного программирования; - принципы разработки сложных программных систем, в том числе правила разработки интерфейса; - основные методы разработки машинных алгоритмов и программ, структуры данных,

		используемые для представления типовых информационных объектов; - определение, свойства, операции и правила использования указателей на переменные и функции в программе на языке высокого уровня; **Уметь:** устанавливать операционные системы Debian GNU/Linux, CentOS, Fedora, Ubuntu, FreeBSD, OpenSolaris; устанавливать дополнительное программное обеспечение как из исходных текстов, так и из официальных репозиториев дистрибутивов; писать простейшие сценарии (sh скрипты), упрощающие рутинные задачи администратора; - использовать методы абстрагирования и управления современных языков программирования для описания и решения конкретных прикладных задач; - строить формальную модель системы (подсистемы) по ее описанию в терминах предметной области; - разработать структуры информационных объектов, функционирующих в программной системе, и соответствующие им структуры данных (в том числе абстрактные); - разработать алгоритм и реализовать программу, выбрав наиболее подходящий метод и язык программирования; - разработать модульную структуру программной системы, обеспечивающие ее функциональную наполненность, и дружественный интерфейс пользователя; - использовать оптимальные методы поиска и сортировки данных; - создавать и использовать абстрактные типы данных, экспериментально (с помощью компьютера) исследовать эффективность алгоритма и программы; - индексировать данные; - хешировать данные; - анализировать существующие структуры данных на предмет оптимальности применения в конкретной задаче. **Владеть:** навыками использования пакетов систем управления виртуальными машинами (Oracle VirtualBox, VMWare); основными приемами работы с командными интерпритаторами Unix (Linux); навыками установки и базовой настройки операционных систем; - методами программирования, разработки эффективных алгоритмов решения прикладных задач; - основными методами разработки машинных алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; - разработкой алгоритмов, используя общие схемы, методы и приемы построения алгоритмов; - технологией представления разнородных данных в виде алгоритмических структур.
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	**Знать:** аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления базами данных; принципы построения информационных систем; 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; **Уметь:** формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; **Владеть:** методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам; методами расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; профессиональной терминологией
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знать:** - основы администрирования вычислительных сетей; принципы построения информационных систем; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; методы и средства контроля эффективности технической защиты информации; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы организации информационных систем в соответствии с требованиями по защите информации; - эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; - возможные действия противника, направленные на нарушение политики безопасности информации, наиболее уязвимые для атак противника элементы компьютерных систем, механизмы решения типовых задач защиты информации **Уметь:** - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - анализировать и оценивать угрозы информационной безопасности объекта; - применять

		отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;- пользоваться нормативными документами по защите информации; - охарактеризовать возможности методов обработки информации, границ их применения, оценивать точность и достоверность полученной информации, устанавливать влияние факторов на достоверность полученной информации, определять объемы хранимой информации, анализировать и оценивать угрозы информационной безопасности. **Владеть:** - методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности автоматизированным системам; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и инструментального контроля показателей технической защиты информации; - методами организации и управления деятельностью служб защиты информации на предприятии; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией. - основными методами определения затрат на информационную безопасность, структуру интеллектуальной собственности предприятий, классификацию и способы минимизации предпринимательских рисков.
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта 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-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** основные понятия и методы в области управления службой безопасности предприятия; содержание управленческой работы руководителя подразделения службы 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; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; - 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. **Уметь:** - определять информационную

		инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; - 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. **Владеть:** - навыками анализа информационной инфраструктуры информационной системы и ее безопасности; - методами выявления угроз информационной безопасности информационных систем; -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 информационной безопасности; - 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.
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**знать:** технические средства реализации информационных процессов, основные законодательные и нормативные документы по защите информации техническими средствами, правовые основы деятельности подразделений охраны, основные демаскирующие признаки объектов охраны, методы и способы технической охраны объектов информатизации и методы оценки их эффективности, основные методы исследования и диагностики технических средств охраны объектов информатизации; – состав, порядок формирования и методы оценки эффективности использования ресурсов для обеспечения информационной безопасности; – показатели и методы оценки эффективности (рентабельности) деятельности структурных подразделений обеспечения информационной безопасности предприятий (организаций);– сущность, структуру и значение экономических потерь от реализации угроз информационной

		безопасности, а также методы и способы оценки стоимости защищаемых информационных ресурсов; – о методах технико-экономического анализа и обоснования выбора проектных решений по оснащению объектов системами защиты информации и оптимизации инженерных решений. **уметь:** - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; выбирать оптимальный метод для численной реализации, эффективно применять ЭВМ для решения прикладных задач, анализировать численные результаты решения задачи; – формулировать цели и задачи по экономической оценке инженерно-технических решений в области обеспечения информационной безопасности;– проводить экономические расчеты и оценивать экономическую эффективность мероприятий по обеспечению защиты информации на предприятии (организации); – определять расходы по статьям сметы затрат на содержание структурных подразделений обеспечения информационной безопасности предприятий (организаций) **владеть:** методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; методами количественного анализа процессов обработки, поиска и передачи информации; – навыками определения экономической эффективности в области обеспечения информационной безопасности.
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**знать:** структуру систем документационного обеспечения. **уметь:** пользоваться нормативными документами по защите информации. **владеть:** типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования.
ПК-9	способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	**Знать: - б**азовый понятийный аппарат в области ИБ; - виды и состав угроз информационной безопасности; - принципы и общие методы обеспечения информационной безопасности; - основные положения государственной политики обеспечения информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой; - виды носителей защищаемой информации; - виды тайн конфиденциальной информации; - виды уязвимости защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; - каналы и методы несанкционированного доступа к конфиденциальной информации; - классификацию видов, методов и средств

		защиты информации; принципы и методы организационной защиты информации. **Уметь:** - выявлять угрозы информационной безопасности применительно к объектам защиты; - определять состав конфиденциальной информации применительно к видам тайны; - выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; - выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; - определять направления и виды защиты информации с учетом характера информации и задач по ее защите; - выполнять поиск, сбор, обработку, анализ и систематизацию информации по теме исследования; - производить выбор методов и средств решения задач исследования, разрабатывать инструментарий для проведения исследований, применять современные информационные технологии. **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 использования современных программных и аппаратных средств при проведении научно-исследовательской работы.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**знать:** основные способы представления информации с использованием математических средств, этапы метода математического моделирования, возможности применения основных математических моделей в прикладных задачах. **уметь:** использовать методы передачи, хранения и защиты информации для исследования различных явлений и процессов, в том числе: методы теории кодирования для решения задач передачи информации по каналам связи с шумами, криптографические методы защиты информации от несанкционированного доступа для передачи информации с использованием как криптосистем с секретными ключами, так и криптосистем с открытыми ключами, знать методы теории информации для решения задач передачи информации по каналам связи без шума. **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам.
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать:** - основные математические методы исследования случайных процессов; - основные теоретико-числовые методы применительно к задачам защиты информации; - 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.

		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; - 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. **Владеть:** - методами выбора основных факторов эксперимента и построения факторных планов; - методами подбора эмпирических зависимостей для экспериментальных данных; - методами оценки коэффициентов регрессионной модели эксперимента; - методами построения оптимальных планов для научно-технических экспериментов; - навыками аналитического и численного решения задач математической статистики; -методами проведения физического эксперимента при выявлении технических каналов утечки информации.
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать:** - базовые способы оценки и повышения защищенности информационных ресурсов в корпоративных информационных системах, - способы инвентаризации программных сервисов и информационных ресурсов; - ключевые точки приложения информационных атак в типовой структуре корпоративных ИС; - методы и алгоритмы реструктуризации и реинжиниринга информационных процессов в рамках корпоративной информационной инфраструктуры; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем **Уметь:** - ставить и решать типовые задачи в области оценки и повышения защищенности корпоративных ИС; - подбирать и использовать адекватные методы и средства защиты информации; – оценивать эффективность методов защиты информационных процессов экспертным путем; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; **Владеть:** - навыками аудита информационной безопасности с использованием современных программно-технических средств; - навыками проведения экспертной оценки уровня безопасности систем; - приемами тестирования уязвимостей корпоративных программно-технических сервисов, типовыми атаками на ИС предприятий; - современным аппаратом для количественной и качественной оценки

		результатов аудита, комплексами средств защиты информации; - навыками управления информационной безопасностью простых объектов.
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**Знать:** - особенности предприятия как сложного экономического объекта управления; - задачи, решаемые с использованием КИС на различных уровнях управления; - компоненты корпоративной информационной системы; - современные технологии построения КИС; - пути достижения максимальной эффективности от внедрения КИС; - принципы построения информационных систем; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - принципы организации информационных систем в соответствии с требованиями по защите информации; - 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. **Уметь:** - анализировать процессы управления на различных уровнях корпоративных систем; - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации. **Владеть:** - методами и средствами выявления угроз безопасности автоматизированным системам; - методами анализа и формализации информационных процессов объекта и связей между ними; - информацией о факторах, определяющие необходимость защиты территории и здания предприятия; - информацией о взаимодействии между субъектами, защищающими и использующими информацию ограниченного доступа; - 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.

ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать:** основные понятия и методы в области управления службой безопасности предприятия; содержание управленческой работы руководителя подразделения службы 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; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; - 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; - основные понятия, законы и модели прогнозирования принятия решений; методологию принятия управленческих решений; - параметры и условия обеспечения качества и эффективности управленческих решений в условиях рисков и неопределенностей; - особенности принятия управленческих решений для обеспечения информационной безопасности. **Уметь:** - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; - применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности. **Владеть:-** 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 информационной безопасности; - 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 разработке модели комплексной системы защиты информации.
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** - компоненты корпоративной информационной системы; - современные технологии построения КИС; современные средства проектирования и создания КИС; - пути достижения максимальной эффективности от внедрения КИС; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - принципы организации информационных систем в соответствии с требованиями по защите информации. **Уметь:** - анализировать процессы управления на различных уровнях корпоративных систем; анализировать специфику процессов управления предприятием; - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. **Владеть:** - методами и средствами выявления угроз безопасности автоматизированным системам; - методами анализа и формализации информационных процессов объекта и связей между ними; - профессиональной терминологией.

4. Требования к тематике выпускной квалификационной работы

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.

-другие тематики, отвечающие общему направлению основной образовательной программы направления 10.03.01. «Информационная безопасность» профиль «Комплексная защита объектов информатизации», рассмотренные и согласованные учебно-методическим советом выпускающей кафедры или большинством преподавательского состава на заседании кафедры.

Структурными элементами выпускной квалификационной работы являются:

- титульный лист (данный лист не нумеруется);
- бланк задания на выполнение квалификационной работы (данный лист не нумеруется);
- аннотация – краткое изложение цели работы и структуры и объема работы на русском и английском языках (лист не нумеруется);
- лист «содержание» (данный лист имеет номер 4 и содержит основной штамп, содержащий сведения: о авторе; о руководителе; о нормоконтролере; их подписи; даты подписи; название работы; шифр работы, согласно утвержденного стандарта предприятия – Владимирского Государственного университета;
- введение (одна - две страницы);
- обзор предметной области или сравнительный анализ объектов исследования или проектирования по теме работы (12-15 страниц);
- основная часть работы (35-40 страниц);
- технико-экономическое обоснование и (или) результаты внедрения работы (не более 5 страниц);
- заключение (1-2 страницы);
- список используемых источников (книг, журналов, интернет ресурсов, не менее 20 источников);
- приложение (при необходимости);
- справка об использовании результатов работы в учебном процессе или на предприятии (при наличии);

В отдельных файлах (не подшитых к работе) представляются вместе с ВКР:

– задание кафедры на работу (бланк задания приводится в приложении 1);
– аннотации на русском и английском языках;
– отзыв научного руководителя;
– рецензия.

Аннотация должна быть развернутой информацией объемом до 1200 печатных знаков, содержащей основные идеи, результаты и выводы. Изложение материала в аннотации должно быть кратким и точным. Перед аннотацией приводят ключевые слова, совокупность которых должна отображать вне контекста основное содержание научной работы. Общее количество ключевых

слов должно быть не меньшей трех и не большей десяти. Ключевые слова должны быть в именительном падеже, через запятую.

Титульный лист содержит: название образовательной организации, факультета, кафедры, графу «допущено к защите», тему ВКР, фамилию, имя и отчество студента; подпись (место для подписи) заведующего кафедрой, научного руководителя, рецензента и. студента. Внизу титульного листа: город и год написания выпускной квалификационной работы.

Пример оформления титульного листа приводится в приложении 2.

Перечень сокращений и условных обозначений приводится на отдельном листе (пример оформления перечня сокращений и условных обозначений дан в приложении 3).

Содержание включает перечисление разделов работы с указанием страницы начала каждой главы и параграфа. Главы и параграфы выпускной квалификационной работы должны быть пронумерованы. Введение, заключение, приложения не нумеруются.

Введение является вступительной частью работы, с которой начинается изложение материала, и по объему занимает примерно 3–5 страницы. Во введении раскрываются:

1) *актуальность работы*, которая определяется несколькими факторами: необходимостью дополнения теоретических построений, относящихся к изучаемому явлению; потребностью науки в новых эмпирических данных и в совершенствовании используемых методов или конкретных технологий управления по отдельным видам деятельности. Достаточно в пределах 0,5-1 страницы текста показать главное – суть проблемной ситуации, из чего и будет видна актуальность темы;

2) *степень разработанности темы* показывает уровень изученности заявленной проблематики в научной литературе, а также направления научных исследований в рамках разрабатываемой темы. Следует подробно и полно охарактеризовать конкретный вклад различных авторов, школ и направлений в разработку темы, а также очертить существующие, на взгляд автора ВКР, белые пятна в рассмотрении темы. Необходимо обосновать недостаточность разработанности темы в научных исследованиях;

3) *цель* – это желаемый конечный результат исследования, то, для чего проводится исследование, что планируется получить в итоге. Цели работы могут быть разнообразными: определение характеристики явлений, не изученных ранее, мало изученных, противоречиво изученных; выявление взаимосвязи явлений; изучение динамики явления; обобщение, выявление общих закономерностей, создание классификации, типологии; создание методики; адаптация технологий, т. е. приспособление имеющихся технологий для использования их в решении новых проблем. Достижение цели ВКР ориентирует студентов на решение выдвинутой проблемы в двух основных направлениях – теоретическом и прикладном;

4) *задачи* – это выбор путей и средств достижения цели в соответствии с выдвинутой гипотезой. Формулировки задач необходимо делать как можно более тщательно, поскольку описание их решения должно составить содержание глав бакалаврской работы;

5) *объектом* может выступать человек, процесс управления в определенной системе, феномены и результаты человеческой деятельности, порождающие проблемную ситуацию и избранные для изучения;

6) *предмет* – это всегда определенные свойства объекта, их соотношение, зависимость объекта и свойства от каких-либо условий. Характеристики предмета измеряются, определяются, классифицируются. Предметом исследования могут быть явления в целом, отдельные их стороны, аспекты и отношения между отдельными сторонами и целым. Именно на него направлено основное внимание выпускника, именно предмет исследования определяет тему работы, которая обозначается на титульном листе как ее заглавие;

7) *методология* представляет собой описание совокупности использованных в работе методов исследовательской деятельности для разработки предмета исследования, достижения его цели и решения поставленных задач;

8) *особенности структуры работы*.

Основную часть выпускной квалификационной работы составляют данные, полученные в результате исследования, их систематизация и обобщение. Основная часть обычно разбивается на две-три главы, каждая из которых, в свою очередь, подразделяется на два-три параграфа. Объем каждой главы в среднем должен составлять 15–20 страницы. В них излагаются вопросы темы. Выпускная квалификационная работа состоит из аналитической и практической частей. Содержание глав основной части работы должно соответствовать теме ВКР и полностью ее раскрывать. Главы должны показать умение автора сжато, логично и аргументированно излагать материал, представление и оформление которого должны соответствовать требованиям, предъявляемым к выпускным квалификационным работам. Все главы ВКР должны заканчиваться краткими выводами (не более 1-2 стр.), но не менее 3 выводов по главе.

Заключение является завершающей частью исследования. Это последовательное, логически стройное изложение полученных итогов и их соотношение с общей целью и конкретными задачами, поставленными и сформулированными во введении. Иными словами, в заключении студент должен показать, как выполнены указанные цели и задачи.

В заключении излагаются также основные выводы. Однако блок выводов не должен составляться путем механического суммирования выводов в конце глав или параграфов, а должен содержать итоговые результаты исследования, которые часто оформляются в виде некоторого количества пронумерованных абзацев. В заключении также проводится общая оценка существующих научных дискуссий; находят отражение авторские варианты решения конкретных вопросов, возникающих в науке и практике. Следует также показать, где и в какой форме могут быть использованы и внедрены предложения по результатам исследования. Заключительный материал желательно излагать без сносок.

Объем заключения рекомендуется в пределах не более 5-6 страниц. Список использованных источников и литературы включает перечень источников, которые были использованы при подготовке ВКР и на которые есть ссылки в основном тексте. Использованная в работе литература:

– является органической частью любой научно-исследовательской работы;

– показывает глубину и широту изучаемой темы;

– позволяет документально подтвердить достоверность и точность приводимых заимствований (таблиц, иллюстраций, фактов, текстов документов);

– характеризует степень изученности конкретной проблемы автором;

– представляет самостоятельную ценность как справочный аппарат для других исследователей;

– является простейшим библиографическим пособием.

Список должен быть озаглавлен «Список использованной литературы». Каждая библиографическая запись в списке получает порядковый номер и начинается с красной строки. В список литературы не включаются те источники, на которые нет ссылок в основном тексте и которые фактически не были использованы в процессе работы.

Объем списка должен включать не менее 20 источников специальной литературы. При написании ВКР следует ориентироваться на наиболее свежие фактические данные источников.

В качестве приложений приводятся расчетные, графические материалы (при значительном объеме вычислительных работ по ВКР); формы документов, отражающих анализ, проведенный в работе; рабочая проектная документация (положения, инструкции, формы документов и т. д.), листинги программ, а также другие материалы, использование которых в тексте перегружает ее и нарушает логическую стройность изложения. Цель приложений – избежать излишней нагрузки текста различными аналитическими, расчетными, статистическими материалами, которые не содержат основную информацию.

5. Оценочные средства для государственной итоговой аттестации

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.

6. Учебно-методическое и информационное обеспечение

а) Основная литература:

• Тельный, А.В. Технические средства охраны : практикум для вузов / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова — Владимир:2012 —139с. ISBN 978-5-9984-00300-2

• Тельный, А.В.. Инженерно-техническая защита информации. Системы охранного телевидения : учебное пособие / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир 2013 .— 143 с.

• Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6 Режим доступа: http://znanium.com/

• Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/

• Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

• Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: ISBN 978-5-9558-0310-4, Режим доступа: http://znanium.com/

• Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с. Режим доступа: http://znanium.com/

• Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.comРежим доступа: http://znanium.com/

• Мишин Д.В. Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2012 .— 94 с. ISBN 978-5-9984-0295-1.

• "Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко; под ред. А.П. Пятибратова. - 4-е изд., перераб. и доп. - М. : Финансы и статистика, 2014." - http://www.studentlibrary.ru/book/ISBN9785279032853.html 736 с.

• Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/

б) Дополнительная литература:

• Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, Режим доступа: http://znanium.com/

• Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.

• Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. ISBN 978-5-369-01450-9. Режим доступа: http://znanium.com/

• Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :

• Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: Режим доступа:

http://znanium.com/
• Файман, О.И. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2010 .— 86 с. ISBN 978-5-9984-0020-9
• Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857
• Кнауб, Л. В. Теоретико-численные методы в криптографии : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7.Режим доступа: http://znanium.com/
• Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html 256 с. ISBN 5-98003-002-6.
• Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.
• Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с. ISBN 978-5-9984-0179-A
• Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2015. - http://www.studentlibrary.ru/book/ISBN5279030139.html 224 с.
• Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С.В. Никифоров.- 2-е изд. - М. : Финансы и статистика, 2007. - http://www.studentlibrary.ru/book/ISBN9785279032808.html 224 с.

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

Нормативно-распорядительное обеспечение

1. Приказ Минобрнауки России от 29 июня 2015 г. № 636 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры».
2. ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам.
3. ГОСТ 7.32-2001. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.
4. ГОСТ 7.82-2001. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание электронных ресурсов.
5. ГОСТ 2.701-2008. Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению.
6. ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления библиографические ссылки.

7. ГОСТ Р 7.0.5-2008. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.
8. ГОСТ 2.501-2013 Единая система конструкторской документации. Правила учета и хранения.
9. ГОСТ 2.302-68 Единая система конструкторской документации. Масштабы.
10. ГОСТ 2.304-81 Единая система конструкторской документации. Шрифты чертежные.
11. ГОСТ 2.004-88 Единая система конструкторской документации. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ.
12. ГОСТ 2.104-2006 Единая система конструкторской документации. Основные надписи.
13. Р 50-77-88 Рекомендации. Единая система конструкторской документации. Правила выполнения диаграмм.
14. ГОСТ 2.301-68 Единая система конструкторской документации. Форматы.
15. ГОСТ Р 54521-2011. Статистические методы. Математические символы и знаки для применения в стандартах
16. СТП 71.3-04. Стандарт предприятия. Дипломное проектирование. Обозначение в документах выпускных квалификационных работ.

Программа государственной итоговой аттестации в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Программу государственной итоговой аттестации разработал доцент кафедры ИЗИ к.т.н.

Тельный А.В.

(ФИО, подпись)

Программа государственной итоговой аттестации рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 07 от 28.12.2016 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Программа государственной итоговой аттестации рассмотрена и одобрена на заседании учебно-методической направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Протокол № 04 от 28.12.2016 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Рабочая программа одобрена на 2017/18 учебный год

Протокол заседания кафедры № 1 от 30.08.17 года

Заведующий кафедрой д.т.н., профессор ________________________ /М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор ________________________ /М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор ________________________ /М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор ________________________ /М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
ПРОГРАММЫ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой д.т.н., профессор ________________________ /М.Ю. Монахов/__

(ФИО, подпись)