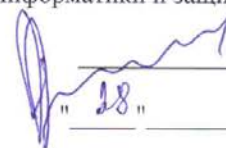


Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

УТВЕРЖДАЮ

Заведующий кафедрой
Информатики и защиты информации

 М.Ю. Монахов
" 28 " 12 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ БАКАЛАВРОВ

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки «Комплексная защита объектов информатизации»

Уровень высшего образования бакалавриат

Форма обучения очная

Владимир 2017

1. Общие положения

Государственная итоговая аттестация (ГИА) направлена на установление соответствия уровня профессиональной подготовки выпускников требованиям ФГОС ВО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации».

Целью ГИА является оценка сформированности компетенций и определение соответствия результатов освоения обучающимися ОПОП соответствующим требованиям ФГОС. ГИА по направлению 10.03.01 «Информационная безопасность» включает защиту бакалаврской выпускной квалификационной работы (ВКР).

Нормативно-правовое обеспечение ФОС для государственной итоговой аттестации бакалавров.

ФОС для государственной итоговой аттестации бакалавров 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 Минобрнауки 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 программе бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность».

Выпускник по направлению подготовки 10.03.01 «Информационная безопасность» с квалификацией (степенью) бакалавр в соответствии 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	<p>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.</p> <p>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.</p> <p>владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.</p>
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	<p>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.</p> <p>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</p> <p>владеть: методикой организации информационного противоборства.</p>
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного	<p>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).</p>

	взаимодействия, в том числе в сфере профессиональной деятельности	<p>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</p> <p>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 общепрофессиональном контексте.</p>
ОК-8	способностью к самоорганизации и самообразованию	<p>знать: различные формы и методы научно-исследовательской работы.</p> <p>уметь: анализировать мировоззренческие, социально и лично значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результата этого анализа.</p> <p>владеть: навыками освоения и внедрения новых систем защиты, сопровождения систем защиты; осуществлять поиск наиболее эффективных путей обработки информации, принципами и методами защиты информации.</p>
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	<p>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;</p> <p>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;</p> <p>владеть: - теоретическими методами курса общей физики; - математическим аппаратом</p>

		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	<p>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.</p> <p>уметь: формировать системный подход к принятию управленческих решений, анализировать альтернативные варианты; - использовать математические методы и модели для решения прикладных задач</p> <p>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.</p>
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	<p>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</p> <p>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</p>

		<p>электрические измерения</p> <p>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.</p>
ОПК-4	<p>способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p>	<p>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.</p> <p>уметь: анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач, применять штатные средства защиты и специализированные продукты для решения типовых задач, квалифицированно оценивать область применения конкретных механизмов защиты, грамотно использовать аппаратные средства защиты 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</p> <p>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.</p>
ОПК-5	<p>способность использовать нормативные правовые акты в профессиональной деятельности</p>	<p>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</p>

		<p>области обеспечения защиты государственной тайны основные принципы и сертификации средств защиты информации.</p> <p>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.</p> <p>владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.</p>
ОПК-6	<p>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</p>	<p>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.</p> <p>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.</p> <p>владеть: навыками безопасного использования технических средств в профессиональной деятельности.</p>
ОПК-7	<p>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</p>	<p>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.</p> <p>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.</p> <p>владеть: профессиональной терминологией, навыками внедрения и эксплуатации современных средств технической охраны, методами и средствами выявления угроз безопасности, методиками проверки</p>

		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	<p>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;</p> <p>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;</p> <p>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.</p>
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>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,</p>

		<p>используемые для представления типовых информационных объектов; - определение, свойства, операции и правила использования указателей на переменные и функции в программе на языке высокого уровня;</p> <p>Уметь: устанавливать операционные системы Debian GNU/Linux, CentOS, Fedora, Ubuntu, FreeBSD, OpenSolaris; устанавливать дополнительное программное обеспечение как из исходных текстов, так и из официальных репозиториях дистрибутивов; писать простейшие сценарии (sh скрипты), упрощающие рутинные задачи администратора;</p> <p>- 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.</p> <p>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.</p>
ПК-3	<p>способность администрировать подсистемы информационной безопасности объекта защиты</p>	<p>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,</p>

		<p>методы и средства контроля эффективности технической защиты информации;</p> <p>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;</p> <p>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</p>
ПК-4	<p>способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p>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</p> <p>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</p>

		<p>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.</p> <p>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.</p>
ПК-5	<p>способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p>	<p>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.</p> <p>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</p>

		<p>(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.</p> <p>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</p>
ПК-6	<p>способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p>	<p>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.</p> <p>Уметь: - определять информационную</p>

		<p>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.</p> <p>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.</p>
ПК-7	<p>способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p>	<p>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</p>

		<p>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.</p> <p>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)</p> <p>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.</p>
ПК-8	<p>способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p>знать: структуру систем документационного обеспечения.</p> <p>уметь: пользоваться нормативными документами по защите информации.</p> <p>владеть: типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования.</p>
ПК-9	<p>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</p>	<p>Знать: - базовый 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</p>

		<p>защиты информации; принципы и методы организационной защиты информации.</p> <p>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.</p> <p>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.</p>
ПК-10	<p>способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p>	<p>знать: основные способы представления информации с использованием математических средств, этапы метода математического моделирования, возможности применения основных математических моделей в прикладных задачах.</p> <p>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.</p> <p>владеть: методами и средствами выявления угроз безопасности автоматизированным системам.</p>
ПК-11	<p>способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</p>	<p>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.</p>

		<p>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.</p> <p>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.</p>
ПК-12	<p>способность принимать участие в проведении экспериментальных исследований системы защиты информации</p>	<p>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</p> <p>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;</p> <p>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</p>

		<p>результатов аудита, комплексами средств защиты информации; - навыками управления информационной безопасностью простых объектов.</p>
<p>ПК-13</p>	<p>способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>	<p>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.</p> <p>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.</p> <p>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.</p>

<p>ПК-14</p>	<p>способность организовывать работу малого коллектива исполнителей в профессиональной деятельности</p>	<p>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.</p> <p>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.</p> <p>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</p>
--------------	---	--

		<p>информацию; -методикой разработке модели комплексной системы защиты информации.</p>
<p>ПК-15</p>	<p>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</p>	<p>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.</p> <p>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.</p> <p>Владеть: - методами и средствами выявления угроз безопасности автоматизированным системам; - методами анализа и формализации информационных процессов объекта и связей между ними; - профессиональной терминологией.</p>

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 проведенного 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-4; 5; 7; 8, ОПК--1-7 ПК-1—15			
Члены ГЭК	ОК 4; ОПК-2; 3;7; ПК-2; 3; 5; 6; 7; 9; 10; 12; 13; 15			

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

Коды	Руководитель ВКР	Члены ГЭК
ОК-4	+	+
ОК-5	+	
ОК-7	+	
ОК-8	-	
ОПК-1	+	
ОПК-2	+	+
ОПК-3	+	+
ОПК-4	+	
ОПК-5	+	
ОПК-6	+	
ОПК-7	+	+
ПК-1	+	
ПК-2	+	+
ПК-3	+	+
ПК-4	+	
ПК-5	+	+
ПК-6	+	+

ПК-7	+	+
ПК-8	+	
ПК-9	+	+
ПК-10	+	+
ПК-11	+	
ПК-12	+	+
ПК-13	+	+
ПК-14	+	
ПК-15	+	+

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

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-4	способность использовать основы правовых знаний в различных сферах 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				
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности				
ОК-8	способностью к самоорганизации и самообразованию				
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач				
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач				
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач				
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации				
ОПК-5	способность использовать нормативные правовые акты в 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				
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				
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				
ПК-2	способность применять программные средства системного, прикладного и специального				

	назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты				
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
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				
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов				
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				
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов				
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации				
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности				
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				

Руководитель _____

Подпись _____ «___» _____ 201__ г.

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

Код компетенции	Компетенция	Показатели уровня сформированности компетенций			
		2- низкий	3-доста- точный	4 выше ожидае мого	5 высо кий
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности				
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач				
ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач				
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				
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты				
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
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				
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				
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации				

ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
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				

Фонд оценочных средств составлен в соответствии с требованиями ФГОС ВПО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

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

Фонд оценочных средств рассмотрен и одобрен на заседании учебно-методической
направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита
объектов информатизации»
Протокол № 4 от 28.12.16 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)