МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮЖНО - РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (НПИ) ИМЕНИ М.И. ПЛАТОВА»

УТВЕРЖДАЮ:

Проректор по ОД ЮРГПУ(НПИ)

_____ Е.М. Дьяконов

_____ 2017 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ

Направление подготовки 10.04.01 «Информационная безопасность,

направленность «Комплексная защита объектов информатизации»

Военный институт

Кафедра «Информационная безопасность»

Новочеркасск, 2017 г.

Фонд оценочных средств составлен на основании рабочего учебного плана, утвержденного Ученым советом ЮРГПУ (НПИ) протоколом № 6 от 26. 01. 2017 г.

Фонд оценочных средств составил к.в.н., доцент, заведующий кафедрой «Информационная безопасность» Баранов В.В.

Фонд оценочных средств обсужден на заседании кафедры «Информационная безопасность» «27» 01 2017 г. Протокол № 6

Заведующий кафедрой «Информационная безопасность» _____ Баранов В.В.

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, КОТОРЫМИ ДОЛЖНЫ ВЛАДЕТЬ ОБУЧАЮЩИЕСЯ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Компетенции обучающихся, установленные федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры), утвержденным приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 года № 1513:

Общекультурные компетенции	
ОК-1	Способность к абстрактному мышлению, анализу, синтезу
ОК-2	Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения
Общепрофессиональные компетенции	
ОПК-1	Способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности
ОПК-2	Способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности
Профессиональные компетенции	
Проектная деятельность:	
ПК-1	Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
ПК-2	Способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-3	Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-4	Способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
Научно-исследовательская деятельность:	
ПК-5	Способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества
ПК-6	Способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок
ПК-7	Способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента
ПК-8	Способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
Организационно-управленческая деятельность:	
ПК-12	Способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения
ПК-13	Способность организовать управление информационной безопасностью
ПК-14	Способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

ПК-15	Способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
ПК-16	Способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Номер компетенции	**Показатели оценивания компетенций** (знания и (или) навыки и (или) опыт деятельности, формируемые данной компетенций)	**Критерии оценивания компетенций на различных этапах их формирования**		
		1-й уровень «УЗНАВАНИЕ»	2-й уровень «ВОСПРОИЗВЕДЕНИЕ»	3-й уровень «ПРИМЕНЕНИЕ»
1	2	3	4	5
ОК-1	Знать: основы теории систем и системного анализа; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы образования технических каналов утечки информации. Уметь: анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности	+	+	
ОК-2	Уметь: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	+		
ОПК-1	Владеть: терминологией предметной области, в том числе на иностранном языке для решения задач профессиональной деятельности			+
ОПК-2	Уметь: применять основные методы исследования профессиональной деятельности.		+	
ПК-1	Знать: основные направления развития информационных (телекоммуникационных) технологий, средств и методов их защиты; национальные, межгосударственные и международные стандарты в области телекоммуникаций и защиты информации. Уметь: проводить мониторинг и анализ нормативных правовых актов, руководящих и методических документов уполномоченных федеральных	+	+	

1	2	3	4	5
	органов исполнительной власти в сфере защиты объектов информатизации от несанкционированного доступа; формировать политику безопасности объектов защиты			
ПК-2	Знать: нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; порядок создания автоматизированных систем в защищенном исполнении Уметь: определять перечень информации (сведений) ограниченного доступа, подлежащих защите в организации; разрабатывать проектную документацию на создание системы защиты информации в организации	+	+	
ПК-3	Знать: современные средства обеспечения информационной безопасности, их функциональные возможности; способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в информационных системах; методы защиты информации от утечки по техническим каналам и от несанкционированного доступа. Уметь: разрабатывать модели угроз безопасности информации в организации; разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации	+	+	
ПК-4	Знать: методики оценки уязвимостей объектов информатизации с точки зрения возможности несанкционированного доступа к ним; средства анализа и контроля защищенности объектов информатизации. Уметь: проводить инструментальный мониторинг защищенности объектов информатизации; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	+	+	

1	2	3	4	5
ПК-5	Знать: фундаментальные и прикладные проблемы информационной безопасности; нормативные правовые акты в области связи, информатизации и защиты информации; основные методы научных исследований	+		
ПК-6	Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности; планировать этапы выполнения НИОКР по созданию средств и систем защиты информации от несанкционированного доступа		+	
ПК-7	Знать: Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, а также наводок информативных сигналов на вспомогательные технические средства и системы, их кабельные коммуникации, а также посторонние проводники, создаваемые методом "высокочастотного облучения" основных технических средств и систем, а также за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах; порядок аттестации объектов информатизации на соответствие требованиям по защите информации Уметь: проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	+	+	
ПК-8	Уметь: организовывать подготовку научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований		+	
ПК-12	Знать: научные основы, цели, принципы, методы и технологии управленческой деятельности; нормативные правовые акты в области связи, информатизации и защиты информации Уметь: работать в коллективе, принимать управленческие решения и оценивать их эффективность	+	+	

1	2	3	4	5
ПК-13	Знать: основные нормативные документы по менеджменту информационной безопасности Уметь: применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах и сетях электросвязи; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области защиты информации	+	+	
ПК-14	Знать: основных производителей и поставщиков программных, программно-аппаратных и технических средств и систем защиты информации, технические характеристики соответствующего оборудования и программного обеспечения. Уметь: проводить анализ рынка программных, программно-аппаратных и технических средств и систем защиты информации; анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации; проводить предпроектное обследование объектов вычислительной техники и выделенных (защищаемых) помещений; разрабатывать эксплуатационную документацию на объект информатизации и средства защиты информации, а также организационно-распорядительную документацию по защите информации); организовать получение организацией лицензий на лицензируемые виды деятельности в сфере обеспечения защиты информации; организовать получение организацией сертификатов на производство товаров и оказание услуг в сфере обеспечения защиты информации;	+	+	
ПК-15	Знать: программно-аппаратные средства защиты информации и порядок ввода их в эксплуатацию; состав и содержание организационно-распорядительных документов, определяющих мероприятия по защите информации; порядок аттестации объектов информатизации на соответствие требованиям по защите информации Уметь: организовывать установку и настройку технических, программных (программно-технических)	+	+	

1	2	3	4	5
	средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации; организовывать обучение персонала использованию технических, программных (программно-технических) средств защиты информации; организовывать опытную эксплуатацию и доработку системы защиты информации; организовывать приемочные испытания системы защиты информации; организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации			
ПК-16	Владеть: навыками разработки организационно-распорядительных документов, определяющих мероприятия по защите информации (концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, положение по защите информации от утечки по техническим каналам, технический паспорт на объект информатизации (выделенное помещение), акты категорирования объектов информатизации, акты классификации автоматизированных систем, приказы, инструкции)			+

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Государственный экзамен по образовательной программе не проводится.

Государственная итоговая аттестация обучающихся проводится в форме защиты выпускной квалификационной работы в виде магистерской диссертации.

Магистерская диссертация представляет собой самостоятельную и логически завершенную выпускную квалификационную работу, связанную с решением задач того вида или видов деятельности, к которым готовится студент (проектная; научно-исследовательская; организационно-управленческая).

Требования к магистерской диссертации:

относится к разряду учебно-исследовательских работ научной направленности, выполняемых студентом самостоятельно под руководством научного руководителя на завершающей стадии обучения по образовательной программе подготовки магистра;

должна содержать совокупность результатов и научных положений, выдвигаемых автором для защиты, иметь внутреннее единство, свидетельствовать о способности автора самостоятельно вести научный поиск, используя теоретические знания и практические навыки, видеть профессиональные проблемы, уметь формулировать задачи исследования и методы их решения;

выполняется студентом по материалам, собранным им лично за период обучения и

научно-исследовательской практики.

Структура и содержание работы определяется темой магистерской диссертации.

Типовая тематика выпускных квалификационных работ (магистерских диссертаций):

1. Методика оценки состояния системы обеспечения информационной безопасности предприятия (указать тип предприятия).
2. Методика оценки состояния системы обеспечения безопасности персональных данных в организации ведомства (указать наименование ведомства).
3. Построение модели безопасности информации для компании (указать тип компании, организации)
4. Проектирование защищённой информационной системы предприятия (указать тип предприятия).
5. Комплексное обеспечение безопасности персональных данных при их обработке в информационной системе Многофункционального центра.
6. Совершенствования системы защиты информации в Государственной информационной системе (указать тип системы).
7. Разработка методических рекомендаций по подготовке и проведению аттестации объектов информатизации (название ведомства, организации).
8. Разработка методических рекомендаций по подготовке и проведению аттестации информационной системы на соответствие требований по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.
9. Разработка методических рекомендаций по подготовке к лицензированию деятельности по технической защите конфиденциальной информации организаций ведомства (наименование ведомства, организации).
10. Методика разработки модели информационной безопасности предприятия ведомства (наименование ведомства).
11. Применение систем защищенного электронного документооборота в информационных системах различных классов защищенности.
12. Проектирование системы защиты от утечек конфиденциальной информации предприятия (наименование предприятия).
13. Разработка методики анализа защищенности информационной системы предприятий ведомства (наименование ведомства).
14. Разработка лабораторного практикума по дисциплине (наименование дисциплины по ИБ).
15. Разработка подсистемы мониторинга событий защиты информации в информационной структуре предприятия (наименование предприятия).
16. Разработка инструментальной среды и организационно-методического обеспечения для проведения лабораторных занятий по дисциплине (наименование дисциплины по ИБ).
17. Разработка инструментальной среды и организационно-методического обеспечения для проведения практических занятий по дисциплине (наименование дисциплины по ИБ).
18. Разработка методических рекомендаций по организации защищенных автоматизированных рабочих мест в ИСПДн организации.
19. Разработка методических рекомендаций для оценки ущерба информационной безопасности предприятия.
20. Разработка подсистемы электронного документооборота для защищенной информационной системы предприятия.
21. Разработка практических рекомендаций по защите конфиденциальной информации в сетях беспроводного доступа предприятия.
22. Разработка рекомендаций по выбору оптимального набора программно-аппаратных средств защиты информации предприятия.
23. Разработка методических рекомендаций по оптимизации политики безопасно-

сти предприятия.

24. Разработка защищенной информационной системы предприятия на основе беспроводных технологий.

25. Разработка практических рекомендаций по организации работы службы информационной безопасности предприятия.

26. Разработка комплекса мер обеспечения информационной безопасности системы видеонаблюдения и охраны.

Научный уровень магистерской диссертации должен соответствовать программе обучения и служить свидетельством того, что ее автор научился самостоятельно вести научный поиск, видеть проблемы в области обеспечения информационной безопасности и знать наиболее общие методы и приемы их решения.

Обязательные разделы выпускной квалификационной работы:

1. Титульный лист.
2. Задание на ВКР.
3. Оглавление.
4. Введение;

Во введении проводится обоснование выбора и актуальность темы исследования, формулируются целевые установки, задачи и методологические основы диссертации. В данном разделе так же указывается объект и предмет, а также выбранный метод исследования. Раскрывается, в чем состоит теоретическая значимость и (или) практическая ценность полученных результатов. Здесь же отмечаются основные положения, которые выносятся на защиту.

5. Основную часть диссертации.

В основной части можно выделить три основных раздела.

Первый раздел – аналитический. В данном разделе проводится анализ существующего положения дел в той области, которой посвящено исследование. Выявляются «слабые стороны» объекта и предмета исследования, производится анализ и обобщение отечественного и зарубежного опыта разработок в данной области. Определяются пути решения задачи оптимизации структуры и повышения эффективности функционирования исследуемой системы (процесса). Выбираются показатели качества и критерии оценки эффективности.

Второй раздел – методический. Здесь выбирается апробированный методический аппарат расчета показателей качества и оценки эффективности объекта исследования. Формируется модель объекта исследования и последовательность проведения расчетов. В соответствии с целями и задачей исследования методический аппарат может разрабатываться полностью, или частично. В этом случае в диссертации проводится его апробация. Приводится (разрабатывается) программное обеспечение, с помощь которого будут проводиться расчеты.

Третий раздел отражает результаты исследования. Проводится синтез объекта исследования, имеющего более высокие параметры, чем у существующего (с учетом выявленных в первом разделе недостатков и несоответствий). С помощью выбранного методического аппарата и программного обеспечения осуществляется расчет численных значений показателей качества и проводится технико-экономическое обоснование выдвинутых предложений. Данные предложения должны быть строго аргументированы и критически оценены.

6. Заключение

В заключении подводятся итоги исследования, делаются обобщения и выводы, а также рассматриваются результаты исследования. В диссертации, имеющей прикладную направленность, должны приводиться сведения о практическом применении полученных результатов, а в диссертации, имеющей научную направленность, - рекомендации о применении научных выводов.

7. Перечень условных обозначений, символов и терминов (при необходимости);

8. Список использованных источников.
9. Приложения.

В приложения выносится материал, поясняющий и дополняющий основную часть исследования. Он может быть представлен в виде таблиц, рисунков, чертежей или текстовых документов.

Магистерские диссертации в соответствии с выбранной тематикой могут носить научно-исследовательскую, научно-методическую или прикладную направленность.

Основным содержанием магистерской диссертации научно-исследовательской направленности является разработка новых, или совершенствование существующих профилей защиты информации, методов (способов) обеспечения комплексной защиты объектов информатизации, моделей системы комплексной защиты информации, а также методик расчета показателей их эффективности.

Основным содержанием магистерской диссертации научно-методической направленности является создание учебно-методических материалов для проведения практических и лабораторных занятий по одному или нескольким направлениям в области информационной безопасности (техническая защита, защита от НСД, нормативно-правовое обеспечение и др.), разработка программного обеспечения для учебно-лабораторных стендов, включающих электронные аналоги измерительных средств и комплексов.

Основным содержанием магистерской диссертации прикладной направленности является проектирование и разработка систем (подсистем) обеспечения информационной безопасности конкретных объектов и организаций, а также методических рекомендаций по их развертыванию и применению, проведение технико-экономических обоснований их эффективности.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Критерии оценки при защите выпускной квалификационной работы (ВКР):

«Отлично»:

ВКР выполнена в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом;

выступление на защите структурировано, раскрыты причины выбора и актуальность темы, цель и задачи работы, предмет, объект и хронологические рамки исследования, логика выведения каждого наиболее значимого вывода; в заключительной части доклада показаны перспективы и задачи дальнейшего исследования данной темы, освещены вопросы дальнейшего применения и внедрения результатов исследования в практику. Длительность выступления соответствует регламенту;

отзыв руководителя и рецензия на ВКР не содержат замечаний;

ответы на вопросы членов экзаменационной комиссии логичны, раскрывают сущность вопроса, подкрепляются положениями монографических источников и нормативно-правовых актов, выводами и расчетами из ВКР, показывают самостоятельность и глубину изучения проблемы студентом;

широкое применение информационных технологий как в самой ВКР, так и во время выступления.

«Хорошо»:

ВКР выполнена в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии с требованиями, предъявляемыми к ней;

выступление на защите структурировано, допускаются одна-две неточности при раскрытии причин выбора и актуальности темы, целей и задач работы, предмета, объекта и хронологических рамок исследования, допускается погрешность в логике выведения одного из наиболее значимых выводов, которая устраняется в ходе дополнительных уточняющихся вопросов; в заключительной части недостаточно отражены перспективы и задачи дальнейшего исследования данной темы, вопросы дальнейшего применения и внедрения результатов исследования в практику. Длительность выступления соответствует ре-

гламенту; отзыв руководителя и рецензия на ВКР не содержат замечаний или имеют незначительные замечания;

в ответах на вопросы членов экзаменационной комиссии допущено нарушение логики, но, в целом, раскрыта сущность вопроса, тезисы выступающего подкрепляются положениями нормативно-правовых актов, выводами и расчетами из ВКР, показывают самостоятельность и глубину изучения проблемы студентом, ограниченное применение информационных технологий как в самой работе, так и во время выступления.

«Удовлетворительно»:

ВКР выполнена в соответствии с целевой установкой, но не в полной мере отвечает предъявляемым требованиям, в т.ч. по оформлению в соответствии со стандартом.

выступление на защите структурировано, допускаются неточности при раскрытии причин выбора и актуальности темы, целей и задач работы, предмета, объекта и хронологических рамок исследования, допущена грубая погрешность в логике выведения одного из наиболее значимых выводов, которая при указании на нее, устраняется с трудом; в заключительной части недостаточно отражены перспективы и задачи дальнейшего исследования данной темы, вопросы дальнейшего применения и внедрения результатов исследования в практику. Длительность выступления превышает регламент;

отзыв руководителя и рецензия на ВКР содержат замечания и перечень недостатков, которые не позволили студенту полностью раскрыть тему;

ответы на вопросы членов экзаменационной комиссии не раскрывают до конца сущности вопроса, слабо подкрепляются положениями монографических источников и нормативно-правовых актов, выводами и расчетами из ВКР, показывают недостаточную самостоятельность и глубину изучения проблемы студентом;

недостаточное применение информационных технологий как в самой ВКР, так и во время выступления. В результате процедуры защиты студент продемонстрировал понимание содержания ошибок, допущенных им при написании ВКР.

«Неудовлетворительно»:

ВКР выполнена с нарушением целевой установки, не отвечает предъявляемым требованиям, в оформлении имеются отступления от стандарта;

выступление на защите не структурировано, недостаточно раскрываются причины выбора и актуальность темы, цели и задачи работы, предмет, объект и хронологические рамки исследования, допускаются грубые погрешности в логике выведения нескольких из наиболее значимых выводов, которые, при указании на них, не устраняются; в заключительной части не отражаются перспективы и задачи дальнейшего исследования данной темы, вопросы дальнейшего применения и внедрения результатов исследования в практику. Длительность выступления значительно превышает регламент;

отзыв руководителя и/или рецензия ВКР содержат аргументированный вывод о несоответствии работы требования ФГОС ВО;

ответы на вопросы членов экзаменационной комиссии не раскрывают сущности вопроса, не подкрепляются положениями нормативно-правовых актов, выводами и расчетами из ВКР, показывают отсутствие самостоятельности и глубины изучения проблемы студентом;

информационные технологии не применяются в работе и во время выступления; в результате процедуры защиты студент демонстрирует непонимание содержания ошибок, допущенных им при написании ВКР.

Результаты защиты ВКР, замечания государственной экзаменационной комиссии обсуждаются на заседаниях кафедры и являются материалом для совершенствования кафедральной работы по организации написания, руководства и рецензирования ВКР. Защищенная ВКР остается на кафедре, по истечению установленного срока хранения передается в архив.