МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«Кабардино-Балкарский государственный университет им. Х.М. Бербекова»

Утверждаю

И.о. директора ИИЭиКТ _____Н.В. Черкесова

«__29__» ____08____2018 г.

ПРОГРАММА

государственной итоговой аттестации по направлению подготовки

10.04.01 «Информационная безопасность»

магистерская программа

«Информационная безопасность экономических систем»

Руководитель ОПОП

_____А. Г. Мустафаев

Заведующий кафедрой

информатики и

информационной безопасности

_____Т.Ю. Хаширова

Нальчик, 2018г.

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ 3
1.1.Виды государственной итоговой аттестации 3
1.2. Характеристика профессиональной деятельности выпускника магистратуры по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры) направленность программы «Информационная безопасность экономических систем» 4
1.2.1.Область профессиональной деятельности выпускника 4
1.2.2. Объекты профессиональной деятельности выпускника 5
1.2.3. Виды профессиональной деятельности выпускника 5
1.2.4. Задачи профессиональной деятельности выпускника 5
2. Требования к результатам освоения программы магистратуры 7
3. Требования к государственному экзамену 13
3.1. Вопросы государственного экзамена 13
3.2. Литература 19
3.3. Критерии и шкалы оценивания 20
4 Требования к выпускной квалификационной работе 21
4.1. Общие требования к выпускной квалификационной работе магистра. 21
4.2. Критерии и шкалы оценивания ВКР 23

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Виды государственной итоговой аттестации

Настоящая программа разработана на основе Федерального закона Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 5 апреля 2017 г. №301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры», приказа Министерства образования и науки Российской Федерации от 29 июля 2015 г. № 636 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», приказа Министерства образования и науки Российской Федерации от 09 февраля 2016 г. № 86 «О внесении изменений в Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Министерства образования и науки Российской Федерации от 29 июня 2015 г. № 636», приказа Министерства образования и науки Российской Федерации от 28 апреля 2016 г. № 502 «О внесении изменений в Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата. программам специалитета, программам магистратуры, утвержденный приказом Министерства образования и науки Российской Федерации от 29 июня 2015 г. № 636», федеральных государственных образовательных стандартов высшего образования, Устава Кабардино-Балкарского государственного университета им. Х.М. Бербекова и иных нормативных правовых актов.

Освоение образовательной программы высшего образования 10.04.01 Информационная безопасность (уровень магистратуры) завершается государственной итоговой аттестацией, которая включает:

- Подготовку к сдаче и сдачу государственного экзамена;
- защиту выпускной квалификационной работы, включая подготовку к защите и процедуру защиты.

Целью государственной итоговой аттестации является установление уровня подготовленности обучающегося, осваивающего основную образовательную программу по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры) к выполнению профессиональных задач и соответствия его подготовки требованиям ФГОС и ОПОП по направлению подготовки, разработанной на основе ФГОС.

Обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные общекультурные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

1.2. Характеристика профессиональной деятельности выпускника магистратуры по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры) направленность программы «Информационная безопасность экономических систем»

1.2.1.Область профессиональной деятельности выпускника

Область профессиональной деятельности выпускников, освоивших программу магистратуры, включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности и защиты информации.

1.2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускников, освоивших программу магистратуры, являются:

- фундаментальные и прикладные проблемы информационной безопасности;
- объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;
- средства и технологии обеспечения информационной безопасности и защиты информации;
- экспертиза, сертификация и контроль защищенности информации и объектов информатизации;
- методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации;
- организация и управление информационной безопасностью;
- образовательный процесс в области информационной безопасности.

1.2.3. Виды профессиональной деятельности выпускника

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу магистратуры по направлению 10.04.01 Информационная безопасность:

- проектная;
- научно-исследовательская;
- организационно-управленческая.

1.2.4. Задачи профессиональной деятельности выпускника

Выпускник, освоивший программу магистратуры в соответствии с видом (видами) профессиональной деятельности, на который (которые) ориентирована программа магистратуры, должен быть готов решать следующие профессиональные задачи:

проектная деятельность:

- системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;
- обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;
- разработка программ и методик испытаний средств и систем обеспечения информационной безопасности;

научно-исследовательская деятельность:

- анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;
- разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;
- выполнение научных исследований с применением соответствующих физических и математических методов;
- подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях;

организационно-управленческая деятельность:

- организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;
- организация управления информационной безопасностью;
- организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (далее – ФСБ России), Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России);
- организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;
- разработка проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной

деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

2. Требования к результатам освоения программы магистратуры

Результаты освоения ОПОП ВО определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения, опыт и личностные качества в соответствии с задачами профессиональной деятельности.

Таблица 1

Планируемые результаты освоения основной профессиональной образовательной программы

Коды компе-тенций	**Название компетенции**	**Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника**
1	2	3
ОК	**ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ ВЫПУСКНИКА:**	
ОК-1	способность к абстрактному мышлению, анализу, синтезу	З: основные методы и технологии абстрактного мышления, анализа и синтеза; У: совершенствовать и развивать уровень абстрактного мышления, анализа и синтеза; использовать абстрактное мышление, анализ, синтез. В: основными методами и технологиями абстрактного мышления, анализа и синтеза; навыками разработки и реализации социальной политики безопасности объектов информатизации, на которых циркулирует информация ограниченного доступа способностью к абстрактному мышлению, анализу, синтезу.
ОК-2	Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	З: современные информационные технологии; методы приобретения с помощью информационных технологий новых знаний и умений и методы использования в практической деятельности новых знаний и умений. У: самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения. В: методологией приобретения с помощью информационных технологий новых знаний и умений.
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ ВЫПУСКНИКА:**	

Коды компе-тенций	Название компетенции	Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника
ОПК-1	способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности	З: профессиональную лексику на государственном и иностранном языке. У: использовать языковые средства в соответствии с целями и ситуацией общения; строить устное выступление и вести диалог. В: разнообразными речевыми тактиками для достижения коммуникативных целей общения на иностранном языке в профессиональной деятельности
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	З: методы научно-исследовательских и проектных работ в профессиональной деятельности У: использовать на практике умения и навыки в организации научно-исследовательских и проектных работ в профессиональной деятельности В: техниками освоения новых методов, позволяющих решать профессиональные задачи, самостоятельно использовать потенциал интегрированных знаний для освоения новых областей и совершенствования уровня своей квалификационной подготовки
ПК	**ПРОФЕССИОНАЛЬНЫЕКОМПЕТЕНЦИИ ВЫПУСКНИКА:**	
проектная деятельность		
ПК-1	Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	З: способы и методы анализа направлений развития информационно-коммуникационных технологий объекта защиты, прогнозирования эффективности функционирования систем информационной безопасности оценки затрат и рисков, создания систем информационной безопасности в соответствии со стратегией развития организации У: организовать анализ направлений развития информационно-коммуникационных технологий объекта защиты, прогнозирование эффективности функционирования систем информационной безопасности и оценку затрат и рисков, создания систем информационной безопасности в соответствии со стратегией развития организации В: навыками анализа развития информационно-коммуникационных технологий объекта защиты, прогнозирования эффективности функционирования систем информационной безопасности и оценки затрат и рисков, создания систем информационной безопасности

Коды компе-тенций	Название компетенции	Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника
ПК-2	Способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	З: методы проектирования сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты У: организовывать и осуществлять контроль за проектированием сложных комплексов управления информационной безопасностью с учетом особенностей объектов защиты В: навыками управления проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	З: принципы организации систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов У: произвести и детально обосновать выбор структуры, принципов организации, систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов В: принципами организации 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 информацион ной безопасности	З: основные стандарты и методики обеспечения защиты сетевых технологий; методы программирования защищенных сетевых технологий У: разрабатывать программы и методики испытаний и систем обеспечения информационной безопасности В: навыками программирования и методиками испытаний средств и систем обеспечения информационной безопасности
научно-исследовательская деятельность		

Коды компе-тенций	Название компетенции	Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника
ПК-5	Способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	З: специфику проблем информационной безопасности современной науки, основные истоки и возможные последствия информационных угроз современного общества У: анализировать фундаментальные и прикладные проблемы информационных технологий объекта защиты в условиях становления современного информационного общества В: навыками анализа фундаментальных и прикладных проблем информационных технологий объекта защиты, создания систем информационной безопасности
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	З: методы сбора, обработки, анализа и систематизации научно-технической информации У: выбирать методы и средства решения задачи, вырабатывать планы и программы проведения научных исследований и технических разработок В: навыками сбора и обработки информации, разработки планов и программ научных исследований
ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	З: методику проведения экспериментальных исследований защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента У: организовать экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента В: навыками организации экспериментальных исследований защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента

Коды компе-тенций	Название компетенции	Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	З: требования международных стандартов и стандартов РФ в части требований к оформлению отчетов, научных докладов и статей У: обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи В: методами стандартизованного оформления научно- технические отчетов, обзоров, выполненных исследований научных докладов и статей
организационно-управленческая деятельность		
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	З: методы организации работы коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ У: использовать методы организации работы коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ В: методами организации работы коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ
ПК-13	способность организовать управление информационной безопасностью	З: основы построения современных системы управления информационной безопасностью У: организовать управление информационной безопасностью В: навыками организации управления информационной безопасностью

Коды компе-тенций	Название компетенции	Краткое содержание / определение и структура компетенции. Характеристика (обязательного) порогового уровня сформированности компетенции у выпускника
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	З: методы организации работы по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России У: применять методы организации работы по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения Информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России В: методами организации работы по совершенствованию, модернизации, унификации 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	З: методы организации выполнения работ по вводу в Эксплуатацию систем и средств обеспечения информационной безопасности У: применять методы организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности В: методами организации выполнения 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	З: методы разработки проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности У: применять методы разработки проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности В: методами разработки проектов организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

3. Требования к государственному экзамену

Государственный экзамен по направлению подготовки 10.04.01 Информационная безопасность является одним из видов государственных аттестационных испытаний в составе государственной итоговой аттестации выпускников КБГУ.

Экзамен проводится с целью проверки уровня и качества общепрофессиональной и специальной подготовки выпускников, позволяющий установить уровень его подготовки к выполнению профессиональных задач и соответствие его требованиям ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность.

К государственному экзамену допускаются лица, завершившие полный курс обучения по ОПОП и успешно прошедшие все предшествующие промежуточные аттестации, предусмотренные учебным планом.

Государственный экзамен проводится в сроки, предусмотренные учебным планом и графиком учебного процесса.

Программа государственного экзамена включает ключевые и практически значимые вопросы по нескольким базовым дисциплинам и обязательным дисциплинам вариативной части, определяющим направленность магистерской программы.

3.1. Вопросы государственного экзамена

1. Стандарты информационной безопасности ISO/IEC, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27005, ISO/IEC 27007, COBIT 5 forInformationSecurity, ITIL.
2. Средства управления информационной безопасностью. Ключевые средства контроля. Группы требований к информационной безопасности организации.
3. Оценка рисков нарушения безопасности. Факторы, необходимые для успешной реализации системы информационной безопасности в организации.

4. Политика информационной безопасности. Документ о политике информационной безопасности.
5. Защита от вредоносного программного обеспечения.
6. Оперирование с носителями информации и их защита.
7. Требование бизнеса по обеспечению контроля доступа.
8. Управление доступом пользователей. Обязанности пользователей.
9. Контроль сетевого доступа.
10. Слежение за доступом к системам и их использованием.
11. Безопасность в среде разработки и рабочей среде.
12. Проверка безопасности информационных систем. Аудит систем.
13. Сертификация средств защиты информации.
14. Классификация угроз и объектов защиты.
15. Методы оценки опасности угроз. Объект информатизации.
16. Классификация объектов защиты. Классификация информации.
17. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP.
18. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
19. Защита информации в локальных вычислительных сетях.
20. Защита информации при межсетевом взаимодействии.
21. Защита информации при работе с системами управления базами данных.
22. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
23. Основные требования и рекомендации по защите служебной тайны и персональных данных.
24. Основные рекомендации по защите информации, составляющей коммерческую тайну
25. Классификация технических каналов утечки информации.
26. Основные показатели технического канала утечки информации

27. Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности.
28. Биометрическая идентификация и аутентификация.
29. Требования к произвольному (дискреционному) управлению доступом.
30. Требования к принудительному (мандатному) управлению доступом.
31. Ролевое управление доступом.
32. Системы активного аудита.
33. Регуляторы безопасности и реализуемые ими цели.
34. Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами.
35. Обеспечение аутентичности IP-пакетов.
36. Обеспечение конфиденциальности сетевого трафика. Основные идеи и понятия протокола TLS.
37. Общие принципы выработки официальной политики предприятия в области информационной безопасности.
38. Подход к выработке процедур для предупреждения нарушений безопасности. Выбор регуляторов для практичной защиты.
39. Ресурсы для предупреждения нарушений безопасности. Реагирование на нарушения безопасности (процедурный уровень).
40. Классификация информации по уровню конфиденциальности. Метки документов. Хранение информации.
41. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии
42. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне. Другие типы нарушителей.
43. Нетехнические меры защиты от внутренних угроз. Психологические меры. Организационные меры.

44. Гибридные технологии firewall. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов.
45. Принципы построения окружения firewall. DMZ-сети. Конфигурация с одной DMZ-сетью. ServiceLog конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети.
46. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.
47. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNScерверы.
48. SMTP-серверы. Политика безопасности firewall. Политика firewall. Реализация набора правил firewall. Тестирование политики firewall. Возможные подходы к эксплуатации firewall.
49. Сопровождение и управление firewall. Физическая безопасность окружения firewall. Администрирование firewall.
50. Встраивание firewall в ОС. Стратегии восстановления после сбоев firewall. Возможности создания логов firewall.
51. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target.
52. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление.
53. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS.
54. Анализ, выполняемый IDS. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS. Активные действия. Сбор дополнительной информации.
55. Изменение окружения. Выполнение действия против атакующего. Пассивные действия. Тревоги и оповещения. Использование SNMP Traps. Возможности отчетов и архивирования.

56. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей.
57. Host-Based анализ уязвимостей. Network-Based анализ уязвимостей. Преимущества и недостатки систем анализа уязвимостей.
58. Цели и задачи использования IDS. Ограничения на ресурсы, существующие в организации. Возможности IDS.
59. Типы компьютерных атак, обычно определяемые IDS. Определение расположения атакующего на основе анализа выходной информации IDS
60. Компоненты DNS и понятие безопасности для них. Сервисы DNS. Инфраструктура DNS. Основные механизмы безопасности для сервисов DNS.
61. Зонная пересылка. Динамические обновления. DNS NOTIFY. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.
62. Причины уязвимости web-сервера. Планирование развертывания web-сервера. Безопасность лежащей в основе ОС.
63. Тестирование безопасности операционной системы. Список действий для обеспечения безопасности ОС, на которой выполняется web-сервер.
64. Безопасное инсталлирование и конфигурирование web-сервера. Безопасное инсталлирование web-сервера. Конфигурирование управления доступом.
65. Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера.
66. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация.

67. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS.
68. Список действий для технологий аутентификации и шифрования. Firewall прикладного уровня для web – ModSecurity. Взаимодействие ModSecurity с пакетным фильтром
69. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы. Роутер и firewall.
70. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backupweb-сервера.
71. Политики и стратегии выполнения backupweb-сервера. Поддержка тестового web-сервера.
72. Поддержка аутентичной копии web-содержимого. Восстановление при компрометации безопасности.
73. Тестирование безопасности web-серверов. Сканирование уязвимостей. Тестирование проникновения.
74. Удаленное администрирование web-сервера. Список действий для безопасного администрирования web-сервера.
75. Проблема защиты информации и информационной безопасности в системах электронного документооборота.
76. Особенности конфиденциального электронного документооборота.
77. Основные виды защищаемой информации в системе электронного документооборота, виды документов ограниченного доступа.
78. Уровни конфиденциальности информации, обрабатываемые в системах электронного документооборота.
79. Угрозы безопасности информации в системах электронного документооборота.
80. Защита от вредоносных программ систем электронного документооборота.
81. Особенности аппаратной защиты электронного обмена информацией.

82. Принципы аппаратной реализации механизмов аутентификации в электронной среде.
83. Интерфейсные средства электронного обмена информацией.
84. Техническая реализация аппаратных средств защиты информации.
85. Система контроля целостности и подтверждения достоверности электронных документов. Применение кодов аутентификации в подсистемах технологической защиты информации.
86. Эффективность аппаратных средств защиты.
87. Угрозы безопасности информации, связанные с использованием электронной почты. Основные методы и средства защиты электронной почты.
88. Особенности эксплуатации систем защищенного электронного документооборота.
89. Обеспечение контроля защиты систем электронного документооборота.
90. Применение блокчейна для создания криптовалют. Алгоритмические и архитектурные различия между наиболее популярными криптовалютами.

3.2. Литература

1. Гринберг А.С. Информационные технологии управления [Электронный ресурс]: учебное пособие для вузов / А.С. Гринберг, Н.Н. Горбачев, А.С. Бондаренко. – Электрон. текстовые данные. – М. : ЮНИТИ-ДАНА, 2017. – 478 c. – 5-238-00725-6. – Режим доступа: http://www.iprbookshop.ru/71234.html
2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] – Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – Режим доступа: http://www.iprbookshop.ru/43183.html

3. Шаньгин В.Ф. Информационная безопасность и защита информации. Издательство: Профобразование, 2017 г. http://www.iprbookshop.ru/63594.html
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Издательство: ДМК Пресс, 2012 г.
5. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.html
6. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] – Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – Режим доступа: http://www.iprbookshop.ru/43183.html
7. Шаньгин В.Ф. Информационная безопасность и защита информации. Издательство: Профобразование, 2017 г. http://www.iprbookshop.ru/63594.html
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Издательство: ДМК Пресс, 2012 г.
9. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.html

3.3. Критерии и шкалы оценивания

Члены государственной экзаменационной комиссии оценивают устные ответы обучающихся на каждый из трёх вопросов, включённых в билет, по 10 балльной шкале: по 3 балла за вопрос и дополнительный бонусный балл:

3 балла – глубокие исчерпывающие знания всего материала образовательной программы, понимание сути процессов и явлений и их взаимосвязи. Логически последовательные, полные, правильные и конкретные

ответы на все вопросы экзаменационного билета и дополнительные вопросы членов государственной экзаменационной комиссии. Активное использование в ответах на вопросы рекомендованной литературы.

2 балла – твёрдые и достаточно полные знания всего программного материала, понимание сущности и взаимосвязи рассматриваемых процессов и явлений. Последовательные, правильные, конкретные ответы на поставленные вопросы. Правильные и конкретные ответы на дополнительные вопросы членов государственной экзаменационной комиссии.

1 балл – знание основных вопросов программы. Правильные, без грубых ошибок, неточности и ошибки в ответах на поставленные вопросы, но удовлетворительное их устранение при наводящих вопросах экзаменаторов. Затруднения в ответах на дополнительные вопросы членов государственной экзаменационной комиссии.

0 – неправильные ответы на вопросы экзаменационного билета, непонимание сущности излагаемых вопросов. Неточные или неправильные ответы на дополнительные вопросы. Демонстрация в ответах на вопросы незнания материала основных дисциплин.

Устанавливаются следующие критерии оценки знаний выпускников.

«Отлично» – 8-10 баллов.

«Хорошо» – 5-7 баллов.

«Удовлетворительно» – 3-4 балла.

«Неудовлетворительно» – 0-2 балла.

4 Требования к выпускной квалификационной работе

4.1. Общие требования к выпускной квалификационной работе магистра

Выпускная квалификационная работа магистра (магистерская диссертация) является самостоятельным научным исследованием, выполненным под руководством научного руководителя. Она содержит совокупность результатов и научных положений, выдвигаемых автором для

публичной защиты, и свидетельствует о способности автора проводить самостоятельные научные исследования, опираясь на теоретические знания и практические навыки.

Основные задачи выполнения выпускной квалификационной работы:

- систематизировать, закрепить и расширить теоретические и практические знания магистранта, получить опыт применения этих знаний при решении конкретных научных и прикладных задач;
- развить и закрепить навыки самостоятельной работы и овладения методологией исследования, анализа и обработки информации, эксперимента при решении разрабатываемых в магистерской диссертации проблем и вопросов;
- определить степень сформированности компетенций, предусмотренных ФГОС, и уровень готовности выпускника магистерской программы к выполнению профессиональных задач и соответствия его подготовки требованиям ФГОС ВО.

Тема магистерской диссертации должна быть актуальной, содержать исследовательскую проблему, элементы научной новизны, отвечать требованиям времени, уровню экономического состояния и перспектив развития страны (региона). При этом она должна соответствовать направленности образовательной программы.

Тема магистерской диссертации определяется на начальном этапе обучения в магистратуре, утверждается вместе с утверждением научного руководителя не позднее, чем за шесть месяцев до начала государственной итоговой аттестации.

Характеристика, структура, объем магистерской диссертации, технические требования по оформлению и другие параметры отражены в Положении о выпускной квалификационной работе, утверждённом проректором КБГУ по УР.

Магистерская диссертация студента-выпускника, выполненная по завершению ОПОП, подлежит обязательному рецензированию, загрузке в

электронно-библиотечную систему КБГУ, проверке на заимствования и защите в государственной экзаменационной комиссии.

4.2. Критерии и шкалы оценивания ВКР

Защита выпускной квалификационной работы заканчивается выставлением итоговых оценок.

Оценка «*отлично*» выставляется за выпускную квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенную теоретическую главу, глубокий анализ, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями и т.д. Она имеет положительные отзывы научного руководителя и рецензента. При защите такой работы студент-выпускник показывает глубокое знание вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, легко и грамотно отвечает на поставленные вопросы.

Оценка «*хорошо*» выставляется за выпускную квалификационную работу, которая носит исследовательский характер, имеет грамотно изложенную теоретическую главу, достаточно подробный анализ и критический разбор практической деятельности, последовательное изложение материала с соответствующими выводами, однако не в полной мере представлены обоснованные предложения. Подобная работа имеет положительный отзыв научного руководителя и рецензента. При её защите студент-выпускник показывает знание вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на большинство поставленных вопросов.

Оценка «удовлетворительно» выставляется за выпускную квалификационную работу, которая носит исследовательский характер, имеет

теоретическую главу, базируется на практическом материале, но имеет поверхностный анализ и недостаточно критический разбор, в ней просматривается непоследовательность изложения материала, представлены необоснованные предложения. В отзывах рецензентов имеются замечания по содержанию работы и методике анализа. При её защите студент-выпускник проявляет неуверенность, показывает слабое знание вопросов темы, не всегда даёт исчерпывающие аргументированные ответы на поставленные вопросы.

Оценка «неудовлетворительно» выставляется, если аппарат исследования не продуман или отсутствует его описание, неудачно сформулированы цель и задачи, выводы носят декларативный характер, в работе не обоснована актуальность проблемы, работа не носит самостоятельного исследовательского характера; не содержит анализа и практического разбора деятельности предприятия (организации); не имеет выводов и рекомендаций; не отвечает требованиям, изложенным в методических указаниях кафедры; работа имеет вид компиляции из немногочисленных источников без оформления ссылок на них или полностью заимствована; в заключительной части не отражаются перспективы и задачи дальнейшего исследования данной темы, вопросы практического применения и внедрения результатов исследования в практику; неумение анализировать научные источники, делать необходимые выводы, поверхностное знакомство со специальной литературой; минимальный библиографический список; студент на защите не может аргументировать выводы, затрудняется отвечать на поставленные вопросы по теме либо допускает существенные ошибки; в отзывах научного руководителя и рецензента имеются существенные критические замечания; оформление не соответствует требованиям, предъявляемым к ВКР; к защите не подготовлены наглядные пособия и раздаточные материалы.