Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ

Наименование образовательной программы (специализация)	Обеспечение безопасности значимых объектов критической информационной инфраструктуры
Направление подготовки (специальность)	10.04.01 Информационная безопасность
Квалификация (степень) выпускника	Магистр
Форма обучения	очно-заочная

Курс	**Трудоемкость, кред.**	**Контактная работа, кол-во час.**	**Форма контроля**
3	6	8	ВКР

1. ЦЕЛИ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Целью итоговой государственной аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих квалификацию магистра по направлению «Информационная безопасность» и профессиональной подготовки выпускников требованиям федерального государственного образовательного стандарта.

Итоговая аттестация проводится в форме защиты выпускной квалификационной работы. К итоговой аттестации допускаются обучающиеся, выполнившие все требования ООП и успешно прошедшие промежуточные аттестационные испытания, предусмотренные учебным планом.

Место проведения итоговой аттестации: профильные предприятия, научно-исследовательские организации и учреждения, обладающие кадровым и научно-техническим потенциалом, необходимым для подготовки магистранта выпускной квалификационной работы и связанные по роду своей производственной, научно-проектной, научно-исследовательской деятельностью с проблематикой в области защиты информации.

Задачи итоговой аттестации

Проведение итоговой аттестации в форме выпускной квалификационной работы позволяет одновременно решить ряд задач:

– ориентирует каждого преподавателя и магистранта на конечный результат;

– позволяет в комплексе повысить качество учебного процесса, качество подготовки магистранта и объективность оценки подготовленности выпускников;

– систематизирует знания, умения и опыт, полученные студентами во время обучения и во время прохождения производственной практики;

– расширяет полученные знания за счет изучения новейших практических разработок и проведения исследований в профессиональной сфере;

– значительно упрощает практическую работу Государственной аттестационной комиссии при оценивании выпускника (наличие перечня профессиональных компетенций, которые находят отражение в выпускной работе).

При выполнении выпускной квалификационной работы обучающиеся должны показать свою способность и умение, опираясь на получение углубленные знания, умения и сформированные универсальные и профессиональные компетенции, самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.

Требование к выпускной квалификационной работе по направлению «Информационная безопасность» должны быть доведены до магистрантов в процессе обучения общепрофессиональных дисциплин и профессиональных модулей. Магистранты должны быть ознакомлены с содержанием, методикой выполнения и критериями оценки результатов защиты за 6 месяцев до начала итоговой аттестации.

2. ВИДЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

В результате освоения основной образовательной программы обучающийся, в соответствии с образовательным стандартом высшего образования НИЯУ МИФИ (далее – ОС НИЯУ МИФИ), проходит итоговые аттестационные испытания. Государственная итоговая аттестация выпускников проводится в соответствии с Положением об итоговой

государственной аттестации выпускников НИЯУ МИФИ. К видам итоговых аттестационных испытаний ГИА выпускников относятся:

Выпускная квалификационная работа - Защита выпускной квалификационной работы проводится с целью определения уровня освоения выпускником профессиональных компетенций, готовности выпускника к выполнению профессиональных видов деятельности, предусмотренных ОС НИЯУ МИФИ.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 – Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 – Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 – Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий
УК-2 – Способен управлять проектом на всех этапах его жизненного цикла	З-УК-2 – Знать: этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами У-УК-2 – Уметь: разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла В-УК-2 – Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта
УК-3 – Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	З-УК-3 – Знать: методики формирования команд; методы эффективного руководства коллективами; основные теории лидерства и стили руководства У-УК-3 – Уметь: разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта; сформулировать задачи членам команды для достижения поставленной цели; разрабатывать командную стратегию; применять эффективные стили руководства командой для достижения поставленной цели В-УК-3 – Владеть: умением анализировать, проектировать

	и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели; методами организации и управления коллективом
УК-4 – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-УК-4 – Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия У-УК-4 – Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия В-УК-4 – Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
УК-5 – Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	З-УК-5 – Знать: закономерности и особенности социально-исторического развития различных культур; особенности межкультурного разнообразия общества; правила и технологии эффективного межкультурного взаимодействия У-УК-5 – Уметь: понимать и толерантно воспринимать межкультурное разнообразие общества; анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия В-УК-5 – Владеть: методами и навыками эффективного межкультурного взаимодействия
УК-6 – Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-УК-6 – Знать: методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения У-УК-6 – Уметь: решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности В-УК-6 – Владеть: технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик
УКЦ-1 – Способен решать исследовательские, научно-технические и производственные задачи в условиях	З-УКЦ-1 – Знать современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы У-УКЦ-1 – Уметь подбирать наиболее релевантные

неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и технологий в цифровой среде	цифровые решения для достижения поставленных целей и задач, в том числе в условиях неопределенности В-УКЦ-1 – Владеть навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий
УКЦ-2 – Способен к самообучению, самоактуализации и саморазвитию с использованием различных цифровых технологий в условиях их непрерывного совершенствования	З-УКЦ-2 – Знать основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении У-УКЦ-2 – Уметь использовать различные цифровые технологии для организации обучения В-УКЦ-2 – Владеть навыками самообучения, самооактулизации и саморазвития с использованием различных цифровых технологий

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности	ПК-1 - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	З-ПК-1 Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и

			надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1 Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1 Владеть: основами проведения технических работ при

			аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности	ПК-2 - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	З-ПК-2 Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации;

			в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа.; У-ПК-2 Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее.;

			В-ПК-2 Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие категорированию	ПК-2.1 - Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие категорированию *Основание:* Профессиональный стандарт: 06.030, 06.034	З-ПК-2.1 Знать: Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; Принципы

			построения АСУ ТП АЭС и критические процессы, происходящие в результате штатной работы. ; У-ПК-2.1 Уметь: Выявлять и собирать сведения о критических процессах в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Определять категории значимости объектов КИИ; Формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; В-ПК-2.1 Владеть: Навыком определения критических процессов в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Навыком определения категории значимости объектов КИИ; Навыком формирования сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Способен осуществлять категорирование объектов КИИ и готовить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об	ПК-2.2 - Способен осуществлять категорирование объектов КИИ и готовить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии	З-ПК-2.2 Знать: Процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; Последствия инцидентов

	отсутствии необходимости присвоения ему одной из таких категорий	необходимости присвоения ему одной из таких категорий *Основание:* Профессиональный стандарт: 06.030, 06.032	информационной и ядерной безопасности; Процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; У-ПК-2.2 Уметь: Разрабатывать необходимые документы, содержащие сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ, по утвержденной им форме. ; В-ПК-2.2 Владеть: Навыком анализа последствий инцидентов информационной и ядерной безопасности; Навыком категорирования объектов КИИ.
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ	ПК-2.3 - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ *Основание:*	З-ПК-2.3 Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные принципы обеспечения безопасности КИИ; Основные

		Профессиональный стандарт: 06.033, 06.034	положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз для АСУ ТП на АЭС; Сущность основных физических процессов и информационных угроз в АСУ ТП в ядерном реакторе, их взаимосвязь; Требования по обеспечению безопасности значимых объектов КИИ.; У-ПК-2.3 Уметь: Планировать, разрабатывать, совершенствовать и осуществлять внедрение мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Выявлять основные информационные угрозы в АСУ ТП ядерного реактора; Проводить оценку необходимости применения средств ядерной защиты реакторов. ; В-ПК-2.3 Владеть: Навыками внедрения мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Навыками внедрения мероприятий по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности значимых объектов КИИ; Навыком

			обоснованного выбора средств защиты информации и средств ядерной защиты реакторов с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ; Навыком общего/детального анализа структуры системы безопасности значимого объекта КИИ.
организационно-управленческий			
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Способен обеспечивать безопасность значимого объекта КИИ на всех стадиях жизненного цикла	ПК-2.4 - Способен обеспечивать безопасность значимого объекта КИИ на всех стадиях жизненного цикла *Основание:* Профессиональный стандарт: 06.031, 06.033, 06.034	З-ПК-2.4 Знать: Принципы организации систем безопасности значимых объектов КИИ и обеспечения их функционирования; Критерии обеспечения ядерной безопасности значимых объектов КИИ.; У-ПК-2.4 Уметь: Анализировать данные, получаемые при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак.;

			В-ПК-2.4 Владеть: Навыком проведения перспективных исследований в области информационной безопасности и ядерной защиты объектов КИИ; Навыком совершенствования системы безопасности значимых объектов КИИ; Навыком управления (администрирования) системой безопасности и реагирования на компьютерные инциденты; Навыком проведения контроля состояния (мониторинг) критических процессов и системы безопасности значимого объекта КИИ.
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Способен планировать и организовывать предпроектное исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности	ПК-7 - Способен планировать и организовывать предпроектное исследование объектов обеспечения ИБ или объектов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.031	З-ПК-7 Знать: основные методы организационного обеспечения информационной безопасности иас; основные виды угроз безопасности операционных систем; защитные механизмы и средства обеспечения безопасности операционных систем. ; У-ПК-7 Уметь: организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; определять методы управления доступом, типы доступа и правила разграничения доступа; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; организовывать

			процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях. ; В-ПК-7 Владеть: основами формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в иас информации ограниченного доступа.
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности	ПК-8 - Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.033, 06.034	З-ПК-8 Знать: профессиональная и криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. организационно-распорядительная документация по защите информации на объекте информатизации; современные

			информационные технологии (операционные системы, базы данных, вычислительные сети); технические каналы утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. ; У-ПК-8 Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации; разрабатывать разрешительную систему

			доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации. ; В-ПК-8 Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации.
научно-исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта	ПК-3 - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3 Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите

			информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3 Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3 Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности	ПК-4 - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4 Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля

			защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4 Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных

			испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4 Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств

			защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.
педагогический			
Выполнение учебной и методической работы в образовательных организациях среднего профессионального образования, высшего образования и дополнительного профессионального образования (ДПО) по дополнительным профессиональным программам (ДПП) в должностях преподавателя и ассистента по дисциплинам направления	Способен руководить научно-исследовательской деятельностью обучающихся по программе бакалавриата (направление информационная безопасность)	ПК-5 - Способен руководить научно-исследовательской деятельностью обучающихся по программе бакалавриата (направление информационная безопасность) *Основание:* Профессиональный стандарт: 01.002	З-ПК-5 Знать: методологию научного исследования, особенности научного исследования в соответствующей отрасли знаний и (или) методология проектной деятельности, особенности проектной деятельности в соответствующей области; теоретические основы и технология научно-исследовательской и проектной деятельности ; У-ПК-5 Уметь: применять нормативные правовые акты и методические документы на всех этапах подготовки и оформления проектных, исследовательских, выпускных квалификационных работ, прохождения практики. ; В-ПК-5 Владеть: методиками оформления методики проектных, исследовательских работ обучающихся по

			программам во и (или) дпп, в том числе выпускных квалификационных работ (если их выполнение предусмотрено реализуемой образовательной программой); организацией подготовки и проведения научных конференций, конкурсов; проектных и исследовательских работ обучающихся .
Выполнение учебной и методической работы в образовательных организациях среднего профессионального образования, высшего образования и дополнительного профессионального образования (ДПО) по дополнительным профессиональным программам (ДПП) в должностях преподавателя и ассистента по дисциплинам направления	Способен методически грамотно строить планы лекционных и практических занятий по разделам учебных дисциплин и публично излагать теоретические и практические разделы учебных дисциплин в соответствии с утвержденными учебно-методическими пособиями	ПК-6 - Способен методически грамотно строить планы лекционных и практических занятий по разделам учебных дисциплин и публично излагать теоретические и практические разделы учебных дисциплин в соответствии с утвержденными учебно-методическими пособиями *Основание:* Профессиональный стандарт: 01.002	З-ПК-6 Знать: особенности организации образовательного процесса по программам бакалавриата и дпп; современные образовательные технологии профессионального образования; основы законодательства российской федерации об образовании и локальные нормативные акты, регламентирующие организацию образовательного процесса, проведение промежуточной и итоговой (итоговой государственной) аттестации обучающихся по программам бакалавриата и (или) дпп, ведение и порядок доступа к учебной и иной документации, в том числе документации, содержащей персональные данные. ; У-ПК-6 Уметь: использовать педагогически обоснованные формы, методы и приемы организации деятельности обучающихся, применять

			современные технические средства обучения и образовательные технологии, в том числе при необходимости осуществлять электронное обучение, использовать дистанционные образовательные технологии, информационно-коммуникационные технологии, электронные образовательные и информационные ресурсы; контролировать соблюдение обучающимися на занятиях требований охраны труда; анализировать и устранять возможные риски жизни и здоровью обучающихся в учебном кабинете (лаборатории, ином учебном помещении); соблюдать требования охраны труда; использовать педагогически обоснованные формы, методы, способы и приемы организации контроля и оценки освоения учебного курса, дисциплины (модуля), образовательной программы, применять современные оценочные средства, обеспечивать объективность оценки, охрану жизни и здоровья обучающихся в процессе публичного представления результатов оценивания: - соблюдать предусмотренную процедуру контроля и методику оценки; - соблюдать нормы

			педагогической этики, устанавливать педагогически целесообразные взаимоотношения с обучающимися для обеспечения. ; В-ПК-6 Владеть: проведением учебных занятий по программам бакалавриата и (или) дпп; организацией самостоятельной работы обучающихся по программам бакалавриата и дпп.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

№ п.п	Наименование экзаменационной части	Кол-во недель	Максимальный балл за раздел	Форма контроля	Индикаторы освоения компетенции
1	Выпускная квалификационная работа	4	100	ВКР	УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, УКЦ-1, УКЦ-2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
ВКР	Выпускная квалификационная работа

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание
1-4	**Выпускная квалификационная работа**
1-1	**Проведение анализа НПА**
2-2	**Решение 1 и 2 задачи ВКР**
3-3	**Решение 3 (и 4) задачи ВКР**
4-4	**Написание заключения ВКР и оформление отчета**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

2. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Москва: НИЯУ МИФИ, 2013

3. 004 К65 Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

4. 004 Д84 Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2015

5. ЭИ З-31 Криптографические методы защиты информации : учебник для вузов, Москва: Юрайт, 2022

6. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

7. 004 О-75 Основы управления информационной безопасностью Кн.1, Москва: Горячая линия - Телеком, 2018

8. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Москва: НИЯУ МИФИ, 2015

9. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

10. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Москва: НИЯУ МИФИ, 2018

11. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Москва: НИЯУ МИФИ, 2018

12. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Москва: НИЯУ МИФИ, 2018

13. 004 М 60 Технические, организационные и кадровые аспекты управления информационной безопасностью КН.4 , Москва: Горячая линия - Телеком, 2017

14. ЭИ М 60 Управление информационной безопасностью : Конспект лекций. Учебное пособие, Москва: НИЯУ МИФИ, 2020

15. 004 М 60 Управление рисками информационной безопасности Кн.2 , Москва: Горячая линия - Телеком, 2017

16. 004 В24 Введение в информационную безопасность : учебное пособие для вузов, А. А. Малюк [и др.], Москва: Горячая линия - Телеком, 2013

17. 004 М21 Введение в защиту информации в автоматизированных системах : учебное пособие для вузов, А. А. Малюк, С. В. Пазизин, Н. С. Погожин, Москва: Горячая линия-Телеком, 2011

18. 621.039 И74 Информационная безопасность систем физической защиты, учета и контроля ядерных материалов : учебное пособие для вузов, Каширин К.А., Пискарев А.С., Погожин Н.С. и др., Москва: МИФИ, 2002

19. 621.039 Б81 Физическая защита ядерных объектов : учебное пособие для вузов, П. В. Бондарев, А. В. Измайлов , А. И. Толстой ; ред. : Н. С. Погожин, Москва: МИФИ, 2008

20. 004 З-31 Стандартизация информационных технологий в аспекте защиты информации в открытых системах : , С. В. Запечников, М.: МИФИ, 2000

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

2. ЭИ Е 67 Нормативное регулирование в области защиты информации : Конспект лекций. Учебное пособие, Москва: НИЯУ МИФИ, 2021

3. ЭИ З-31 Основы интеллектуального анализа данных и машинного обучения : Конспект лекций. Учебное пособие, Москва: НИЯУ МИФИ, 2022

4. 004 З-31 Основы построения виртуальных частных сетей : учебное пособие для вузов, Москва: Горячая линия - Телеком, 2011

5. 004 Ц 75 Цифровые технологии в системе управления "Умными городами" : Научно-аналитический сборник, Москва: Научный консультант, 2022

6. 004 И74 Информационная безопасность открытых систем Т.1 Угрозы, уязвимости, атаки и подходы к защите, , : Горячая линия - Телеком, 2006

7. 004 И74 Информационная безопасность открытых систем Т.2 Средства защиты в сетях, , Москва: Горячая линия-Телеком, 2008

8. 004 М21 Защита информации : конспект лекций, А. А. Малюк, Москва: МИФИ, 2004

9. 004 М21 Основы теории защиты информации : конспект лекций, А. А. Малюк, Москва: МИФИ, 2004

10. 004 М21 Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов, А.А. Малюк, Москва: Горячая линия - Телеком, 2004

11. 004 Г37 Основы защиты информации : Учебник для вузов, В. А. Герасименко, А. А. Малюк, М.: МИФИ, 1997

12. 33 Г67 Экономика научно-технической деятельности в современных условиях : учебное пособие, Горбатов В.С., Малюк А.А., М.: МИФИ, 1989

13. 681.3 К64 Защита информации от утечки по цепям заземления средств вычислительной техники : Учеб. пособие, Кондратьев Н.А., Толстой А.И., Шакиров М.З., М.: МИФИ, 1994

14. 004 О-75 Основы информационной безопасности автоматизированных банковских систем : Учеб. пособие, Курило А.П., Милославская Н.Г., Михайлов С.Ф., Толстой А.И., М.: МИФИ, 2001

15. 65 Л12 Лабораторный практикум по курсу "Элементы автоматизации организационной деятельности" : Учеб.пособие, Под ред.Горбатова В.С.,Малюк А.А., М.: МИФИ, 1988

16. 0 З-31 Криптографические протоколы и их применение в финансовой и коммерческой деятельности : учебное пособие для вузов, С. В. Запечников, Москва: Горячая линия-Телеком, 2007

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. СПО «Терьер-3.0» (Т-211)

2. СПО «Ревизор сети 1.0» (Т-211)

3. СПО «НКВД» (Т-211)

4. СПО «Агент инвентаризации» (Т-211)

5. СПО «Фикс 2.02» (Т-211)

6. СПО «Ревизор - 2XP» (Т-211)

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. База научно-технической информации (например, ВИНИТИ РАН) ()

2. www.fstec.ru; www.gost.ru; www.fsb.ru. ()

3. http://www.scinet.cc ()

4. https://bit.spels.ru/index.php/bit ()

5. http://library.mephi.ru/ ()

https://online.mephi.ru/

http://library.mephi.ru/

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Выпускная квалификационная работа магистра (магистерская диссертация) в соответствии с ФГОС ВО должна представлять собой законченную теоретическую или экспериментальную научно-исследовательскую работу, выполненную самостоятельно, связанную с решением актуальной научно-технической или другой профильной проблемы, определяемой спецификой направления подготовки и выбранной магистерской программой направления подготовки.

1. Порядок выполнения ВКР (диссертации магистра)

1.1. ВКР выполняется студентом индивидуально под руководством научного руководителя и консультантов в соответствии с графиком, устанавливаемым кафедрой.

1.2. ВКР выполняется на базе полученных знаний и практических навыков, полученных студентом в течение всего срока обучения в вузе, прохождения практик и научно-исследовательской работы, выполняемой в магистратуре. Подготовка магистерской диссертации выполняется в течение последнего (4-го, 5-го) семестра обучения в объеме, устанавливаемом учебным планом.

1.3. Научным руководителем ВКР является штатный сотрудник либо сотрудник-совместитель кафедры, имеющий ученую степень доктора или кандидата наук. Научным руководителем ВКР, как правило, назначается сотрудник, который являлся научным руководителем научно-исследовательской работы магистранта. Научные руководители и темы ВКР утверждаются ректором университета по представлению выпускающей кафедры.

Магистранту дополнительно могут назначаться консультанты по теоретической, экспериментальной, макетной, экономической, организационно-правовой, нормативно-технической либо экономической части проекта (в зависимости от темы конкретной ВКР). Консультантами могут являться сотрудники НИЯУ МИФИ либо сотрудники сторонних организаций, в которых выполняется работа над ВКР. Консультант выдает задание по соответствующей части ВКР, контролирует его выполнение и принимает выполненное задание перед предъявлением студентом ВКР научному руководителю.

В случае, если основным местом выполнения ВКР является сторонняя организация, студенту обязательно назначается консультант по практической (теоретической и практической) части ВКР из числа сотрудников этой организации, имеющих высшее образование. В этом случае на кафедру должно быть представлено письмо, заверенное печатью организации, о согласии принять студента для выполнения ВКР с указанием фамилии, имени, отчества (полностью) и должности консультанта, его контактного телефона и адреса электронной почты.

1.4. Задание на выполнение ВКР должно быть согласовано и подписано студентом, консультантами и научным руководителем. Заполненный бланк задания студент предъявляет для утверждения зам. зав. каф. по учебной работе. Смена утвержденной темы ВКРи и научного руководителя не допускается.

1.5. В установленные кафедрой сроки на кафедре проводится предварительная защита (предзащита) ВКР. Для предзащиты ВКРй кафедра проводит заседание учебно-методического совета.

На предзащиту должны быть представлены следующие материалы:

1) полностью оформленное «Задание на выполнение ВКР (диссертации магистра»;

2) предварительный вариант ВКР, оформленный в соответствии с установленными требованиями (изложены в п. 2 настоящего документа), имеющий согласующую подпись научного руководителя;

3) копия ВКР в электронном виде (файл в формате DOC или RTF);

4) проект текста доклада, подписанный студентом и имеющий согласующую подпись научного руководителя;

5) проект иллюстративного материала, который предполагается использовать при защите ВКР;

6) сведения о предполагаемом рецензенте ВКР: фамилия, имя, отчество (полностью), место работы, должность, ученая степень, ученое звание;

7) действующие образцы программно-технических средств, созданных в ходе выполнения выпускной квалификационной работы (если имеются);

8) копии публикаций по теме ВКР: учебных пособий, научных статей, тезисов докладов на конференциях.

Предзащита каждой работы состоит из доклада автора работы (не более 10 мин.) и ответов на вопросы членов комиссии.

В докладе рекомендуется отразить:

а) развернутое наименование темы проекта, область его приложения и актуальность, постановку задачи проекта, включая требования к разрабатываемым решениям (изделиям, продуктам и т.п.);

б) состояние исследуемого (разрабатываемого) вопроса на основе обзора литературных источников;

в) анализ и обоснование выбранных методов и средств решения поставленной задачи;

г) формулировку главных научных и инженерных вопросов проекта, подвергшихся исследованию и разработке;

д) основные выводы по проектированию, оценку их теоретической и практической значимости.

В заключительной части доклада, которая строится по тексту «Заключения» ВКР, целесообразно перечислить общие выводы из ее текста (не повторяя более частные обобщения, содержащиеся в разделах основной части ВКР) и собрать воедино основные рекомендации, выработанные в процессе работы над ВКР.

При подготовке текста доклада следует учитывать, что продолжительность доклада на заседании ГАК не может превышать 20 минут.

Доклад должен сопровождаться демонстрацией иллюстративных материалов в виде презентации в формате Power Point, предназначенной для показа через проектор (из расчета приблизительно 1 слайд на 1 минуту доклада).

Если в ходе выполнения ВКР студентом были разработаны действующие образцы программно-технических средств, их работа может быть продемонстрирована комиссии кафедры на предзащите (на защите в ГАК демонстрация их работы не проводится).

Комиссия выдает рекомендации по доработке ВКР и иллюстративного материала к защите ВКР в ГАК, а также назначает рецензента ВКР.

2. Требования к оформлению ВКР

2.1. Структура и оформление ВКР должны соответствовать основным требованиям стандарта ГОСТ 7.32-2017 – «Отчет о научно-исследовательской работе – Структура и правила оформления».

2.2. Структурными элементами ВКР являются:

- титульный лист;
- задание на выполнение ВКР;
- лист аннотации (в пояснительной записке имеет заголовок «Реферат»);
- содержание;
- определения;
- обозначения и сокращения;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения.

Они включаются в текст диссертации строго в указанном порядке. Обязательные структурные элементы выделены полужирным шрифтом. Остальные структурные элементы включают в ВКР по усмотрению исполнителя с учетом настоящих требований и требований ГОСТ 7.32-2017.

2.3. При оформлении ВКР следует придерживаться следующих правил и рекомендаций.

Титульный лист должен соответствовать утвержденной на кафедре форме. На титульном листе должны быть подписи автора, научного руководителя ВКР, всех консультантов, (для этого форма бланка может корректироваться), рецензента и заведующего кафедрой (или его заместителя).

Заполненное «Задание на выполнение ВКР» (два листа) вшивается после титульного листа.

Лист аннотации должен содержать статистические данные о работе (количество страниц, рисунков, таблиц, количество разделов, объем работы, в том числе основной части), перечень ключевых слов и реферат.

Во введении обязательно должны быть обоснованы актуальность, теоретическая и практическая значимость работы, сформулирована цель работы и перечислены задачи, решаемые для достижения поставленной цели. Объем введения, как правило, не превышает 2 – 2,5 страниц.

Основная часть, как правило, состоит из 3 – 5 разделов, каждый из которых характеризуется логической завершенностью и при необходимости может делиться на подразделы и пункты. Первые разделы, как правило, содержат обзор рассматриваемой предметной области со ссылками на источники информации и постановку задачи работы. Далее следует изложение аналитических, теоретических и прикладных результатов, полученных лично автором в процессе выполнения работы. Заключительные разделы содержат практические аспекты работы, описание макетной, экспериментальной части, обсуждение возможностей применения полученных результатов в других работах. Рекомендуется в конце каждого раздела формулировать краткие выводы (1 – 2 абзаца) по данному разделу. Разделы основной части должны быть пронумерованы сквозной нумерацией, начиная с первого (введение к отчету и заключение не нумеруются!). Наибольший раздел не должен более, чем в 2 – 3 раза, превышать наименьший.

В заключении формулируется основной результат работы и (по пунктам) выводы по результатам выполненной работы (как правило, 3 – 5 выводов), а также указываются возможные (планируемые) пути и перспективы продолжения работы. Объем заключения, как правило, не превышает 1,5 – 2 страниц.

Диссертация магистра должна быть отпечатана шрифтом Times New Roman № 12 через 1,5 интервала на одной стороне белой бумаги формата А4. Размеры полей: сверху, снизу и слева – 20 мм, справа – 10 мм. Листы обязательно должны быть скреплены жестким соединением и пронумерованы сквозной нумерацией (кроме листов задания, которые при нумерации не учитываются). Рекомендуемый объем текстовой части выпускной квалификационной работы магистра (без учета иллюстраций, таблиц, списка литературы, оглавления и приложений) составляет 60 – 100 страниц. По тексту диссертации должны содержаться ссылки на источники информации, из которых заимствован материал. Ссылки допускаются только цифровые, на публикации, приведенные в списке использованных источников. Источники должны быть упорядочены по порядку встречаемости ссылок на них в тексте пояснительной записки.

3. Оформление документов перед защитой диссертации магистра

3.1. Защита диссертации магистра проводится на заседаниях Государственной аттестационной комиссии (ГАК). Дата сдачи студентом диссертации и всех документов ответственному секретарю ГАК устанавливается кафедрой.

3.2. Законченная диссертация, подписанная на титульном листе автором и консультантами, текст доклада и иллюстративный материал, который планируется использовать на защите, представляется студентом научному руководителю. Научный руководитель обязан дать отзыв о диссертации по установленной форме не позднее чем за один день до назначенной даты сдачи диссертации ответственному секретарю ГАК. Отзыв должен содержать:

1) оценку соответствия проекта заданию;

2) характеристику самостоятельности работы студента над проектом;

3) оценку глубины проработки темы в целом и отдельных ее частей;

4) оценку проекта по 4-х балльной системе ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно").

Руководитель может отметить в отзыве оригинальность темы проекта или методов, использованных при его выполнении, высказать рекомендации по поводу представления проекта на конкурс, выставку, опубликования в печати основных положений проекта, а также рекомендовать автора проекта для поступления в аспирантуру.

3.3. Подписанная научным руководителем диссертация (со вшитым в нее «Заданием на выполнение ВКР (диссертации магистра)»), отзыв научного руководителя и доклад представляются заведующему кафедрой (или его заместителю), который на основании изучения этих материалов и с учетом результатов предзащиты диссертации на кафедре решает вопрос о допуске студента к защите в ГАК, подписывая диссертацию на титульном листе.

В случае, когда заведующий кафедрой не считает возможным допустить студента к защите, этот вопрос рассматривается на заседании кафедры с приглашением студента и его научного руководителя. Если кафедра решает, что студент не может быть допущен к защите по вине студента, то он отчисляется из НИЯУ МИФИ.

Служебную записку со списками студентов, допущенных и не допущенных кафедрой к защите ВКР в ГАК, заведующий кафедрой (или его заместитель) передает деканавт (копию – ответственному секретарю ГАК).

3.4. По каждой ВКР кафедрой назначается рецензент. Рецензентом ВКР может быть профессор, преподаватель, сотрудник НИЯУ МИФИ, а также сотрудники научно-исследовательских и промышленных организаций, имеющие ученую степень и опыт работы по тематике проекта. Рецензентом не может быть сотрудник кафедры, которая является выпускающей для студента, а также лицо, имеющее с автором дипломного проекта совместные публикации по теме дипломного проекта.

Рецензент обязан дать рецензию по установленной форме. Рецензия на ВКР должна содержать:

- оценку соответствия проекта специальности;
- оценку глубины проработки темы в целом и отдельных ее частей;
- замечания по содержанию проекта, выявленные недостатки;
- оценку проекта по 4-х балльной системе ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно");

В рецензии наряду с положительными сторонами проекта отмечаются его недостатки, в частности, указываются отступления от логичности и грамотности изложения материала и его библиографического оформления, выявляются фактические ошибки и т.п. Если рецензент не является штатным сотрудником НИЯУ МИФИ, то его подпись должна быть заверена ответственным работником кадрового аппарата и печатью организации.

3.5. В установленный срок студент обязан сдать ответственному секретарю ГАК следующие документы:

1) диссертацию магистра, подписанную на титульном листе студентом, научным руководителем, консультантами, рецензентом и зав. кафедрой;

2) электронная копия диссертации;

3) отзыв научного руководителя;

4) рецензию на дипломный проект;

5) компакт-диск с подготовленной презентацией, на котором должны быть указана фамилия студента, контактный телефон и дата защиты; на диске должен быть только файл презентации с именем, состоящим из фамилии и инициалов студента на русском языке; дополнительно следует изготовить 15 экземпляров распечатки слайдов презентации на листах формата А4 для всех членов ГАК и принести их непосредственно на защиту (если планируется использовать иллюстративный материал в виде плакатов, то сдавать их заранее не нужно – их следует приносить непосредственно на защиту);

6) Титульная страница отчета системы Антиплагиат, подписанная студентом и научным руководителем.

Отсутствие хотя бы одного документа или одной подписи на любом документе является достаточным основанием для отказа в приеме ВКР к защите в ГАК.

С целью обеспечения надлежащего качества выполнения диссертации магистра сданные работы подлежат проверке с использованием системы «Антиплагиат». Нормальным уровнем оригинальности текста, свидетельствующим о самостоятельном выполнении работы, считается показатель не менее 70%. Студентам перед сдачей диссертации магистра ответственному секретарю ГАК рекомендуется провести самопроверку в свободно доступной версии системы «Антиплагиат» [http://www.antiplagiat.ru].

3.6. Студент, не представивший диссертацию магистра к защите в установленный срок без уважительной причины, отчисляется из НИЯУ МИФИ.

4. Защита магистерской диссертации в ГАК

4.1. Защита магистерских диссертаций проходит на открытых заседаниях ГАК (с приглашением всех желающих). К защите магистерских диссертаций деканатом допускаются студенты, полностью выполнившие весь учебный план, допущенные кафедрой к защите (в порядке, изложенном в п. 3.3) и своевременно сдавшие ответственному секретарю ГАК документы по перечню, приведенному в п. 3.5.

4.2. Устанавливается следующая процедура защиты магистерских диссертаций на заседаниях ГАК.

Секретарь ГАК приглашает на защиту очередного студента, объявляет тему магистерской диссертации, называет фамилию его научного руководителя и зачитывает представленные на этого студента документы.

Затем студенту предоставляется слово для изложения основных положений своей работы. Продолжительность доклада не может превышать 20 минут. Речь докладчика должна быть ясной, понятной и убедительной для всех членов ГАК (не только для специалистов узкого профиля, знакомых с тематикой конкретной работы). Доклад обязательно должен сопровождаться показом иллюстративного материала: плакатов или слайдов. Доклад и иллюстративные материалы должны соответствовать требованиям, изложенным в п. 1.5 настоящего документа.

По окончании доклада члены ГАК могут задать докладчику любые вопросы, касающиеся существа выполненного им проекта. Студенту следует отвечать на них четко и лаконично, проявлять скромность в оценке своих научных результатов и тактичность к задающим вопросы.

Затем секретарем ГАК зачитываются отзыв научного руководителя магистерской диссертации и рецензия. Если оценка, выставленная рецензентом, является положительной, допускается не зачитывать рецензию полностью, ограничиваясь только критическими замечаниями. Если рецензент оценил работу «неудовлетворительно», рецензия должна быть зачитана целиком. После этого студенту предоставляется слово для ответа на критические замечания, содержащиеся в рецензии. Студент должен отвечать на рецензию по существу сделанных рецензентом замечаний, принимая либо аргументированно отводя их.

Затем начинаются прения по докладу, в которых могут участвовать все присутствующие в зале. Обсуждение работы должно носить характер научной дискуссии, проходить в корректной и доброжелательной обстановке.

4.3. Результаты защиты каждой магистерской диссертации определяются оценками «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Решение об оценке принимается на закрытом заседании ГАК (после защиты всех диссертаций данного дня) открытым голосованием. При равном числе голосов голос председателя ГАК является решающим.

Все заседания ГАК протоколируются с фиксацией всех заданных вопросов, ответов, особых мнений и т. д. В протоколе указывается присвоенная квалификация, а также вид диплома (с отличием или без отличия), выдаваемого выпускнику. Результаты защиты магистерских диссертаций объявляются в день защиты, после оформления протоколов заседания ГАК.

ГАК может рекомендовать лучшие проекты к выдвижению на факультетские, институтские, отраслевые и Всероссийские конкурсы студенческих работ, к оформлению их результатов в виде статьи или доклада с последующим представлением к публикации в виде статьи в научном издании или в виде тезисов доклада на научной конференции.

Авторов наиболее интересных и глубоких проектов ГАК может рекомендовать для поступления в аспирантуру НИЯУ МИФИ по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Рекомендации для поступления в аспирантуру НИЯУ МИФИ на бюджетные места выдаются только студентам-дипломникам, получившим диплом с отличием. Рекомендация автора проекта для поступления в аспирантуру, содержащаяся в отзыве научного руководителя, не является достаточным основанием для выдачи ГАК рекомендации в аспирантуру.

4.4. Студент, получивший оценку «неудовлетворительно» при защите магистерской диссертации, отчисляется из университета. Он может быть допущен к повторной защите магистерской диссертации (не более одного раза) в течение 3 лет со дня первой защиты магистерской диссертации, для чего восстанавливается на контрактной основе на период подготовки магистерской диссертации.

4.5. Студенту, не защитившему магистерскую диссертацию в установленный срок по уважительной причине, подтвержденной документально, может быть предоставлен академический отпуск. Для этого студент в период обучения должен сдать в деканат факультета личное заявление с приложенными к нему документами, подтверждающими уважительность причины.

4.6. Магистерские диссертации на бумажном носителе и сопроводительные документы хранятся на кафедре в течение пяти лет со дня защиты. Магистерские диссертации в электронном виде хранятся в банке данных кафедры.

4.7. Дипломы о высшем образовании выдаются студентам, успешно защитившим магистерские диссертации, в студенческом отделе кадров в течение одного года со дня защиты магистерской диссертации в обмен на полностью оформленный обходной лист. По истечении этого срока невостребованные дипломы сдаются в архив.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Целью итоговой аттестации является установление уровня подготовки выпускника кафедры стратегических информационных исследований (№ 43) НОЦ "БИКС" ИИКС и факультета очно-заочного (вечернего) обучения НИЯУ МИФИ к выполнению профессиональных задач и соответствия его подготовки требованиям образовательного стандарта высшего образования ОС НИЯУ МИФИ 10.04.01.

Итоговая аттестация выпускников осуществляется на основе

– оценки содержания выпускных квалификационных работ, проводимых Государственной экзаменационной комиссией (далее по тексту ГЭК) и оформляемой протоколами ГЭК;

– решения о присвоении выпускнику квалификации (степени) магистр по направлению «Информационная безопасность» и выдаче диплома о высшем профессиональном образовании государственного образца, проводимого на основании протоколов ГЭК по положительным результатам итоговой государственной аттестации и оформляемого протоколом ГАК.

Основными функциями ГЭК являются:

– комплексная оценка уровня подготовки выпускника и определение соответствия подготовки выпускника требованиям ОС НИЯУ МИФИ 10.04.01 и уровня его подготовки с учетом критериев основной образовательной программы "Обеспечение безопасности значимых объектов критической информационной инфраструктуры", утвержденных ректором НИЯУ МИФИ;

– выявление умений и навыков применения теоретических знаний для решения конкретных научных, технических, экономических и социальных задач в области своей специальности;

– разработка рекомендаций, направленных на совершенствование подготовки студентов, на основании результатов работы государственных экзаменационных комиссий.

Выпускные квалификационные работы (ВКР) выполняются в форме магистерской диссертации, которая проводятся на базе полученных знаний и практических навыков, приобретенных магистрантом в течение всего срока обучения в вузе, прохождения практик и выполнения научно-исследовательской работы, выполняемой в магистратуре.

Защита выпускной квалифицированной работы проходит на открытом заседании ГЭК с приглашением всех желающих.

Устанавливается следующая процедура защиты дипломных проектов на заседании ГЭК.

Секретарь ГЭК вызывает на защиту очередного соискателя, объявляет тему магистерской диссертации, называет фамилию его научного руководителя и руководителя магистерской программы и подтверждает представление на выпускника следующих документов:

– справка деканата о сданных экзаменах и зачетах;

– пояснительная записка к ВКР;

– распечатка презентации ВКР;

– отзыв руководителя ВКР и руководителя магистерской программы;

– рецензия на ВКР.

Затем магистранту предоставляется время для изложения основных положений своей выпускной работы. Продолжительность доклада не должна превышать 10 минут. Речь выступающего должна быть ясной, понятной и убедительной для всех членов ГЭК (не только для специалистов узкого профиля, знакомых с тематикой конкретной работы). Доклад обязательно должен сопровождаться показом иллюстративного материала: слайдов. В процессе защиты диссертации магистрант должен продемонстрировать:

– способности к самостоятельному творческому мышлению;

– владение методами и методиками исследований, выполняемых в процессе работы;

– способность к научному анализу полученных результатов, разработке защищаемых положений и выводов, полученных в работе;

– умение оценить возможности использования полученных результатов в научной, преподавательской и практической деятельности.

По окончании доклада члены ГЭК могут задать докладчику вопросы, ка-сающиеся существа выполненной им работы. Магистранту следует отвечать на них четко и лаконично, проявлять скромность в оценке своих научных резуль-татов и тактичность к задающим вопросы.

Затем секретарем ГЭК зачитываются отзыв научного руководителя вы-пускной квалификационной работы и руководителя магистерской программы, а также рецензия. Если оценка, выставленная рецензентом за выполненную работу, является положительной, допускается не зачитывать рецензию полностью, ограничиваясь только критическими замечаниями. Если рецензент оценил работу «неудовлетворительно», рецензия должна быть зачитана целиком. После этого магистранту предоставляется слово для ответа на критические замечания, содержащиеся в рецензии. Отвечать на рецензию необходимо по существу сделанных рецензентом замечаний, принимая, либо аргументировано отводя их. В случае если магистерская диссертация имеет междисциплинарный характер или связана с тематикой

сторонней организации, где проходила научно-исследовательская работа магистранта, выпускающей кафедре предо-ставляется право приглашения научных консультантов и соруководителей по отдельным разделам работы, которые также могут давать свои отзывы.

Затем начинаются прения по докладу, в которых могут участвовать все присутствующие на защите. Обсуждение работы должно носить характер научной дискуссии, проходить в корректной и доброжелательной обстановке. Все решения комиссии оформляются протоколами, куда вносятся оценки, записываются заданные вопросы и особые мнения.

Результаты защиты ВКР определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", исходя из данных «Основных критериев оценки знаний студентов при проведении итоговой аттестации», и объявляются в тот же день после оформления в установленном порядке протоколов заседаний экзаменационных комиссий. В тех случаях, когда защита выпускной квалификационной работы признается неудовлетворительной, ГЭК устанавливает – может ли магистрант представить к повторной защите ту же работу с доработкой, определенной комиссией, или же обязан разработать новую тему, которая устанавливается кафедрой.

ГЭК может рекомендовать лучшие магистерские диссертации к выдвижению на факультетские, институтские и Всероссийские конкурсы студенческих работ, к оформлению их результатов в виде статьи или доклада с последующим представлением к публикации в виде статьи в научном издании или в виде тезисов доклада на научной конференции.

Протоколы ГЭК по защите ВКР подшиваются в личные карточки магистрантов и хранятся в архиве МИФИ.

Пояснительные записки к магистерской диссертации на бумажном носителе и сопроводительные документы хранятся на кафедре в течение пяти лет со дня защиты.

Решение о присвоении выпускнику квалификации (степени) «магистр» по направлению 10.04.01 «Информационная безопасность» и выдаче диплома о высшем образовании государственного образца принимает Государственная комиссия по положительным результатам итоговой.

Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов комиссий, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов председатель комиссии (или заменяющий его заместитель председателя комиссии) обладает правом решающего голоса.

После окончания работы государственной комиссии на основании протоколов ГЭК и оценки содержания ВКР председатель ГЭК представляет отчет об итогах работы, в котором отмечаются положительные и отрицательные стороны подготовки магистров.

Автор(ы):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):

Горбатов В.С.