Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: очная

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

для контроля освоения компетенций при проведении Государственной итоговой аттестации

Москва 2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ СОСТАВИЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

ОБЩАЯ ЧАСТЬ

Фонд компетентстно-ориентированных оценочных материалов для проведения Государственной итоговой аттестации (далее ГИА) позволяет оценить освоение компетенций:

РПК-1. Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ.

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

УК-2. Способен управлять проектом на всех этапах его жизненного цикла.

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

ОПК-2. Способен разрабатывать технический проект системы (подсистемы, компонента системы) обеспечения информационной безопасности.

ОПК-3. Способен разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности.

ОПК-4. Способен осуществлять в ручном или автоматизированном режиме сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы научных исследований и технических разработок.

ОПК-5. Способен проводить научные исследования, ставить и реализовывать физические и математические эксперименты, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

ПК-1. Способен организовывать работу по управлению функционированием СОИБ организации в соответствии с современными трендами информационной безопасности, на основе документального и инструментального анализа текущего состояния защищенности информационной инфраструктуры.

ПК-2. Способен применять математические методы и инновационные технологии при построении процедур оценки и управления рисками информационной безопасности.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ

А) Оценочные средства для сдачи государственного экзамена

Государственный экзамен учебным планом не предусмотрен.

Б) Оценочные средства для защиты ВКР

I. Перечень компетенций и контрольных вопросов для проверки результатов освоения основной образовательной программы

1. Компетенция: РПК-1 Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ

– Что их перечисленного не относится к видам производственных рисков?.

– Анализ бизнес-процессов модели хозяйствующего субъекта .

– Принцип "необходимого знания" в отношении зон безопасности подразумевает:.

– Управление производительностью информационных систем проводится с целью:.

2. Компетенция: УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

– Технологическое свойство управленческого решения - это.

– Системное свойство управленческого решения - это.

– Наиболее удачное определение управленческого решения - это.

– Юридическое свойство управленческого решения – это.

– Какое существует научно-методическое обеспечение аудита информационной безопасности информационных систем?.

– Какое существует научно-методическое обеспечение для защиты коммерческой тайны в корпоративной информационной системе?.

3. Компетенция: УК-2 Способен управлять проектом на всех этапах его жизненного цикла

– Сетевой график представляет из себя.

– Риск проекта – это.

– В результате какого вида деятельности по управлению проектом появляется сетевой график работ?.

– В результате какого вида деятельности по управлению проектом появляется диаграмма Ганта?.

– Как осуществляется разработка алгоритмов и методик оценки эффективности систем обеспечения информационной безопасности на имитационных моделях?.

4. Компетенция: УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

– Феномен коллективной безответственности состоит в том, что при увеличении численности группы индивидуальная ответственность каждого.

– Групповые нормы — это.

– Какое существует научно-методическое обеспечение для расследования инцидентов информационной безопасности информационных систем?.

– Какая существует оценка возможности создания единой методики защиты информации?.

5. Компетенция: УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

– Какое существует научно-методическое обеспечение для обучения методам и технологиям администрирования сетевого оборудования в защищенных информационных системах?.

– Какое научно-методическое обеспечение используется обучения технологиям криптографической защиты информации?.

– Формальные признаки логико-смысловых связей между элементами текста.

– Тематические лексико-грамматические средства.

– Признаки изученных грамматических явлений и особенности структуры простых и сложных предложений изучаемого иностранного языка, усложненных конструкций в структуре предложения.

6. Компетенция: УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

– Какие могут возникнуть проблемы при создания единой методологии гарантированной защиты информации для различных видов тайн?.

– Какое существует научно-методическое обеспечение для обучения технологиям тестирования безопасности прикладного программного обеспечения, используемого в WEB-сервисах?.

– Теоретические основы организационного поведения.

– Важнейшие элементы как самой организации, так и ее окружающей среды, политический контекст.

7. Компетенция: УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки

– Как разработать методику проведения теста на проникновение в информационные системы финансово-кредитных организаций на основе лучших практик?.

– Как необходимо провести сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ?.

– Теории лидерства, особенности коммуникативного пространства.

– Организационное поведение является отраслью.

– Одним из основных свойств личности является .

8. Компетенция: ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

– Безопасность при использовании мобильных программ не обеспечивается.

– Политика ИБ включает.

– Что такое IP-пакет?.

– Что такое информационная система?.

– Что понимается под показателем защищенности информационной системы?.

9. Компетенция: ОПК-2 Способен разрабатывать технический проект системы (подсистемы, компонента системы) обеспечения информационной безопасности

– Что является главным предназначением деятельности по организации информационной безопасности (ОИБ) организации?.

– Какие специфические черты и присущи в современных условиях организации информационной безопасности?.

– Что включает в себя управление рисками в общем виде?.

– Какие два основных уровня управления в концептуальном плане включает в себя СМИБ?.

– Как разрабатывается методика проведения, выявления и расследования инцидентов утечки информации в корпоративных информационных системах с использованием DLP-систем?.

10. Компетенция: ОПК-3 Способен разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности

– Моделирование каких процессов непрерывности бизнеса существует в информационной безопасности?.

– Какие существуют методы организации аналитических работ в ИТ-проекте?.

– Основные виды и процедуры обработки информации, модели и методы решения задач обработки информации.

– Предмет и цель правового регулирования в области государственной тайны.

– Как оценивается эффективность систем управления информационной безопасности на имитационных моделях?.

– Какие существуют технологии внедрения облачной электронной подписи в ЕАИС ФТС РОССИИ?.

– Какие этапы включает в себя процесс оценивания процессов СУИБ?.

– В чем заключается выполнение этапа «Реализации» цикла PDCA?.

– Что такое управление ИБ как процессный подход?.

11. Компетенция: ОПК-4 Способен осуществлять в ручном или автоматизированном режиме сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы научных исследований и технических разработок

– Пять принципов поиска нового по системе профессора П.К. Ощепкова.

– Критерии принятия риска .

– Различие между шаблонным и нешаблонным мышлением.

– Процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения.

– Методологические принципы современной науки, направления, концепции, источники знания и приемы работы с ними.

– Моделирование процессов влияет на алгоритм обработки информации на побочные электромагнитные излучения в ПЭВМ?.

– Как необходимо проводить мониторинг политики сетевой безопасности на основе модели сценариев атак?.

12. Компетенция: ОПК-5 Способен проводить научные исследования, ставить и реализовывать физические и математические эксперименты, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

– Цикл проектирования систем включает.

– Критерии принятия риска .

– Различие между шаблонным и нешаблонным мышлением.

– Современное программное и аппаратное обеспечение информационных и автоматизированных систем.

– Методы и приемы научного исследования в области проектирования и управления информационными системам.

– Методы планирования и проведения мероприятий по созданию (разработке) научного проекта для решения конкретной задачи.

– Какое научно-методическое обеспечение используется обучения технологиям защиты информационных систем от кибератак в формате “attack-defense”?.

– Какое существует научно-методическое обеспечение для применения механизмов защиты конфиденциальной речевой информации в сегменте корпоративной сети VOIP?.

13. Компетенция: ПК-1 Способен организовывать работу по управлению функционированием СОИБ организации в соответствии с современными трендами информационной безопасности, на основе документального и инструментального анализа текущего состояния защищенности информационной инфраструктуры

– Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности..

– Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов..

– Оформление, регистрация и выдача «Аттестата соответствия». .

– Что такое методология управления качеством:.

14. Компетенция: ПК-2 Способен применять математические методы и инновационные технологии при построении процедур оценки и управления рисками информационной безопасности

– Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов..

– Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная)..

– Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации..

– Раскройте содержание и порядок проведения организационных работ по использованию экспертных методов в исследованиях..

– Что называется рисками проекта? .

II. Описание шкалы оценивания

Шкала и критерии оценивания результатов защиты ВКР

№	Показатель	Шкала оценки	Критерий оценивания	Вес показателя, %
1	Оценка результатов обучения по дисциплинам (модулям) и практикам учебного плана	5 4 3	средний балл по приложению к диплому с округлением до сотых долей	
2	Доклад и демонстрационный материал	5	- доклад и демонстрационный материал охватывают весь объем ВКР, имеют логическое и четкое построение; - объем и оформление демонстрационной части соответствует установленным требованиям; - время доклада находится в рамках, установленных в Положении о	

			государственной итоговой аттестации обучающихся в ФГБОУ ВО «НИУ «МЭИ»; - обучающийся уверенно и профессионально, грамотным языком, ясно, чётко и понятно излагает содержание и суть работы	
		4	- доклад и демонстрационный материал охватывают весь объем ВКР, логичность и последовательность построения доклада несущественно нарушены; - объем и оформление демонстрационной части соответствует установленным требованиям; - время доклада несущественно выходит за рамки, установленные в Положении о государственной итоговой аттестации обучающихся в ФГБОУ ВО «НИУ «МЭИ»; - обучающийся в целом уверенно, грамотным языком, четко и понятно излагает содержание и суть работы	
		3	- доклад и демонстрационный материал охватывают большую часть объема ВКР, логичность и последовательность построения доклада нарушены; - объем и оформление демонстрационной части в целом соответствует установленным требованиям; - время доклада существенно выходит за рамки, установленные в Положении о государственной итоговой аттестации обучающихся в ФГБОУ ВО «НИУ «МЭИ»; - обучающийся излагает	

			содержание и суть работы неуверенно, нечетко, допускает ошибки в использовании профессиональной терминологии;	
		2	- доклад отличается поверхностной аргументацией основных положений; - логичность и последовательность построения доклада нарушены; - время доклада существенно выходит за рамки, установленные в Положении о государственной итоговой аттестации обучающихся в ФГБОУ ВО «НИУ «МЭИ»; - обучающийся излагает содержание и суть работы неуверенно и логически непоследовательно, показывает слабые знания предмета выпускной квалификационной работы;	
3	Отзыв руководителя о работе и рецензия	5	на основе отзыва руководителя и рецензии по решению ГЭК	
		4		
		3		
4	Ответы на вопросы членов ГЭК	5	обучающийся отвечает на вопросы грамотным языком, ясно, чётко и понятно; вопросы, задаваемые членами ГЭК, не вызывают у обучающегося существенных затруднений;	
		4	обучающийся отвечает на вопросы грамотным языком, чётко и понятно; большинство вопросов, задаваемых членами ГЭК, не вызывают у обучающегося существенных затруднений;	
		3	на поставленные вопросы обучающийся отвечает неуверенно, логически непоследовательно, допускает погрешности,	

			путается в профессиональной терминологии;	
		2	обучающийся неправильно отвечает на поставленные вопросы или затрудняется с ответом	

* – сумма весов показателей должна быть 100%

Каждый член ГЭК выставляет оценки по каждому показателю в соответствии со шкалой и критериями оценивания результатов защиты ВКР. Оценка результатов защиты ВКР каждым членом ГЭК определяется интегрально с учетом веса каждого показателя.

Итоговая оценка за защиту ВКР определяется как среднеарифметическая оценок, выставленных членами ГЭК с округлением до целого числа.