

**Министерство науки и высшего образования Российской Федерации  
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

**Программа  
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

<b>Блок</b>	<b>Блок 3 «Государственная итоговая аттестация»</b>
<b>Трудоемкость в зачетных единицах</b>	<b>4 семестр - 6 з.е.</b>
<b>Часов (всего) по учебному плану</b>	<b>216 часов</b>
<b>в том числе:</b>	
подготовка к процедуре защиты и защита выпускной квалификационной работы	4 семестр - 216 часов

**ПРОГРАММУ 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

## 1. ЦЕЛЬ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

**Цель государственной итоговой аттестации** – Подготовка специалистов, умеющих определять цели, стратегии и политику информационной безопасности корпоративных информационных систем (КИС) организации, управлять системой информационной безопасности КИС на основе требований отечественных и международных стандартов и рекомендаций, обосновывать предложения по совершенствованию системы информационной безопасности с учетом стратегических целей развития хозяйствующего субъекта.

Программа ориентирована на подготовку профессиональных специалистов в области управления информационной безопасностью, обладающих широким кругозором и получивших комплекс технических, экономических, организационных и правовых знаний. Выпускники будут обладать компетенциями в области теоретических и организационно-правовых аспектов безопасности компьютерных систем, криптографических и статистических методов защиты, типовых подсистем и решений обеспечения информационной безопасности. Магистерская программа «Управление информационной безопасностью» непосредственно связана с положениями Программы комплексного развития НИУ МЭИ в части формирования конкурентоспособных специалистов, способных внести практический вклад в инновационное развитие в сфере информационной безопасности, как в энергетической, так и в других отраслях народного хозяйства Российской Федерации..

### **Задачами государственной итоговой аттестации:**

– оценка сформированности всех компетенций, установленных образовательной программой;

– оценка освоения результатов обучения требованиям федерального государственного образовательного стандарта по направлению подготовки 10.04.01 «Информационная безопасность» и профессиональных стандартов.

## 2. РЕЗУЛЬТАТЫ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

К результатам обучения выпускника относятся следующие компетенции:

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.

### **3. ФОРМА, СРОКИ И ТРУДОЕМКОСТЬ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Общая трудоемкость государственной итоговой аттестации составляет 6 зачетных единиц, 216 часов.

Государственная итоговая аттестация представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы.

Государственная итоговая аттестация проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

Государственная итоговая аттестация является завершающей частью образовательной программы и проводится в 4 семестре после успешного прохождения промежуточной аттестации по всем дисциплинам (модулям) и практикам образовательной программы.

В государственную итоговую аттестацию входит подготовка к процедуре защиты и защита выпускной квалификационной работы.

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы.

### **4. ПОДГОТОВКА К СДАЧЕ И СДАЧА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА**

Государственный экзамен учебным планом не предусмотрен.

### **5. ТРЕБОВАНИЯ К ВЫПУСКНЫМ КВАЛИФИКАЦИОННЫМ РАБОТАМ И ПОРЯДКУ ИХ ВЫПОЛНЕНИЯ**

#### **5.1. Требования к тематике выпускных квалификационных работ**

Тематика ВКР должна соответствовать области (сфере), объекту и типам задач профессиональной деятельности, к которым готовится выпускник в рамках освоения образовательной программы.

Тематика выпускной квалификационной работы должна быть актуальной, соответствовать основным стратегическим целям развития науки и практики, современным теоретическим и практическим подходам, отражать специфику программы «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность».

Примерная тематика ВКР:

1. Проактивные системы информационной безопасности и особенности их применения в корпоративных информационных системах..

2. Применение технологий проактивной защиты SIEM при мониторинге событий информационной безопасности..
3. Моделирование и оценка уровня ПЭМИ для стационарных компьютеров организационно-техническими методами..
4. Моделирование процессов влияния алгоритмов обработки информации на побочные электромагнитные излучения в ПЭВМ..
5. Повышение уровня доверия к технологии блокчейн с использованием подхода «Общих критериев»..
6. Моделирование процессов непрерывности бизнеса в информационной безопасности..
7. Мониторинг политики сетевой безопасности на основе модели сценариев атак..
8. Научно-методическое обеспечение для обучения технологиям криптографической защиты информации..
9. Научно-методическое обеспечение обучения технологиям защиты информационных систем от кибератак в формате “attack-defense”..
10. Научно-методическое обеспечение расследования инцидентов информационной безопасности информационных систем..
11. Научно-методическое обеспечение защиты коммерческой тайны в корпоративной информационной системе..
12. Научно-методическое обеспечение применения механизмов защиты конфиденциальной речевой информации в сегменте корпоративной сети VOIP..
13. Научно-методическое обеспечение обучения технологиям создания удостоверяющего центра на основе OpenSSL..
14. Научно-методическое обеспечение обучения методам и технологиям администрирования сетевого оборудования в защищенных информационных системах..
15. Научно-методическое обеспечение аудита информационной безопасности информационных систем..
16. Научно-методическое обеспечение для обучения технологиям тестирования безопасности прикладного программного обеспечения, используемого в WEB-сервисах..
17. Разработка научно-методического обеспечения обучения администрированию безопасности операционных систем..
18. Разработка методики проведения теста на проникновение в информационные системы финансово-кредитных организаций на основе лучших практик..
19. Разработка описательных вариативных моделей объектов критической информационной инфраструктуры..
20. Оценка возможности создания единой методики защиты информации..
21. Разработка способа мониторинга безопасности IoT-устройств на базе MQTT-брокера..
22. Проблема создания единой методологии гарантированной защиты информации для различных видов тайн..
23. Технологии внедрения облачной электронной подписи в ЕАИС ФТС РОССИИ..
24. Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ..
25. Разработка методики проведения выявления и расследования инцидентов утечки информации в корпоративных информационных системах с использованием DLP-систем..
26. Разработка алгоритмов и методик оценки эффективности систем обеспечения информационной безопасности на имитационных моделях..
27. Оценка эффективности систем управления информационной безопасностью на имитационных моделях..
28. Реагирование на инциденты информационной безопасности в банковской сфере с использованием платформы «SECURITY VISION»..
29. Управление событиями информационной безопасности в SIEM-системах..

30. Использование системы мониторинга Zabbix в качестве сканера безопасности..

## 5.2. Требования к ВКР

## 5.3. Объем текстовой части

## 5.4. Объем демонстрационной части

## 5.5. Порядок выполнения ВКР

## 5.6. Процедура защиты ВКР

Защита ВКР проводится в порядке, утвержденном в Положении о государственной итоговой аттестации обучающихся в ФГБОУ ВО «НИУ «МЭИ».

## 5.7. Критерии оценки результатов защиты ВКР

К ГИА допускается обучающийся после успешного прохождения промежуточной аттестации по всем дисциплинам (модулям) и практикам образовательной программы. Сформированность компетенций, установленных образовательной программой, подтверждается результатами обучения по дисциплинам (модулям) и практикам учебного плана.

На защите ВКР оценивается способность выпускника осуществлять профессиональную деятельность не менее чем в одной области (сфере) профессиональной деятельности и решать задачи профессиональной деятельности не менее чем одного типа, установленные образовательной программой.

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	средний балл по приложению к диплому с округлением до сотых долей	
		4		
		3		
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	

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

			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 4 3	на основе отзыва руководителя и рецензии по решению ГЭК	
4	Ответы на вопросы членов ГЭК	5 4 3 2	обучающийся отвечает на вопросы грамотным языком, ясно, чётко и понятно; вопросы, задаваемые членами ГЭК, не вызывают у обучающегося существенных затруднений; обучающийся отвечает на вопросы грамотным языком, чётко и понятно; большинство вопросов, задаваемых членами ГЭК, не вызывают у обучающегося существенных затруднений; на поставленные вопросы обучающийся отвечает неуверенно, логически непоследовательно, допускает погрешности, путается в профессиональной терминологии; 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.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИА

При подготовке к ГИА студент может воспользоваться

### 6.1 Печатные и электронные издания:

1. Валдайцев, С. В. Управление инновационным бизнесом : Учебное пособие для вузов по экономическим специальностям / С. В. Валдайцев . – М. : Юнити, 2001 . – 343 с. - ISBN 5-238-00252-1 .

2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для вузов по специальности 075400 "Комплексная защита объектов информации" / А. А. Малюк . – М. : Горячая Линия-Телеком, 2004 . – 280 с. - ISBN 5-935171-97-X .

3. Саак, А. Э. Информационные технологии управления : учебник для вузов по специальности "Государственное и муниципальное управление" / А. Э. Саак, Е. В. Пахомов, В. Н. Тюшняков . – 2-е изд . – СПб. : Питер, 2010 . – 320 с. + CD-ROM . – (Учебник для вузов) . - ISBN 978-5-91180-680-4 .

4. Хорев, П. Б. Защита информационных систем : учебное пособие по курсам "Защита информации", "Методы и средства защиты компьютерной информации" по направлениям "Прикладная математика и информатика", "Информационные системы и технологии" и "Прикладная информатика" / П. Б. Хорев, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2010 . – 88 с. - ISBN 978-5-383-00546-0 .

5. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальности 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина . – М. : АКАДЕМИЯ, 2009 . – 272 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4242-8 .

6. Минзов, А. С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса : учебно-методическое пособие / А. С. Минзов, Л. М. Кунбутаев, Нац. исслед. ун-т "МЭИ", Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : ВНИИГеосистем, 2011 . – 84 с. - ISBN 978-5-8481-0083-9 .

7. Трофимова, Л. А. Методы принятия управленческих решений : учебник для бакалавров по направлению "Менеджмент" / Л. А. Трофимова, В. В. Трофимов, С.-Петерб. гос. экономич. ун-т . – М. : Юрайт, 2013 . – 335 с. – (Бакалавр. Базовый курс) . - ISBN 978-5-9916-3167-9 .

8. Бабаш, А. В. Информационная безопасность. История защиты информации в России : [учебное пособие] / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин . – М. : КДУ, 2015 . – 736 с. - ISBN 978-5-98227-928-6 .

9. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлению "Информационная безопасность" / П. Б. Хорев . – 2-е изд., испр. и доп . – М. : Форум : ИНФРА-М, 2017 . – 352 с. – (Высшее образование) . - ISBN 978-5-00091-004-7 .

10. Система менеджмента информационной безопасности ГОСТ Р ИСО/МЭК 27001-2006 (проекты документов) : [учебно-методическое пособие] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Р. А. Сябаев, М-во образования и науки Рос. Федерации, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИгеосистем, 2019 . – 98 с. - Авт. указаны на обороте тит. л. - ISBN 978-5-8481-0234-5 .

11. Теория и практика принятия управленческих решений : учебник для обучающихся по программам высшего образования направления 38.04.04 "Государственное и муниципальное управление" (квалификация (степень) "магистр") / Г. И. Москвитин, [и др.], Рос. экономич. ун-т им. Г. В. Плеханова ; ред. Г. И. Москвитин . – М. : КноРус, 2019 . – 340 с. – (Бакалавриат и магистратура) . - ISBN 978-5-406-06684-3 .

12. Минзов, А. С. Управление рисками информационной безопасности : [монография] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов ; ред. А. С. Минзов ; Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – Москва : ВНИИгеосистем, 2019 . – 106 с. - ISBN 978-5-8481-0240-6 .

13. Организационное поведение : учебник и практикум для вузов по экономическим направлениям и специальностям / С. А. Барков, О. В. Гавриленко, В. И. Зубков, [и др.] ; ред. С. А. Барков . – Москва : Юрайт, 2020 . – 453 с. – (Высшее образование) . - Авторы указаны на 6-й с. - ISBN 978-5-534-00926-2 .

14. Антонов И. Ю.- "Стратегия и методология инновационного развития: зарубежный и отечественный опыт", Издательство: "Дашков и К", Москва, 2013 - (159 с.)

15. А. И. Егоров- "Основы теории управления", Издательство: "Физматлит", Москва, 2007 - (506 с.)

16. Прохорова О. В.- "Информационная безопасность и защита информации", (2-е изд., испр.), Издательство: "Лань", Санкт-Петербург, 2020 - (124 с.)

17. "Интеллектуальный анализ данных средствами MS SQL Server 2008", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (337 с.)

18. Бондаренко И. С., Демчишин Ю. В.- "Методы и средства защиты информации", Издательство: "МИСИС", Москва, 2018 - (32 с.)

19. А. К. Шилов- "Управление информационной безопасностью", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2018 - (121 с.)

20. Басенко В. П., Жуков Б. М., Романов А. А.- "Организационное поведение", Издательство: "Дашков и К", Москва, 2020 - (384 с.)

## **6.2 Лицензионное и свободно распространяемое программное обеспечение:**

1. СДО "Прометей"
2. Office / Российский пакет офисных программ
3. Windows / Операционная система семейства Linux
4. Видеоконференции (Майнд, Сберджаз, ВК и др)
5. Антиплагиат ВУЗ

## **6.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:**

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - [http://biblioclub.ru/index.php?page=main\\_ub\\_red](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>
4. База данных ВИНТИ online - <http://www.viniti.ru/>
5. Электронные ресурсы издательства Springer - <https://link.springer.com/>
6. База данных Web of Science - <http://webofscience.com/>
7. База данных Scopus - <http://www.scopus.com>

8. Национальная электронная библиотека - <https://rusneb.ru/>  
 9. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>  
 10. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>  
 11. Информо - <https://www.informio.ru/>

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

При подготовке к ГИА и проведения ГИА используются учебные аудитории и помещение для самостоятельной работы обучающихся. Примерный перечень помещений приведен в таблице.

Тип помещения	Номер аудитории, наименование	Оснащение
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стол письменный, стул, принтер, кондиционер, вешалка для одежды, светильник потолочный с диодными лампами, компьютерная сеть с выходом в Интернет, компьютер персональный
Помещения для консультирования	М-511, Учебная аудитория	стол преподавателя, парта, стул, экран, мультимедийный проектор, доска маркерная, компьютер персональный
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	стол преподавателя, парта, стул, экран, мультимедийный проектор, доска маркерная, компьютер персональный
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер, коммутатор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, шкаф для хранения инвентаря, шкаф для документов, стол, стул, светильник потолочный с люминесцентными лампами, коммутатор, тумба, электрические розетки, запасные комплектующие для оборудования, информационные (интернет) розетки
Помещения для самостоятельной работы	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, компьютер персональный, сервер, электрические розетки, компьютерная сеть с выходом в Интернет, информационные (интернет) розетки, вешалка для одежды, тумба, кондиционер, коммутатор, доска маркерная, экран, мультимедийный проектор
Помещения для самостоятельной работы	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, компьютер персональный, сервер, электрические розетки, информационные (интернет) розетки, светильник потолочный с люминесцентными лампами, коммутатор, доска маркерная, экран, мультимедийный проектор, кондиционер

Помещения для консультирования	К-601, Учебная аудитория	стол преподавателя, стул, парта со скамьей, экран, мультимедийный проектор, доска меловая, светильник потолочный с люминесцентными лампами, трибуна
--------------------------------	--------------------------	---