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

Направление подготовки: 10.03.01 Информационная безопасность

Наименование образовательной программы: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: очная

Программа
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Блок	**Блок 3 «Государственная итоговая аттестация»**
Трудоемкость в зачетных единицах	**8 семестр - 6 з.е.**
Часов (всего) по учебному плану	**216 часов**
в том числе:	
подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы	8 семестр - 216 часов

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
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 – Оценка подготовленности обучающегося к решению задач профессиональной деятельности.

Задачами государственной итоговой аттестации:

– оценка сформированности всех компетенций, установленных образовательной программой;

– оценка освоения результатов обучения требованиям федерального государственного образовательного стандарта по направлению подготовки 10.03.01 «Информационная безопасность» и профессиональных стандартов.

2. РЕЗУЛЬТАТЫ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

К результатам обучения выпускника относятся следующие компетенции:

ОК-1. способностью использовать основы философских знаний для формирования мировоззренческой позиции.

ОК-2. способностью использовать основы экономических знаний в различных сферах деятельности.

ОК-3. способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма.

ОК-4. способностью использовать основы правовых знаний в различных сферах деятельности.

ОК-5. способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

ОК-6. способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.

ОК-7. способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.

ОК-8. способностью к самоорганизации и самообразованию.

ОК-9. способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности.

ПСК-1. Способность администрировать подсистемы информационной безопасности объектов, объекты энергетики КВО РФ, эксплуатирующие АСУ ТП.

ПСК-2. Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасносго функционирования объектов энергетики с элементами АСУ ТП.

ПСК-3. Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП.

ОПК-1. способностью анализировать физические явления и процессы для решения профессиональных задач.

ОПК-2. способностью применять соответствующий математический аппарат для решения профессиональных задач.

ОПК-3. способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач.

ОПК-4. способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

ОПК-5. способностью использовать нормативные правовые акты в профессиональной деятельности.

ОПК-6. способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.

ОПК-7. способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

ПК-1. способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

ПК-2. способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

ПК-3. способностью администрировать подсистемы информационной безопасности объекта защиты.

ПК-4. способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

ПК-5. способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

ПК-6. способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

ПК-7. способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

ПК-8. способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.

ПК-9. способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

ПК-10. способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

ПК-11. способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

ПК-12. способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

ПК-13. способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

ПК-14. способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности.

ПК-15. способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

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 8 семестре после успешного прохождения промежуточной аттестации по всем дисциплинам (модулям) и практикам образовательной программы.

В государственную итоговую аттестацию входит подготовка к процедуре защиты и процедура защиты 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 «Организация и технология защиты информации» по направлению 10.03.01 «Информационная безопасность».

Примерная тематика ВКР:

1. Разработка модели нарушителя информационной безопасности в организации, относящейся к критической информационной инфраструктуре.
2. Разработка модели нарушителя информационной безопасности в организации.
3. Разработка модели угроз информационной безопасности в финансовокредитном учреждении.
4. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам.
5. Имитационное моделирование сценариев рисков информационной безопасности.
6. Защита персональных данных финансово-кредитной организации.
7. Мониторинг состояния объекта на основе оценки рисков.
8. Аттестация системы информационной безопасности государственной информационной системы.
9. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001.
10. Защита интеллектуальной собственности в организации.
11. Защита служебной тайны в организации.
12. Защита информации в концепции стандарта COBIT 5.0 (на примере некоммерческой организации).
13. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации).
14. Защита коммерческой тайны в организации.

15. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере финансово-кредитного учреждения).

16. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере организации малого (среднего) бизнеса).

17. Инвентаризация информационных активов организации.

18. Защита электронного документооборота на предприятии.

19. Защита персональных данных в медицинских учреждениях.

20. Защита персональных данных в организации с участием государства (муниципальном образовании).

21. Защита персональных данных в коммерческой организации.

22. Анализ рисков информационной безопасности в информационной системе персональных данных.

23. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей.

24. Инвентаризация и классификация информационных активов организации при оценке рисков.

25. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении.

26. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении.

27. Внедрение технологии управления информацией и событиями безопасности (SIEM-системы) в организации.

28. Внедрение технологий предотвращения утечки информации (DLP-системы) в организации.

29. Разработка программы проведения внутреннего аудита информационной безопасности организации.

30. Разработка программы проведения аудита информационной безопасности в организации.

31. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации».

32. Разработка средств автоматизации для исследования программного обеспечения по требованиям безопасности информации.

33. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации.

34. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении.

35. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа.

36. Администрирование системы резервного копирования для защиты информационных активов организации.

37. Администрирование средств межсетевого экранирования в системе защиты информации организации.

38. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации.

39. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга.

40. Разработка рекомендаций по защите конфиденциальной информации от утечки по акустическому каналу из защищаемого помещения пассивными методами.

41. Разработка предложений по повышению защищенности вычислительной техники по каналу ПЭМИ пассивными методами.

42. Разработка проекта системы защиты конфиденциальной информации в организации.

43. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации.

44. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи.

45. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации.

46. Моделирование рисков информационной безопасности в информационных системах, построенных по технологии блокчейн.

47. Моделирование угроз персональным данным в организации.

48. Формирование требований к сотруднику службы информационной безопасности при внедрении профессиональных стандартов.

49. Организация мониторинга действий персонала организации с целью выявления инцидентов информационной безопасности.

50. Организация аудита информационной безопасности организации с использованием специального программного обеспечения.

51. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux.

52. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux.

53. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux.

54. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux.

55. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows.

56. Организация расследования инцидентов информационной безопасности на предприятии.

57. Управление поведением персонала при организации безопасной работы в информационной системе организации.

58. Организация проверки и оценки уровня подготовки персонала предприятия, участвующего в обработке конфиденциальной информации.

59. Разработка частных политик информационной безопасности для организации.

60. Организация режима коммерческой тайны на предприятии.

61. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики.

62. Оценка и анализ рисков с использованием программного обеспечения CORAS.

63. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей.

64. Исследование механизмов целостности и доступности информации на платформе блокчейн..

65. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации.

66. Анализ уязвимостей систем удаленного видеонаблюдения на предприятии.

67. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах.

68. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ.

69. Подготовка персонала организации, использующего в работе конфиденциальную информацию с использованием дистанционных образовательных технологий.

70. Разработка технического проекта создания защищаемого помещения в организации.

71. Автоматизация процессов менеджмента информационной безопасности в организации.

72. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии.

73. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия.

74. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет.

75. Защита локальной вычислительной сети организации с использованием IDS/IPS систем.

76. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных.

77. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных.

78. Обеспечение безопасности сетевого взаимодействия с использованием технологии IPSec.

79. Внедрение в организации системы резервного копирования.

80. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации.

81. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN.

82. Разработка и внедрение электронной подписи в документооборот организации.

83. Применение систем контроля и управления процессами («вывода на печать» или «вывода на внешние носители информации» или «отправки файлов через интернет» или «отправки файлов по электронной почте») в (название организации).

84. Программная защита информационной системы организации на основе возможностей операционной системы.

85. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места.

86. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики).

87. Обеспечение режима конфиденциальности в организации при увольнении сотрудников.

88. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию.

89. Обеспечение безопасности информации на объектах критической информационной инфраструктуры.

90. Разработка комплекса мероприятий по сертификации средства защиты информации.

91. Разработка комплекса мероприятий по сертификации средства обработки конфиденциальной информации.

92. Разработка комплекса мероприятий по лицензированию деятельности предприятия по технической защите конфиденциальной информации.

93. Разработка политики информационной безопасности организации.

94. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN.

95. Защита от несанкционированных проводных подключений к локальной сети (название организации).

96. Применение технологии активного аудита информационной безопасности в организации.

97. Внедрение системы менеджмента инцидентов информационной безопасности в коммерческом банке.

98. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия.

99. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов.

100. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу.

101. Разработка проекта технической защиты конфиденциальной информации на предприятии от ее утечки по (конкретный вид) каналу.

102. Разработка и реализация программы повышения осведомленности сотрудников предприятия (организации) в области информационной безопасности.

103. Документальное обеспечение режима коммерческой тайны предприятия.

104. Разработка комплекта документации по результатам аттестации объекта информатизации (автоматизированной системы).

105. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персона и степени их дублирован.

106. Методика генерации сценариев целевых атак на информационные системы.

107. Методика инвентаризации, классификации и анализа информационных активов организации.

108. Обеспечение информационной безопасности Интернета вещей в цифровой экономике.

109. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков.

110. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos.

111. Моделирование уязвимостей протоколов защиты SSL.

112. Моделирование уязвимостей протоколов защиты TLS.

113. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании.

114. Криптографические способы контроля целостности и их практическая реализация.

115. Защита информации с использованием методов и технологий упрощенной криптографии в организации.

116. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности.

117. Проведение аудита информационной безопасности организации с использованием сканера безопасности.

118. Расследование инцидентов информационной безопасности в организации.

119. Разработка программы специального обследования защищаемого помещения (кабинета, переговорной комнаты, конференц-зала и т.д.) предприятия (организации).

120. Организация центра управления информационной безопасностью в финансовокредитном учреждении.

5.2. Требования к ВКР

Полностью оформленный диплом автор сдает руководителю за 10 рабочих дней до защиты (+2 CD-диска с текстом работы).

Руководитель проводит со студентом предзащиту с участием заведующего или заместителя заведующего по учебной работе.

Не позднее чем за 7 рабочих дней до защиты автор передает диплом рецензенту.

Диплом, отзыв руководителя и рецензия на работу должны быть представлены на подпись заведующему кафедрой для допуска к защите не позднее чем за 2 рабочих дня до заседания ГЭК.

Рекомендуемая продолжительность защиты ВКР — не более 30 минут. Процедура защиты ВКР состоит из следующих этапов:
•объявление секретаря ГЭК об очередной защите ВКР (автор ВКР, тема ВКР, руководитель ВКР и наличие полного комплекта документов)
•доклад обучающегося
•представление отзыва руководителя ВКР и рецензии(й)
•ответы обучающегося на вопросы членов ГЭК.

5.3. Объем текстовой части

Подготовка к защите ВКР начинается на последнем семестре обучения в соответствии с календарным графиком учебного плана.
Практические материалы для выполнения ВКР собираются студентом в ходе преддипломной практики.
Тема выпускной квалификационной работы должна быть актуальной, представлять научный и (или) практический интерес и соответствовать выбранному студентом направлению подготовки.
Перечень тем выпускных квалификационных работ разрабатывается выпускающей кафедрой. Обучающемуся предоставляется право выбора темы выпускной квалификационной работы из числа тем, предложенных выпускающей кафедрой.
По письменному заявлению обучающийся может предложить свою тему с необходимым обоснованием целесообразности её разработки для практического применения в соответствующей области профессиональной деятельности или на конкретном объекте профессиональной деятельности.
Темы ВКР утверждаются протоколом заседания кафедры.
Для подготовки выпускной квалификационной работы студенту назначается руководитель и, при необходимости, консультанты.
Основные функции научного руководителя выпускной квалификационной работы:
– формирование задания на подготовку ВКР;
– консультирование студента по подбору литературных источников и информации, необходимых для выполнения ВКР;
– проведение систематических консультаций по проводимому исследованию;
– контроль выполнения хода работы, оценка содержания выполненной работы по частям и, в случае необходимости, внесение корректировок;
– представление письменного отзыва, содержащего характеристику работы студенты в период подготовки ВКР;
– оказание помощи (консультирование студента) в подготовке презентации и вступительного слова (доклада) для защиты ВКР.
В обязанности консультанта входит:
– оказание помощи студенту в подборе необходимой литературы, в части содержания консультируемого вопроса;
– контроль хода выполнения выпускной квалификационной работы, в части содержания консультируемого вопроса.
После утверждения темы выпускной квалификационной работы научный руководитель совместно со студентом и, при необходимости, с привлечением консультанта, разрабатывает задание на подготовку выпускной квалификационной работы.
Задание включает в себя название, перечень подлежащих разработке вопросов, перечень исходных данных, необходимых для выполнения ВКР (нормативные правовые акты, научная и специальная литература, конкретная первичная информация), календарный план-график выполнения отдельных разделов ВКР, срок представления законченной работы.

ВКР выполняется студентом самостоятельно в соответствии с заданием.
Контроль за ходом выполнения работ, предусмотренных заданием, осуществляется научным руководителем. Отставание от календарного плана подготовки выпускной квалификационной работы доводится научным руководителем до сведения заведующего кафедрой.
Написание ВКР имеет целью закрепление, систематизацию и расширение теоретических знаний и углублённое исследование актуальных проблем в сфере "Технологии разработки программного обеспечения". В процессе выполнения ВКР студент должен показать теоретические знания, полученные в процессе обучения, проявить навыки самостоятельной работы, способность решать конкретные практические задачи..

5.4. Объем демонстрационной части

К защите к выпускной квалификационной работы допускается студент успешно сдавший государственный экзамен, а также при наличии письменной рецензии рецензента и отзыва научного руководителя, после получения на титульном листе выпускной квалификационной работы подписей научного руководителя и допуска заведующего кафедрой (или заместителя заведующего кафедрой по учебной работе)..

5.5. Порядок выполнения ВКР

1. Получение задания на ВКР от руководителя.
2. Согласование и утверждение структуры работы руководителем ВКР.
3. Выполнение ВКР в соответствии с заданием.
4. Оформление ВКР в соответствии с требованиями.
5. Экспертиза готовой выпускной квалификационной работы на заимствования.
6. Передача написанной и оформленной работы для получения отзыва руководителя.
7. Подготовка доклада и презентационного материала для защиты 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 4 3	средний балл по приложению к диплому с округлением до сотых долей	30
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	15
		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	5 4 3	на основе отзыва руководителя по решению ГЭК	15
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;	40

		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.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИА

При подготовке к ГИА студент может воспользоваться

6.1 Печатные и электронные издания:

1. Петренко, С. А. Аудит безопасности Intranet / С. А. Петренко, А. А. Петренко . – М. : ДМК Пресс, 2002 . – 416 с. – (Информационные технологии для инженеров) . - ISBN 5-940741-83-5 .

6.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей"
2. Office / Российский пакет офисных программ
3. Windows / Операционная система семейства Linux
4. Майнд Видеоконференции
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

3. Научная электронная библиотека - https://elibrary.ru/

4. Электронные ресурсы издательства Springer - https://link.springer.com/

5. База данных Web of Science - http://webofscience.com/

6. База данных Scopus - http://www.scopus.com

7. Национальная электронная библиотека - https://rusneb.ru/

8. ЭБС "Консультант студента" - http://www.studentlibrary.ru/

9. Журнал Science - https://www.sciencemag.org/

10. Электронная библиотека МЭИ (ЭБ МЭИ) - http://elib.mpei.ru/login.php

11. Информационно-справочная система «Кодекс/Техэксперт» - Http:\\proinfosoft.ru; http://docs.cntd.ru/

12. Открытая университетская информационная система «РОССИЯ» - https://uisrussia.msu.ru

13. Федеральный портал "Российское образование" - http://www.edu.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-303, 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-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, компьютер персональный, экран, мультимедийный проектор, стенд лабораторный, телевизор, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, компьютер персональный, экран, мультимедийный проектор, стенд лабораторный, телевизор, кондиционер
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