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: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: очно-заочная

Программа
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Блок	**Блок 3 «Государственная итоговая аттестация»**
Трудоемкость в зачетных единицах	**10 семестр - 6 з.е.**
Часов (всего) по учебному плану	**216 часов**
в том числе:	
подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы	10 семестр - 216 часов

Москва 2019

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 – определить соответствие результатов освоения обучающимся основной образовательной программы «Безопасность автоматизированных систем» по направлению подготовки 10.03.01 «Информационная безопасность», соответствующим требованиям федерального государственного образовательного стандарта.

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 10 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 «Безопасность автоматизированных систем» по направлению 10.03.01 «Информационная безопасность».

Обучающемуся может предоставляться право выбора темы ВКР в установленном порядке, вплоть до предложения своей тематики с необходимым обоснованием целесообразности ее разработки. Тематика ВКР должна соответствовать области (сфере), объекту и типам задач профессиональной деятельности, к которым готовится выпускник в рамках освоения образовательной программы.

Примерная тематика ВКР:

1. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux;.
2. Оценка опасности уязвимостей беспроводных информационных технологий на основе Kali Linux;.
3. Методы и технологии обнаружения скрытых контейнеров в сообщениях методами статистического анализа;.
4. Методика генерации сценариев целевых атак на информационные системы;.
5. Разработка квестов по обучению технологии проникновения в защищенную сеть (этичный хакинг);.
6. Инвентаризация и классификация информационных активов организации при оценке рисков;.

7. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации);.

8. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики;.

9. Организация расследования инцидентов информационной безопасности на предприятии;.

10. Оценка опасности уязвимостей смарт-контрактов в технологии блокчейн;.

11. Технологии реверсинга (обратного программирования) и их применение при исследовании недекларированных функций программного обеспечения;.

12. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей;.

13. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности;.

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

15. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos.

16. Моделирование уязвимостей протоколов защиты SSL;.

17. Моделирование уязвимостей протоколов защиты TLS;.

18. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании;.

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

20. Проведение аудита информационной безопасности организации с использованием сканера безопасности;.

21. Расследование инцидентов информационной безопасности в организации;.

22. Организация центра управления информационной безопасностью в финансово-кредитном учреждении;.

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

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

25. Обеспечение информационной безопасности Интернета вещей в цифровой экономике;.

26. Организация аудита информационной безопасности организации с использованием специального программного обеспечения;.

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

28. Анализ методов обеспечения информационной безопасности в беспроводных сетях передачи информации;.

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

30. Оценка защищенности помещения от утечки речевой информации по линиям охранно-пожарной сигнализации;.

31. Исследование уязвимостей системы радиотехнической идентификации систем и объектов;.

32. Оценка защищенности автоматизированного рабочего места от утечки конфиденциальной информации по каналу ПЭМИ при применении средств активной защиты;.

33. Оценка защищенности АРМ от утечки конфиденциальной информации по каналу ПЭМИ матрицы монитора;.

34. Оценка защищенности автоматизированного рабочего места от утечки конфиденциальной информации по каналу ПЭМИ считывателя SD-карт;.

35. Оценка защищенности конфиденциальной информации организации, обрабатываемой в ТСПИ от утечки за счет наводок;.

36. Оценка защищенности технических средств и систем организации, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации;.

37. Оценка защищенности помещения организации от утечки речевой конфиденциальной информации по каналу электроакустических преобразований;.

38. Оценка защищенности помещения организации от утечки речевой конфиденциальной информации по акустическому (виброакустическому) каналу;.

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

40. Моделирование угроз персональным данным в организации;.

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

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

43. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении;.

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

45. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении;.

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

47. Аттестация системы информационной безопасности государственной информационной системы;.

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

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

50. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа;.

51. Разработка и внедрение электронной подписи в документооборот организации;.

52. Оценка и анализ рисков с использованием программного обеспечения CORAS;.

53. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга;.

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

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

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

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

58. Разработка технического проекта создания защищаемого помещения в организации;.

59. Разработка программы проведения аттестационных испытаний по оценке защищенности автоматизированного рабочего места от утечки информации по электромагнитному каналу;.

60. Разработка программы проведения аттестационных испытаний по оценке защищенности переговорной комнаты (конференц-зала и т.д.) от утечки информации по

акустическому (виброакустическому, акустоэлектрическому, электроакустическому) каналу;.

61. Разработка программы специального исследования защищенности средств ВТСС в конференц-зале от утечки речевой информации по акустоэлектрическому каналу;.

62. Разработка программы специального исследования защищенности ТСПИ и ВТСС в кабинете руководителя от утечки опасных сигналов ПЭМИН;.

63. Разработка программы специальной проверки технических средств и систем организации, обрабатывающих конфиденциальную информацию;.

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

65. Разработка технического задания на систему защиты информации в переговорной комнате (конференц-зале) организации от утечки по (конкретный вид ТКУИ) каналу;.

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

67. Разработка программы проведения радиомониторинга в защищаемом помещении организации;.

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

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

70. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов;.

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

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

73. Обеспечение безопасности информации на объектах критической информационной инфраструктуры;.

74. Имитационное моделирование сценариев рисков информационной безопасности;.

75. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам;.

76. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001;.

77. Разработка проекта технической защиты информации в кабинете руководителя организации от утечки по (конкретный вид) каналу;.

78. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персона и степени их дублирования;.

79. Разработка проекта системы защиты конфиденциальной информации в организации;.

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

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

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

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

84. Внедрение системы антивирусной защиты в организации;.

85. Администрирование системы резервного копирования для защиты информационных активов организации;.

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

87. Защита информации в вычислительной сети организации с использованием возможностей провайдеров;.

88. Защита локальной вычислительной сети организации от несанкционированного доступа к её ресурсам с использованием маршрутизаторов уровня локальных сетей;.

89. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN;.

90. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows;.

91. Программная защита информационной системы организации на основе возможностей операционной системы;.

92. Администрирование программно-аппаратного комплекса «Аккорд» на рабочих станциях организации;.

93. Защита сетевого хранилища организации;.

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

95. Защита беспроводных подключений к локальной вычислительной сети при использовании точек доступа общего пользования;.

96. Администрирование локальной вычислительной сети организации при использовании сервисов и ресурсов сети интернет;.

97. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN;.

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

99. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии;.

100. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию;.

101. Мониторинг состояния объекта на основе оценки рисков;.

102. Методика инвентаризации, классификации и анализа информационных активов организации;.

103. Защита интеллектуальной собственности в организации.

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

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

106. 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);.

107. Защита файлового архива организации средствами операционной системы;.

108. Автоматизация процессов менеджмента информационной безопасности в организации;.

5.2. Требования к ВКР

ВКР состоит из двух обязательных частей:

– текстовой части;

– демонстрационная часть, представляющая собой графический материал и/или электронную презентацию. Демонстрационная часть содержит необходимые для наиболее полного представления работы конструкторские проработки (чертежи), схемные решения, демонстрационные плакаты (с отражением на них, в том числе, синтезированных и/или

использованных математических моделей, алгоритмов, структур программ, полученных результатов и т.д.). По согласованию с руководителем возможно представление макетов, физических моделей, видеофайлов, документированных актов и т.п.
К содержанию ВКР предъявляются следующие требования:
– соответствие содержания сформулированной теме;
– полнота раскрытия темы;
– логическая последовательность и завершенность.
В соответствии с планом ВКР должна быть разделена на отдельные логически связанные части, снабженные короткими и ясными заголовками, отражающими смысл излагаемого в них материала.

5.3. Объем текстовой части

Рекомендуемый объем основной части ВКР (не включая приложений) должен быть не менее 40 и не более 80 листов стандартно набранного текста (1,5 интервала, не менее 12 кегля, единый тип шрифта по всей работе), оформленного по ГОСТ 7.32-2017, ГОСТ Р 2.105-2019, ГОСТ 2.106-2019. Рекомендуемый объем ВКР по разделам:
– введение – 1–3 стр.,
– основная часть (главы) – не менее 35–55 стр.,
– заключение – 1–3 стр.
Рекомендуемый объем приложений не регламентируется, однако должен быть обоснован реальной необходимостью представления материалов.

5.4. Объем демонстрационной части

Рекомендуется в графическую часть включать 3–4 листа формата А1 в зависимости от необходимости раскрытия объекта.
Рекомендуется в электронную презентацию должна содержать не менее 6 и не более 12 слайдов.

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	25
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	20
		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	на основе отзыва руководителя по решению	15

		3	ГЭК	
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. Минзов, А. С. Профессиональная этика в сфере информационной и экономической безопасности : [монография] / А. С. Минзов, Нац. исслед. ун-т "МЭИ", Ин-т информац. и экономич. безопасности . – М. : ВНИИгеосистем, 2013 . – 132 с. - ISBN 978-5-8481-0135-5 .

2. 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 .

3. Дао К.Х. Информационная безопасность в АСУ ТП : магистерская диссертация / Дао К.Х., Нац. исслед. ун-т "МЭИ", Кафедра автоматизированных систем управления технологическими процессами (АСУТП) . – М., 2015 . – 87 с. - диссертация только в электронном виде,для чтения перейдите в электронную библиотеку МЭИ .

4. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие для вузов по специализациям специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / В. И. Васильев . – 2-е изд., испр . – М. : Машиностроение, 2013 . – 172 с. – (Для вузов) . - ISBN 978-5-94275-667-3 .

5. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников . – 2-е изд., стереотип . – М. : КноРус, 2013 . – 136 с. + CD . – (Бакалавриат) . - ISBN 978-5-406-02760-8 .

6. Шубин, В. И. Беспроводные сети передачи данных : учебное пособие для вузов по направлению 210700 "Инфокоммуникационные технологии и системы связи" / В. И. Шубин, О. С. Красильникова . – 2-е изд . – М. : Вузовская книга, 2013 . – 104 с. - ISBN 978-5-9502-0725-9 .

7. Правовое обеспечение контроля, учета, аудита и судебно-экономической экспертизы : учебник для студентов вузов, обучающихся по юридическим, экономическим направлениям / Е. М. Ашмарина, Н. М. Артемов, А. Б. Быля, [и др.] ; ред. Е. М. Ашмарина . – 2-е изд., перераб. и доп . – Москва : Юрайт, 2020 . – 299 с. – (Высшее образование) . - Под общим руководством В. В. Ершова . - ISBN 978-5-534-09038-3 .

8. Абдухалилов, Г. А. Разработка методики автоматизированного проектирования схем оперативной блокировки цифровых подстанций: 05.14.02 "Электрические станции и электроэнергетические системы" : автореферат кандидата технических наук / Г. А. Абдухалилов, Нац. исслед. ун-т "МЭИ" . – М., 2017 . – 20 с.

9. Скрыдлов, Е. И. Устройство контроля и передачи на верхний уровень параметров цифровых трансформаторов тока на современных цифровых подстанциях : магистерская диссертация / Е. И. Скрыдлов, Нац. исслед. ун-т "МЭИ", Кафедра информационно-измерительной техники (ИИТ) . – М., 2015 . – 49 с. - диссертация только в электронном виде,для чтения перейдите в электронную библиотеку МЭИ .

10. 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 .

11. 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 .

12. Скородумова, О. Б. Хакеры как феномен информационного пространства / О. Б. Скородумова . – 2004 // Социологические исследования (СОЦИС) : Ежемесячный научный и общественно-политический журнал . – 02/2004 . – N2 . – с.70-80 . - В статье исследуется один из важных аспектов обеспечения информационной безопасности - борьба с хакерами, рассматриваются истоки хакерства, противоречивость оценок этого феномена и др. аспекты.

13. В. И. Аверченков- "Аудит информационной безопасности", (4-е изд., стер.), Издательство: "ФЛИНТА", Москва, 2021 - (269 с.)

14. Трофимов В. Б., Темкин И. О.- "Экспертные системы в АСУ ТП", Издательство: "Инфра-Инженерия", Вологда, 2020 - (284 с.)

15. А. Абденов, Г. Дронова, В. Трушин- "Современные системы управления информационной безопасностью", Издательство: "Новосибирский государственный технический университет", Новосибирск, 2017 - (48 с.)

16. "Информационная безопасность", Издательство: "ГРОТЕК", Москва, 2012 - (51 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. 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	Ж-120, Машинный зал ИВЦ	сервер, кондиционер, коммутатор

аттестации		
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